

VU LEARNING HUB

vulearninghub.xyz

HIGHLIGHTED HANDOUT

CS627

CS627

CS627 by VU Learning HUB

Prepared for VU students • Free study resources

<https://vulearninghub.xyz>



CYBER SECURITY

Microsoft
CERTIFIED
Systems Administrator

Microsoft
CERTIFIED
Systems Engineer

CS-627 MIDTERM

Topics (1-6 Weeks)

Compiled by : YASIR EJAZ
(MCP, MCSE, MCSA)

0321-5253058

0321-5620799

yasirejaz@gmail.com

Cyber Security

Importance of Cyber Security

- Mobile Phones
- Total population of Pakistan (2020) → 219,067,896
- Number of **mobile phone users in Pakistan** has reached 161.183 million, as of May 2019.
 - Smart phones
 - Traditional phones:
 - SMS / Call Scams

Importance of Cyber Security

- Drones

- Here's How Hackers Could Have Spied On Your DJI Drone Account

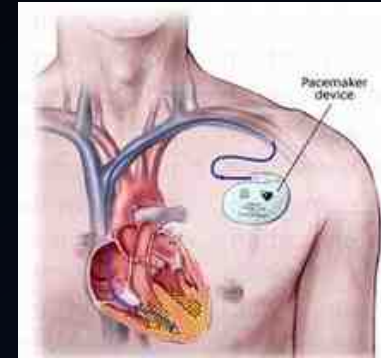
- https://thehackernews.com/2018/11/dji-drone-hack_8.html



Importance of Cyber Security

- Health / Medical

- **Pacemaker:** a device for stimulating the heart muscle and regulating its contractions.



- **Robotic Surgeons**

- 5 Medical Robots Making a Difference in Healthcare

- <https://online-engineering.case.edu/blog/medical-robots-making-a-difference>

- **Remote Surgery**

- China completes world's first 5G remote surgery in test on animal

- <https://www.youtube.com/watch?v=yFR61jjL1vo>

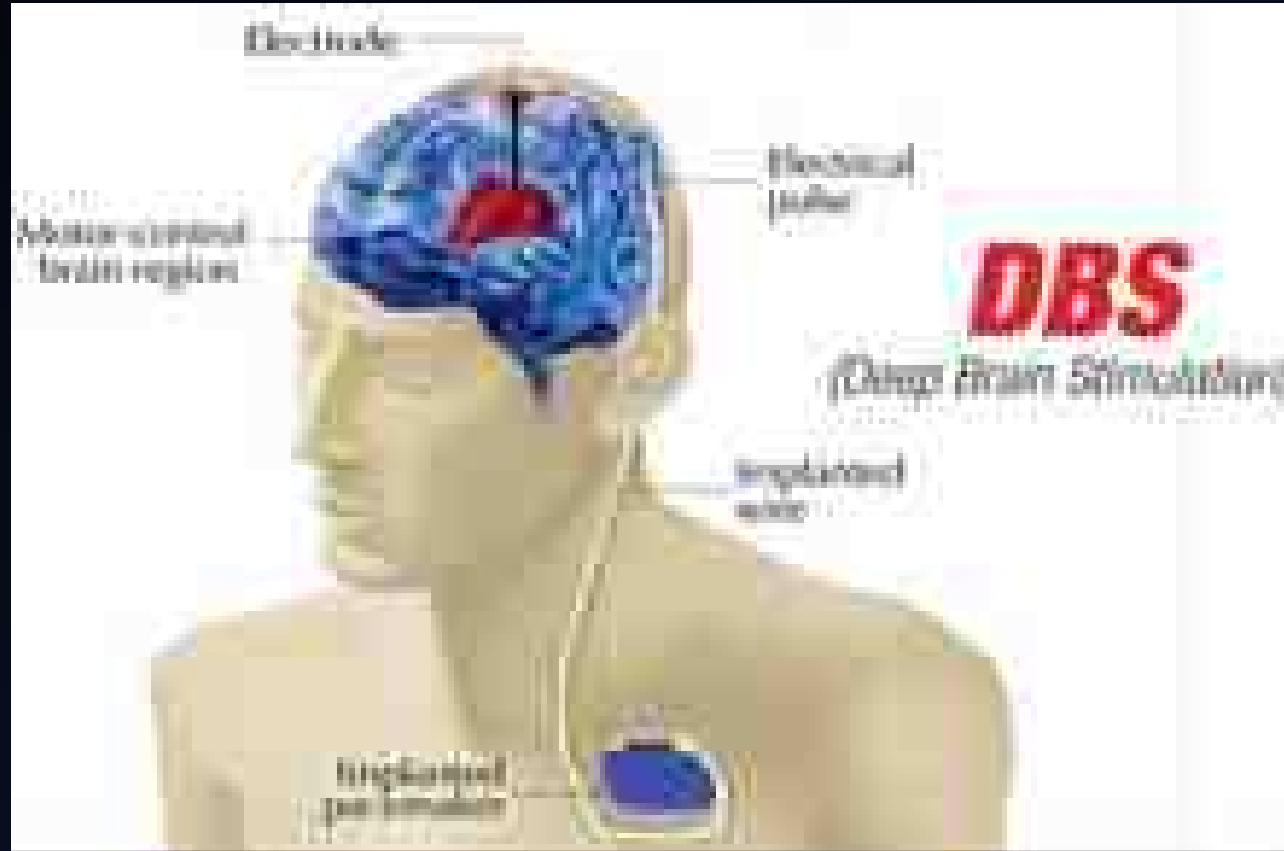
- Robot Helps Perform First Long-Distance Heart Surgery

- A surgeon in India performed the first remote heart operation on a patient 20 miles away.

- <https://www.popularmechanics.com/technology/robots/a28941179/robot-performs-first-long-distance-heart-surgery/>



Bluetooth in health



- The field of 'Cyber Security' is becoming more important due to increased reliance on
 - computer systems
 - the Internet
 - wireless network standards
 - such as Bluetooth and Wi-Fi
 - due to the growth of "smart" devices
 - including smartphones, televisions, and the "Internet of things".
- Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.
 - Ease of use results in increasing underlying complexity

What is Cyber Security?

- Cyber

- Relating to or characteristic of the culture of computers, information technology, and virtual reality.
- **Cyberspace** is a term for virtual reality coined by William Gibson.
 - <https://en.wikipedia.org/wiki/Cyberspace>
- **Cyber-** is derived from "**cybernetic**", [<https://en.wikipedia.org/wiki/Cybernetics>] which comes from the **Greek word** κυβερνητικός meaning '*skilled in steering or governing*'.
 - Pronunciation:
[<https://forvo.com/word/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%B7%CF%84%CE%B9%CE%BA%CF%8C%CF%82/>]
- **Cybernetics**: the science of communications and automatic control systems in both machines and living things.
- Used to describe **policies** and **politics** regarding **computer systems** and **networks**.
- Term used in **Information Technology** industry and the **Internet** era.
 - https://en.wikipedia.org/wiki/Internet-related_prefixes#.22Cyber-.22
 - <https://en.wikipedia.org/wiki/Cyber>

What is Cyber Security?

- Security

- Degree of 'protection' [safe & secure].
- The state of being free from danger or threat.
- **Security** is freedom from, or resilience against, potential harm caused by others. [Wikipedia]
 - <https://en.wikipedia.org/wiki/Security>

What is Cyber Security?

- **Computer security, cybersecurity or information technology security (IT security)** is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.
 - https://en.wikipedia.org/wiki/Computer_security

Security Realms

- Information Security
- IT Security
- Cyber Security
- Network Security
- System Security
- Data Security
- Operating System Security
- Physical Security

Information Security

- **Information security**, sometimes shortened to **infosec**, is the 'practice of protecting information' by mitigating information risks.
- It is part of information risk management.
- It typically involves preventing or at least reducing the probability of unauthorized/inappropriate access, use, disclosure, disruption, deletion/destruction, corruption, modification, inspection (monitor), recording or devaluation of data and/or systems.
- Information may take any form, e.g. electronic or physical.

Cyber Security vs InfoSec



GENERAL SECURITY

TOP SECRET

INFORMATION SECURITY

Information security is the protection of information and communication systems from unauthorized access, use, disclosure, modification, or destruction. It is a critical component of overall security and is essential for the protection of sensitive information and the integrity of systems.

Information security is a multidisciplinary field that involves the application of security principles and practices to the protection of information and communication systems. It is a dynamic field that evolves as technology and threats change.

Information security is a critical component of overall security and is essential for the protection of sensitive information and the integrity of systems.

Information security is a critical component of overall security and is essential for the protection of sensitive information and the integrity of systems.

Information security is the protection of information and communication systems from unauthorized access, use, disclosure, modification, or destruction. It is a critical component of overall security and is essential for the protection of sensitive information and the integrity of systems.

Information security is a multidisciplinary field that involves the application of security principles and practices to the protection of information and communication systems. It is a dynamic field that evolves as technology and threats change.

Information security is a critical component of overall security and is essential for the protection of sensitive information and the integrity of systems.

Information security is a critical component of overall security and is essential for the protection of sensitive information and the integrity of systems.

Cyber Security Jobs & Careers

<https://www.cybersecurityeducation.org/careers/>

- Start at any point in your life / career.
- Wide range of responsibilities.
- Crux of the job is to **protect online data and systems** from being compromised.
- Cyber security careers are **complex**.
- Many roles can be found with banks, retailers and government organizations.
- On the job, you can expect to:
 - **safeguard** an organization's files and network
 - install / configure firewalls
 - create security plans
 - monitor activity
 - If a breach occurs, you'll be responsible for **identifying the problem** and **finding a solution** quickly.
- Because of the frequency of cyber attacks, **careers are varied** and **qualified professionals are in demand**.
- If you're ready to get started in this fast-growing career, start exploring cyber careers now.

Job Titles

- Cyber Security Vendor
 - Solution Provider
 - Services
- Security Auditor
- PenTester / Ethical Hacker
- Security Analyst
- InfoSec Engineer
- InfoSec Consultant

- Malware Analyst
- Forensic Analyst/Expert/Investigator
- Incident Handler / Manager
- InfoSec / Cyber Security Specialist
- InfoSec Manager
- CISO

TOP 10 CYBER SECURITY JOB TITLES

- 1. Security Engineer
- 2. Security Analyst
- 3. Information Security Analyst
- 4. Information Security Engineer
- 5. Network Security Engineer
- 6. Information Technology Security Analyst
- 7. Information Security Manager
- 8. Information Assurance Engineer
- 9. Senior IT Auditor
- 10. Security Administrator



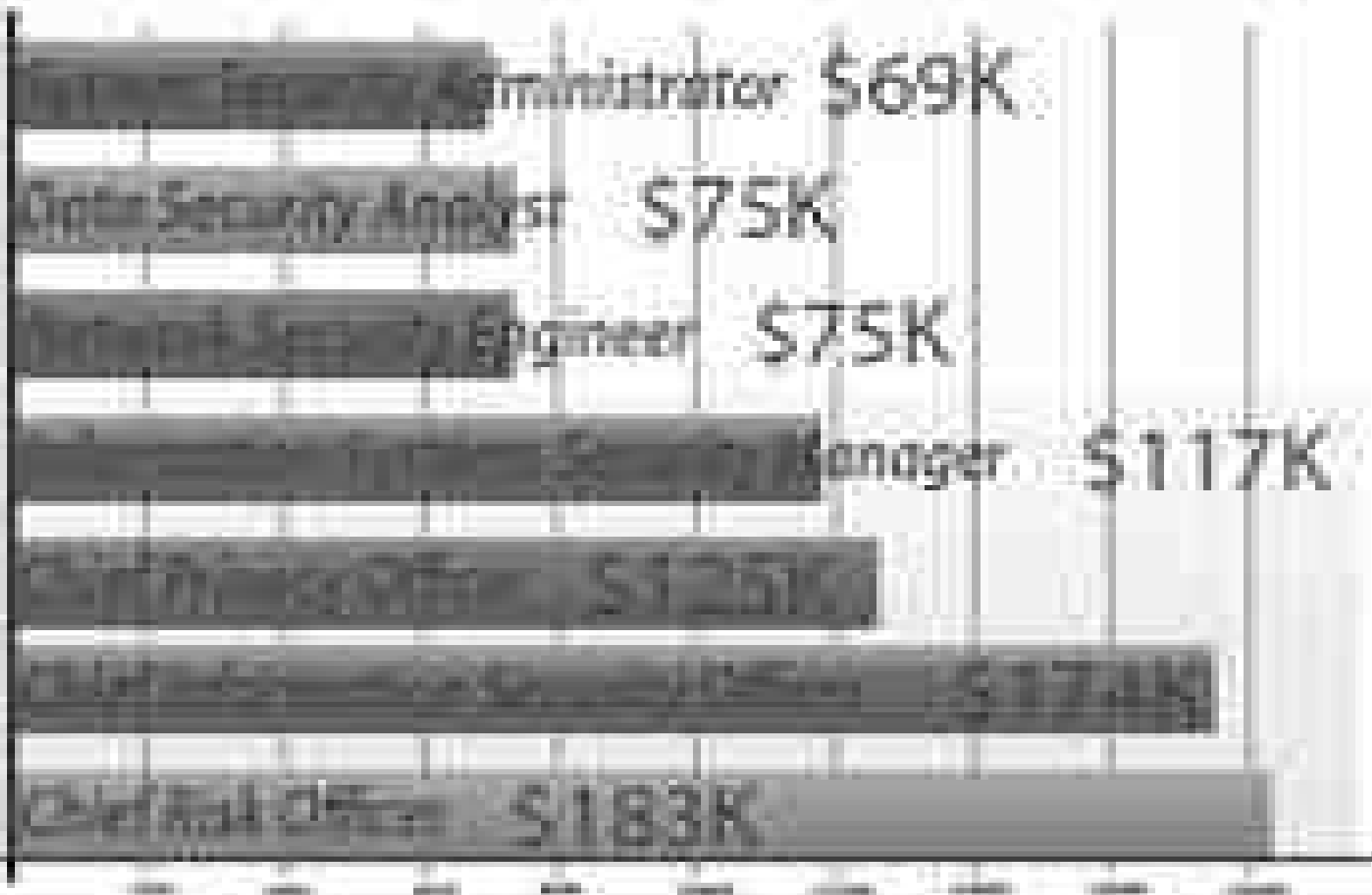
Here are the 10 highest-paying job titles in cybersecurity in the US

- Application security engineer
- Director of information security
- Senior security consultant
- Cloud engineer
- Software architect
- Penetration tester
- Risk manager
- Chief information officer
- Security engineer
- Information manager

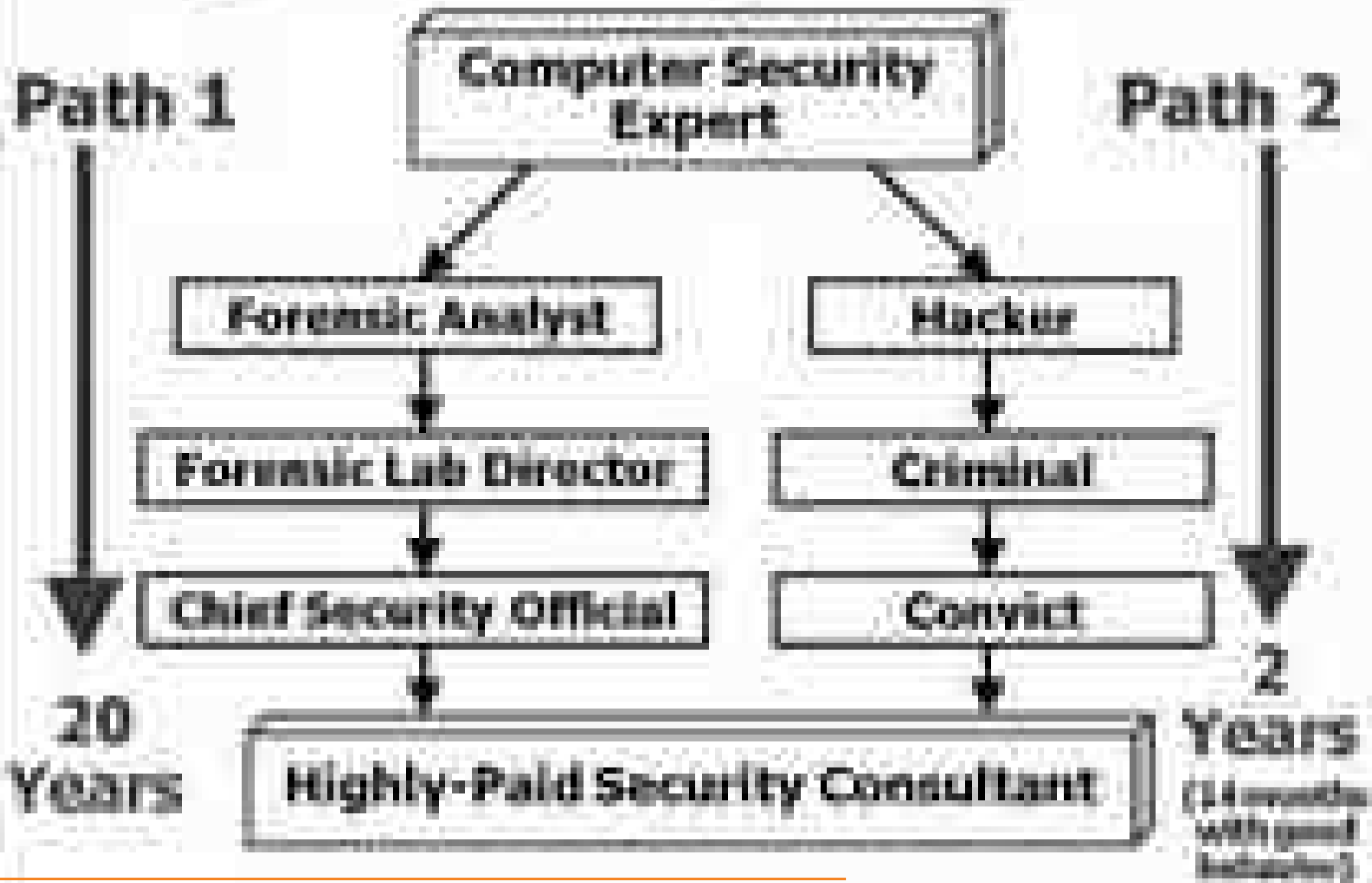


Hot IT Career Choices

MEDIAN ANNUAL WAGES



Computer Security Career Paths



Job Sectors

- Internships
- Education
 - Teaching / Training
 - Universities / Certs
- CERTs
- Private Organizations
- Government Institutes
- Financial Sector
- Law Enforcement & Military
- Freelancing
- Independent Consultant



Offensive Security – Jobs

<https://www.offensive-security.com/careers/>



Offensive Security – Jobs

<https://www.flexjobs.com/jobs/telecommuting-jobs-at-offensive-security-services>



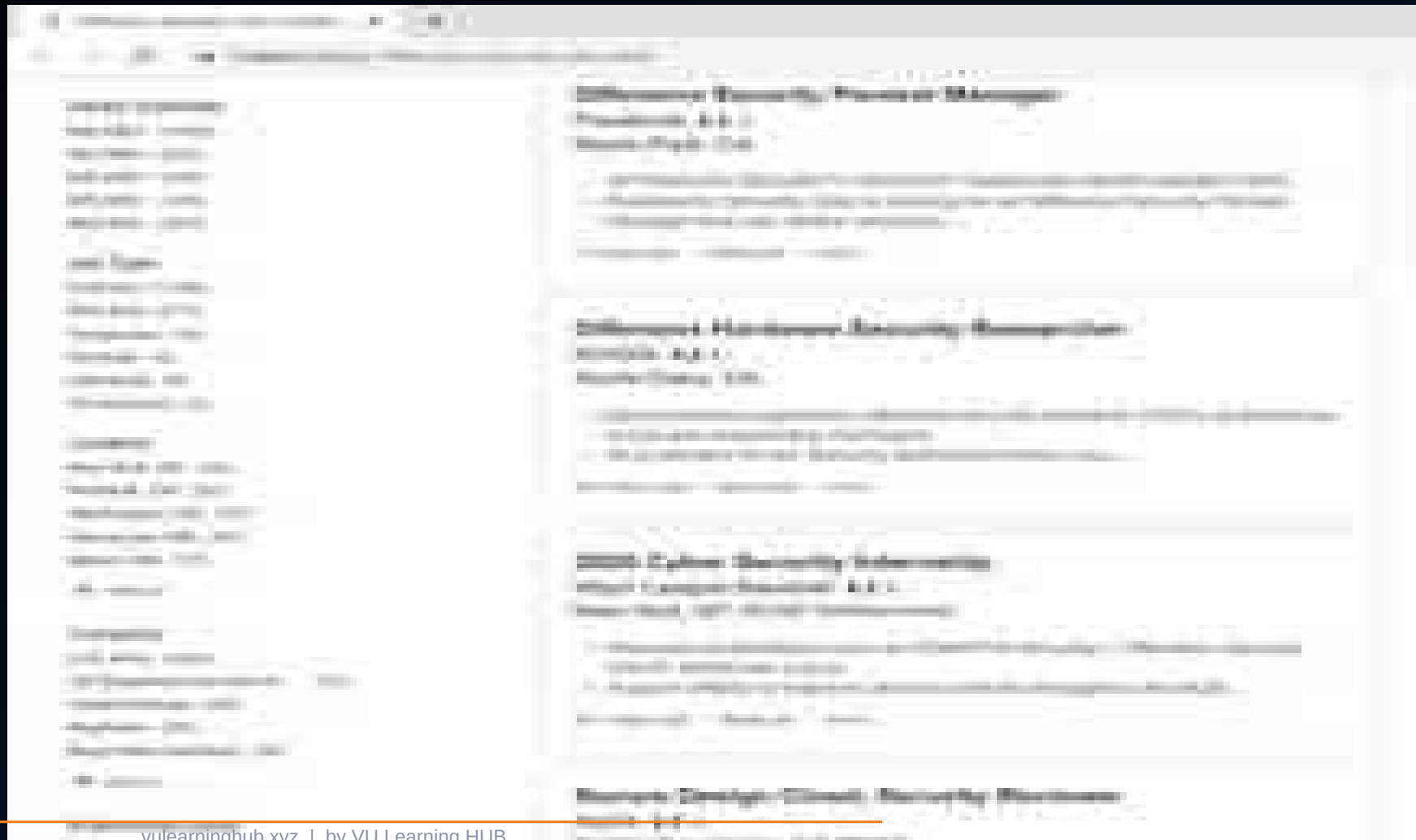
Offensive Security – Jobs

<https://www.flexjobs.com/jobs/telecommuting-jobs-at-offensive-security-services>



Offensive Security – Jobs

<https://www.indeed.com/q-Offensive-Security-jobs.html>



CYBRARY Career Opportunities

<https://www.cybrary.it/join-our-team/>



CYBRARY Career Opportunities

<https://www.cybrary.it/contribute/>



CYBRARY Career Opportunities

<https://www.cybrary.it/contribute/>



CYBRARY Instructor

<https://jobs.lever.co/cybrary/299bcf29-3b8a-46b9-8b33-4fd454f6f0de>



CYBRARY Instructor

<https://jobs.lever.co/cybrary/299bcf29-3b8a-46b9-8b33-4fd454f6f0de>



CYBRARY Instructor

<https://jobs.lever.co/cybrary/299bcf29-3b8a-46b9-8b33-4fd454f6f0de>



Fiverr Security Projects

<https://www.fiverr.com/gigs/cyber-security>

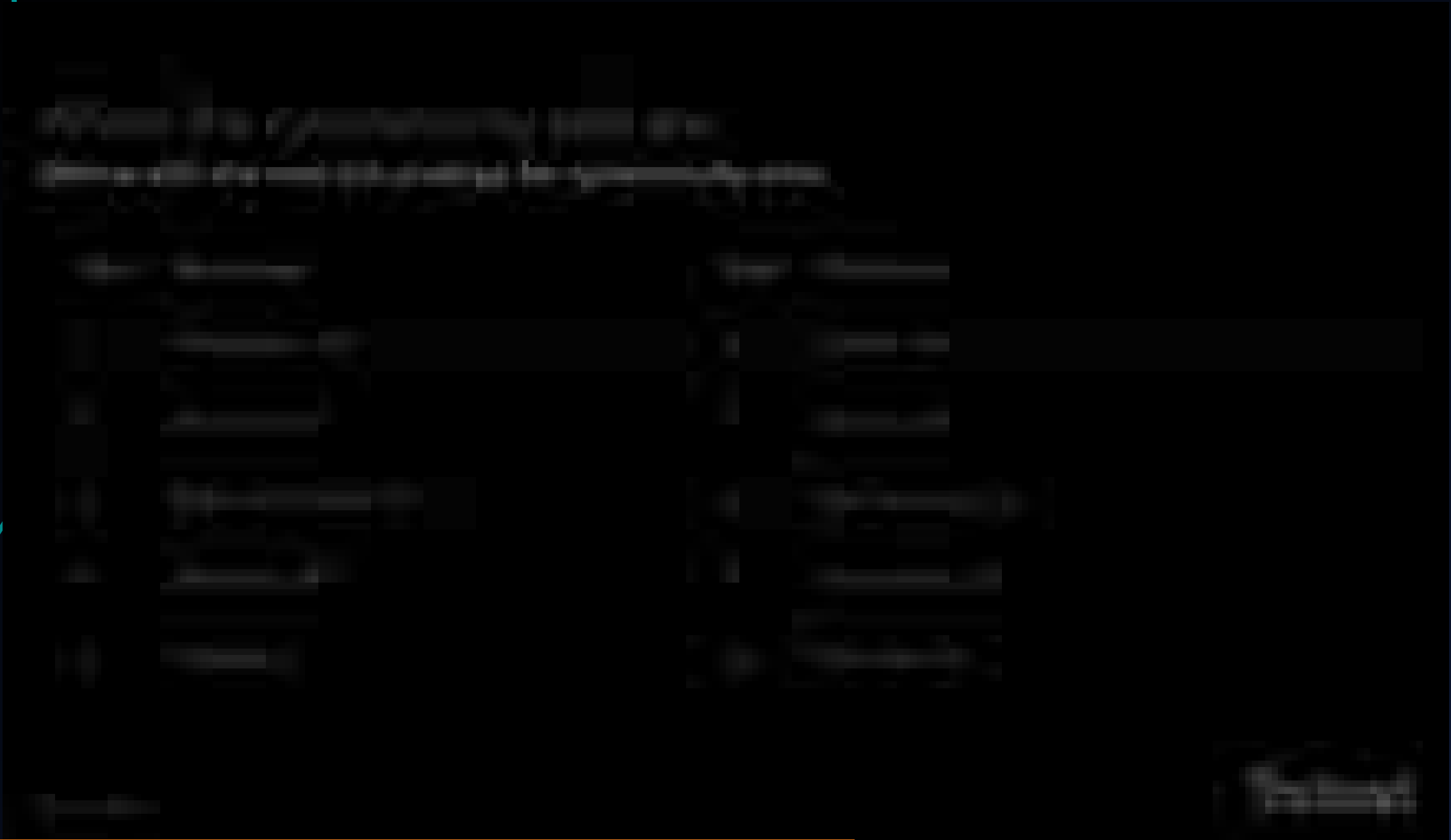


Online Job Application / Search Sources

- Job Websites / Online Career Portals
- Social Media
 - Facebook
 - LinkedIn
- Company Websites
- InfoSec Organization's career portals

Other Ways

- Search for company contact, submit CV's, turn up in-person.
- Word of mouth
 - Increase your social circle
- Attend InfoSec/IT related meetups, seminars, workshops & conferences.



Pre-requisites / Previous Knowledge

- Hardware
 - PC, Server, DC
 - Network Devices: Router, Switch, Load Balancer
- Operating Systems
 - Microsoft Windows, Apple Mac, Unix, Linux
- Networking
 - OSI, TCP/IP, Ports, Protocols, Devices
- Virtualization / Cloud Computing
- Programming / Scripting



ACCESS GRANTED

User Authentication and Access Control



Authentication

Accounting

Authorization

Authentication, Authorization, and Accounting (AAA)

Authentication



Confirms users
are who they say they are.

Authorization



Gives users permission
to access a resource.

Accounting



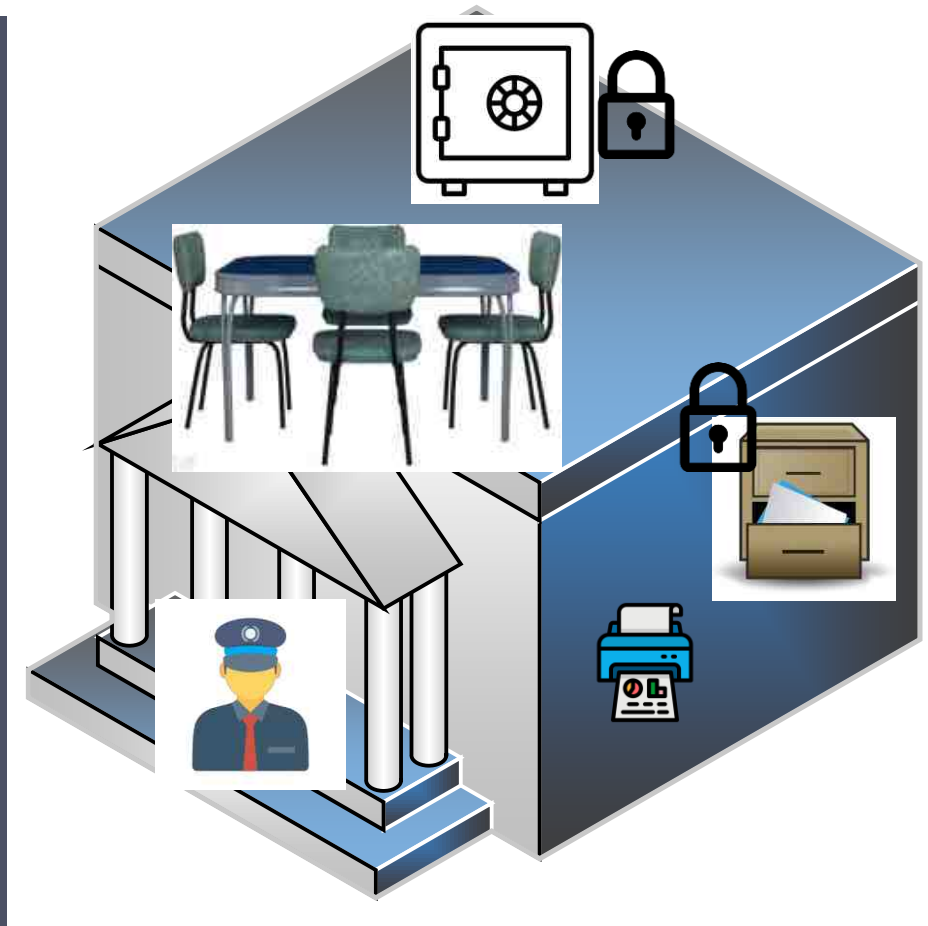
Measures the resources a user
consumes during access

Authentication, Authorization, and Accounting (AAA)

AAA is a term referred to the framework for

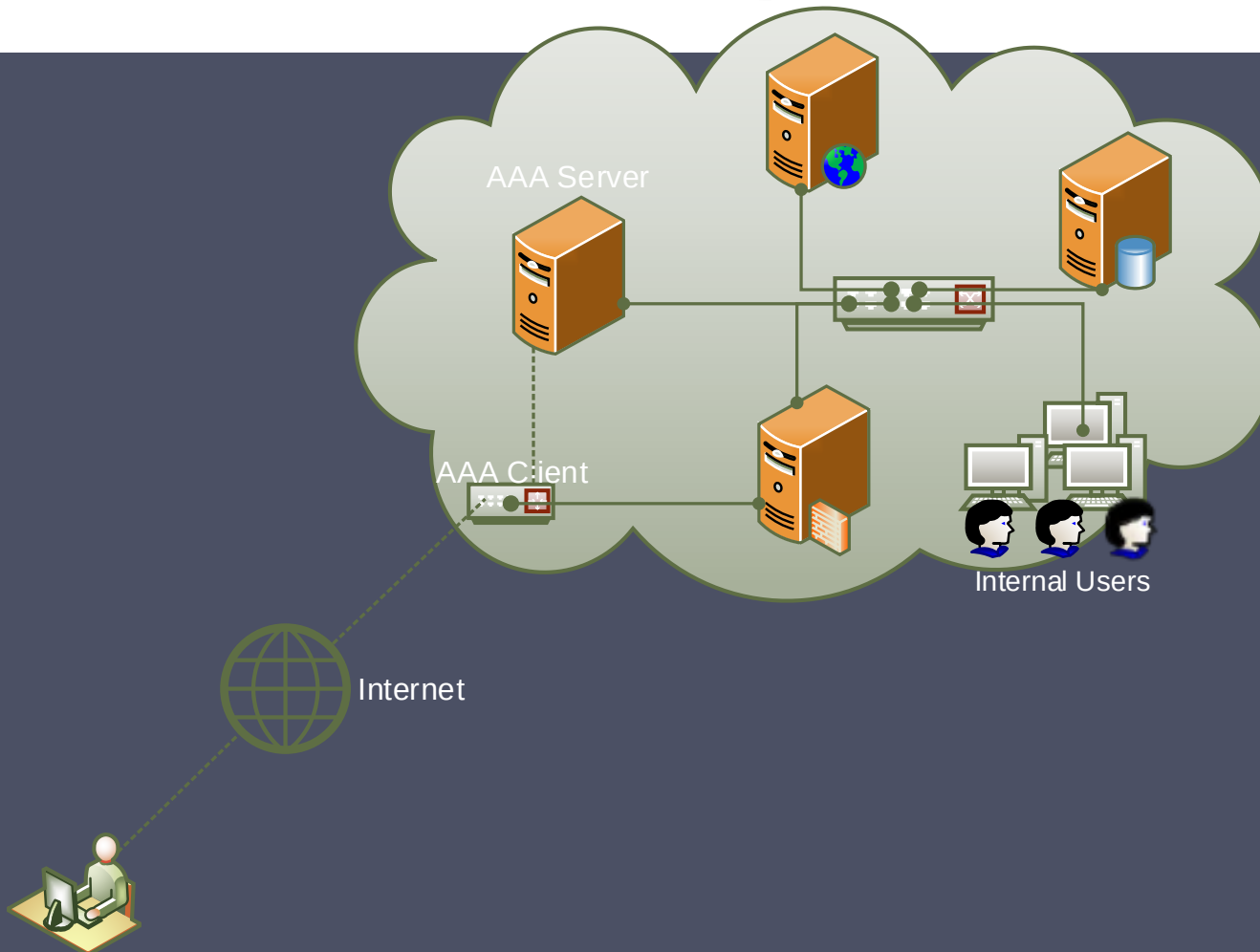
- Intelligently controlling access to the systems and resources
- Enforcing policies
- Auditing usage...

Illustration Physical World

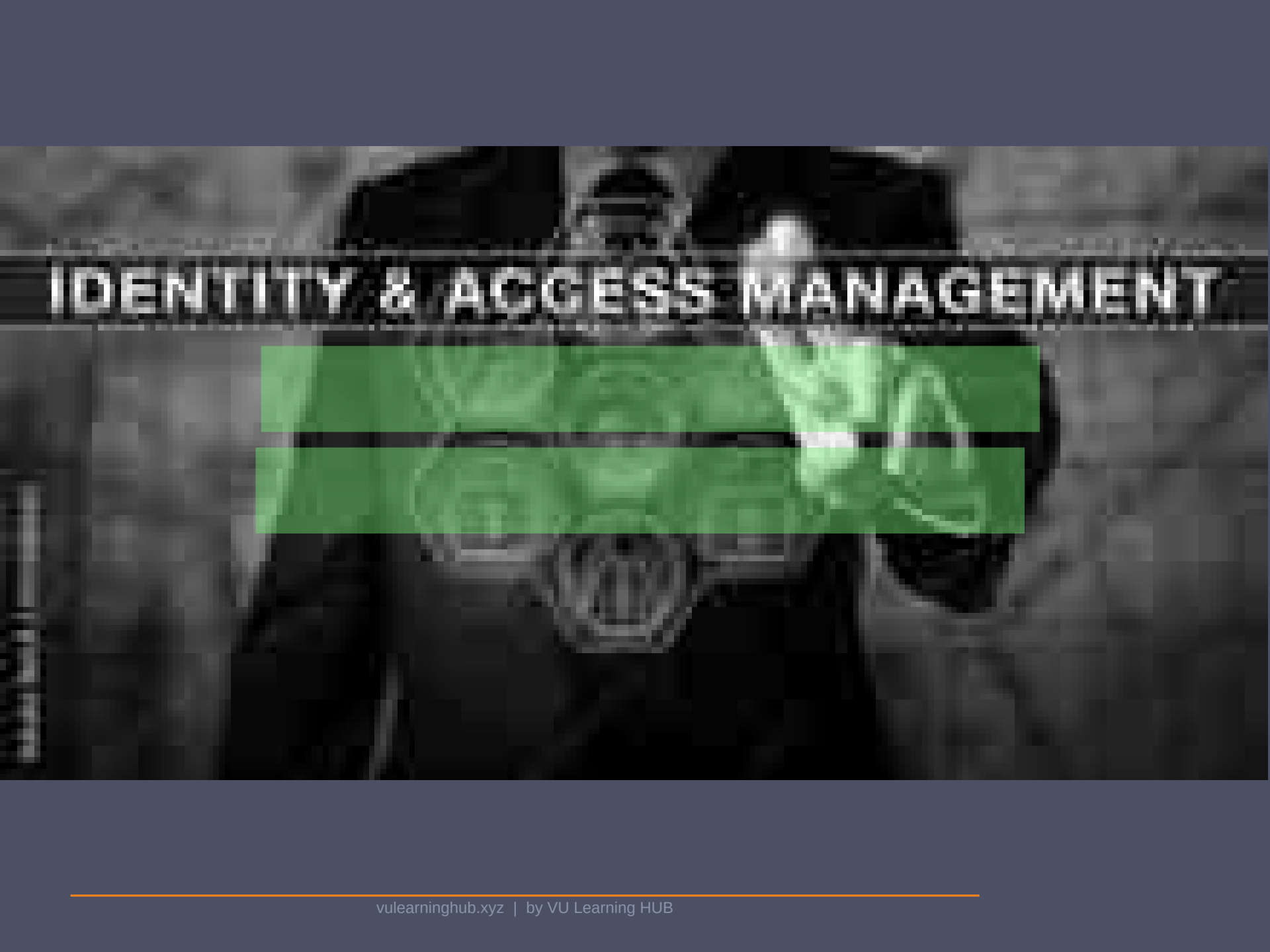


Illustration

Cyber World



IDENTITY & ACCESS MANAGEMENT



AAA vs. IAM

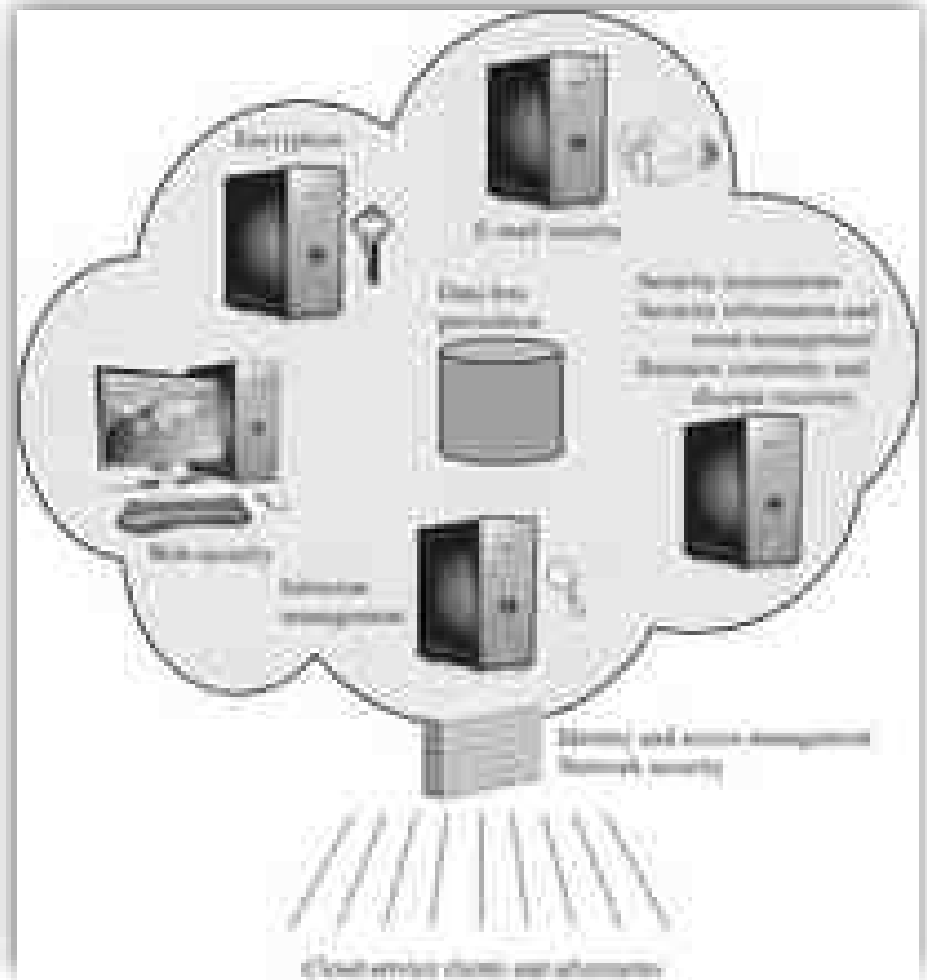
- AAA (Authentication, Authorization, and Accounting) is a general term that refers to a set of security processes that control access to computer resources.
- AAA servers are primarily used for network infrastructure.
- IAM (Identity and Access Management) is a specific set of technologies and policies used to manage access to an organization's IT resources.
- IAM systems are used for managing access to enterprise applications and data.

Identity and Access Management (IAM)

To ensure that the right people and things have

- ☞ the right access to
- ☞ the right resources
- ☞ at the right time.

IAM include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way.



Elements of Cloud Security as a Service

Identity Theft

- Consumers lost \$56 billion to identity fraud in America during 2021 [CNBC]
- The COVID-19 pandemic has created more points of vulnerability
- Identity theft scams - criminals interact directly with consumers to steal their information through methods such as robocalls and phishing emails.
- Three common red flags to watch
 - o Unsolicited calls or emails
 - o High-pressure tactics
 - o Outdated passwords



MEANS OF

USER AUTHENTICATION

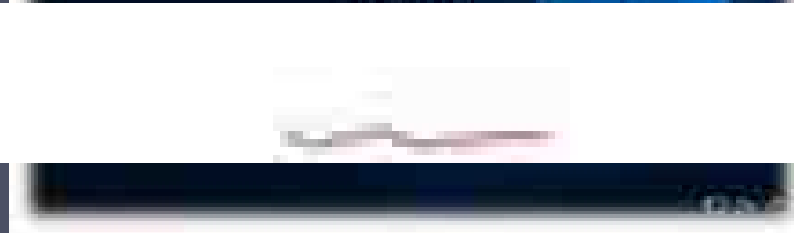
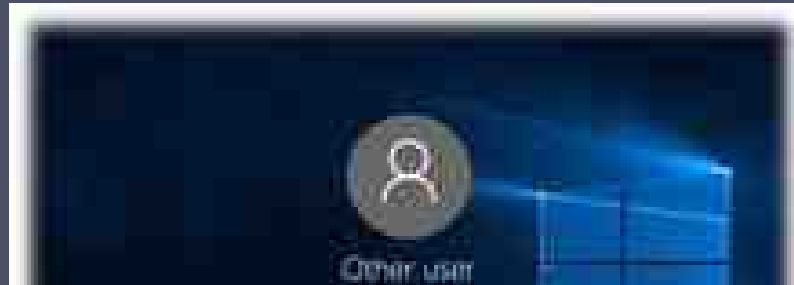
Recap



The four means of authenticating user identity are based on:

1/4
Something
the
individual
knows

- Passwords and prearranged questions



The four means of authenticating user identity are based on:

2/4

Something the individual possesses (token)

- Smartcard, electronic keycard, physical key



The four means of authenticating user identity are based on:

3/4

Something
the individual
is (static
biometrics)

- Fingerprint, retina, face



The four means of authenticating user identity are based on:

4/4

Something the individual does
(dynamic biometrics)

- Voice pattern, handwriting, typing rhythm



Summary

The four means of authenticating user identity are based on:

Something the individual knows

- Password, PIN, answers to prearranged questions

Something the individual possesses

- Smartcard, electronic keycard, physical key

Something the individual is (static biometrics)

- Fingerprint, retina, face

Something the individual does (dynamic biometrics)

- Voice pattern, handwriting, typing rhythm



PASSWORD

BASED

AUTHENTICATION

Password Based Authentication



• Widely used line of defense against intruders

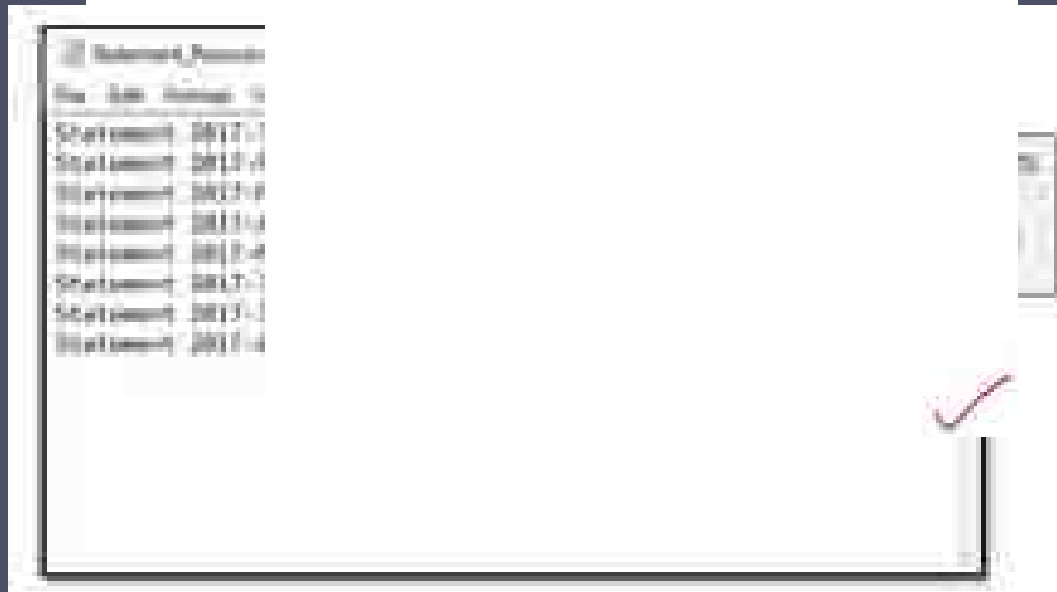
- User provides name/login and password
- System compares password with the one stored for that specified login

• The user ID:

- Determines that the user is authorized to access the system
- Determines the user's privileges
- Is used in discretionary access control

PASSWORD STORAGE

Plain Text



- Storing passwords in plaintext dangerous
 - o because it puts both the system and users at risk.

PASSWORD STORAGE

Hash Function

Demo



SIGN

Email

Passw



5

3



Created by

Business
analytics

1

2

3

4

1

1

Validate a password



Password Vulnerabilities

Password Hacking and Cracking

- Password hacking and cracking are terms that are often used interchangeably, but there is a subtle difference between the two.
- Password Hacking
 - o refers to gaining unauthorized access to a system
 - o Usually, original password is changed
- Password Cracking
 - o to the process of attempting to recover a password
 - o Usually, original password is NOT changed

Password Vulnerabilities

Exploiting user mistakes

- Users more likely use default passwords, write or share the passwords through social engineering tactics

Exploiting multiple password use

- Different network devices share the same or a similar password for a given user

Electronic monitoring

- Password communicated across a network in plaintext format

Brute force Attack

- Try all possible passwords

Offline dictionary attack

- Compares the password hashes against hashes of commonly used passwords

Rainbow table attacks

- Pre-compute tables of hash values of ALL passwords*

Offline Dictionary Attack

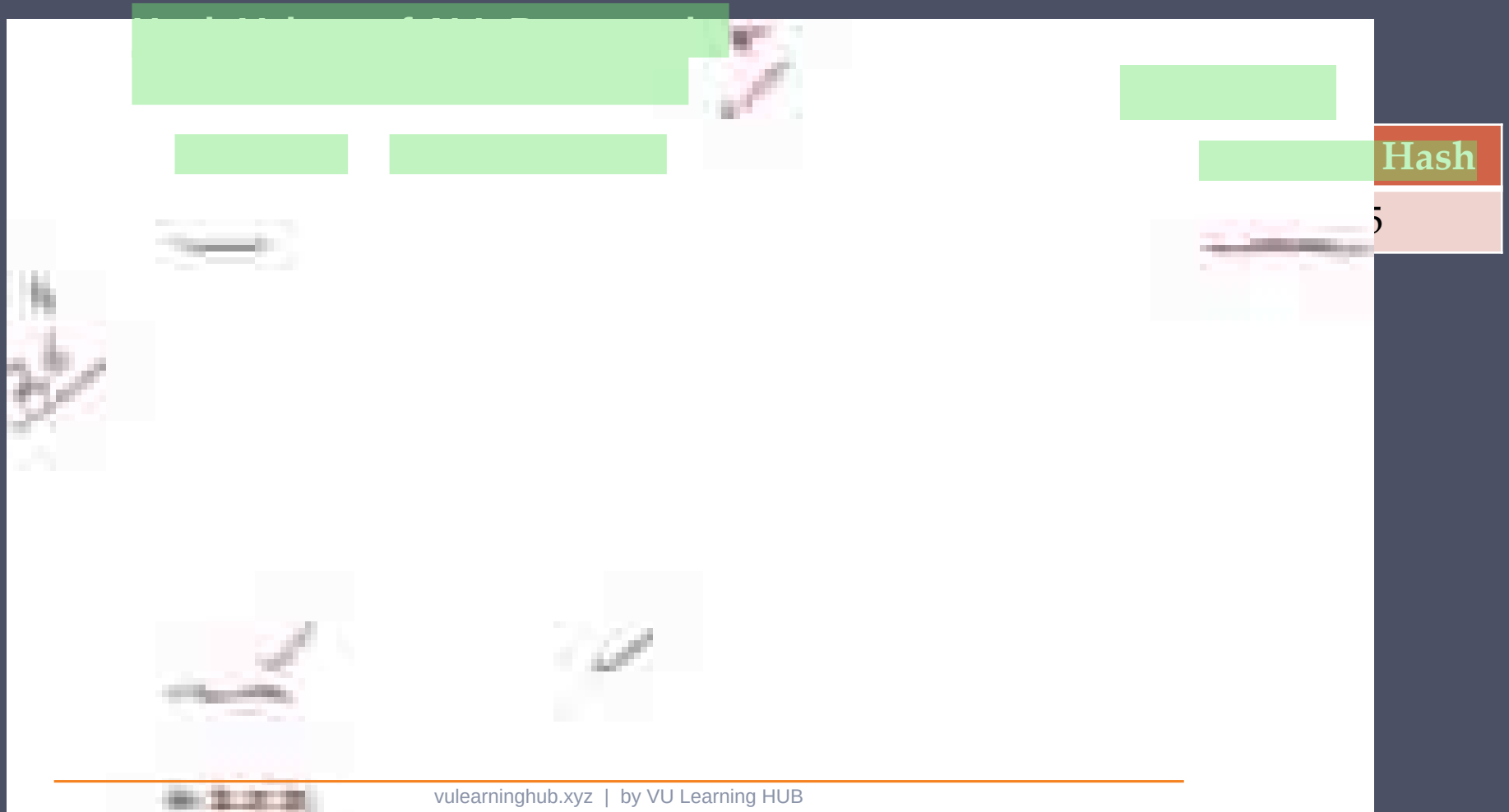
Dictionary of Commonly Used Passwords

Password	Password Hash
...	...

Target User

UID	Password Hash
	s

Rainbow Table Attack





Securing Passwords

Modern Approaches

- Complex password policy
 - o Forcing users to pick stronger passwords
- However, password-cracking techniques have also improved
 - o The processing capacity available for password cracking has increased dramatically
 - o The use of sophisticated algorithms to generate potential passwords
 - o Studying examples and structures of actual passwords in use

Password File Access Control

One way to block offline guessing attacks by denying access to encrypted passwords (password hashes)

Make
available
only to
privileged
users

Shadow
password
file

vulnerabilities

Weakness
in the OS
that allows
access to the
file

Accident
with
permissions
making it
readable

Users with
same
password
on other
systems

Access from
backup
media

Sniff
passwords
in network
traffic

Password Selection Strategies

User education

Users can be told the importance of using hard to guess passwords and can be provided with guidelines for selecting strong passwords



Computer generated passwords

Users have trouble remembering them



Reactive password checking

System periodically runs its own password cracker to find guessable passwords



Complex password policy

User is allowed to select their own password, however the system checks to see if the password is allowable, and if not, rejects it

Goal is to eliminate guessable passwords while allowing the user to select a password that is memorable



Memory Cards and Smart Cards

Recall

The four means of authenticating user identity are based on:

Something the individual knows

- Password, PIN, answers to prearranged questions

Something the individual possesses (token)

- Smartcard, electronic keycard, physical key

Something the individual is (static biometrics)

- Fingerprint, retina, face

Something the individual does (dynamic biometrics)

- Voice pattern, handwriting, typing rhythm

Memory Cards

- Can store but do not process data
- The most common is the magnetic stripe card e.g. ATM
- Can include an internal electronic memory
- Can be used alone for physical access
 - Hotel room
 - ATM
- Provides significantly greater security when combined with a password or PIN
- Drawbacks of memory cards include:
 - Requires a special reader
 - Loss/theft of token/memory card
 - User dissatisfaction



Smart Tokens



<https://upload.wikimedia.org/wikipedia/commons/d/db/SecurityTokens.CryptoCard.agr.jpg>

Physical characteristics:

- Include an embedded microprocessor
- A smart token may look like a bank card
- Can look like calculators, keys, small portable objects

User interface:

- Manual interfaces include a keypad and display for human/token interaction

Electronic interface

- A smart card or other token requires an electronic interface to communicate with a compatible reader/writer
- Contact and contactless interfaces

Authentication protocol:

- Classified into three categories:

- Static
- Dynamic password generator
- Challenge-response

Smart Cards

- Most important category of smart token

- Has the appearance of a credit card
- Has an electronic interface
- May use any of the smart token protocols

- Contains

- An entire microprocessor

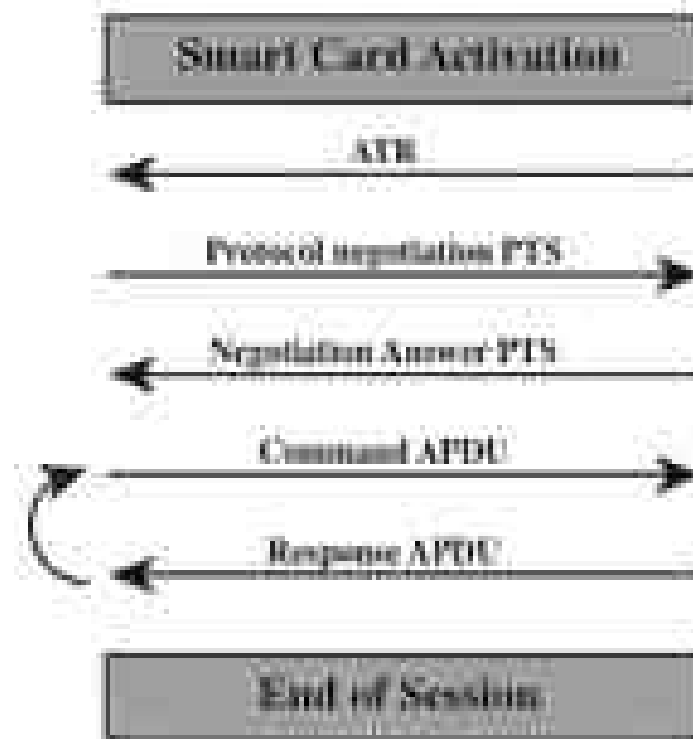
- Processor
- Memory
- I/O ports

- Typically include three types of memory

- Read-only memory (ROM)
 - Stores data that does not change during the card's life
- Electrically erasable programmable ROM (EEPROM)
 - Holds application data and programs
- Random access memory (RAM)
 - Holds temporary data generated when applications are executed



Interaction Between Reader and Smart Card



APDU = application protocol data unit
ATR = Answer to reset
PTS = Protocol type selection



Biometric Authentication

Recall

The four means of authenticating user identity are based on:

Something the individual knows

- Password, PIN, answers to prearranged questions

Something the individual possesses (token)

- Smartcard, electronic keycard, physical key

Something the individual is (static biometrics)

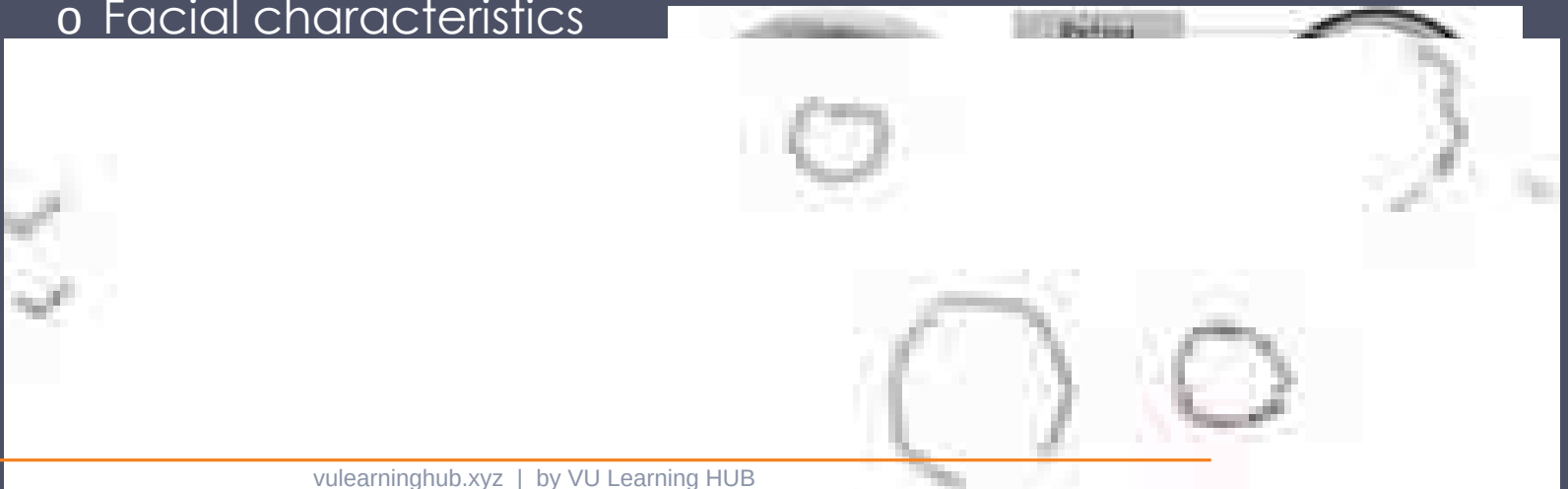
- Fingerprint, retina, face

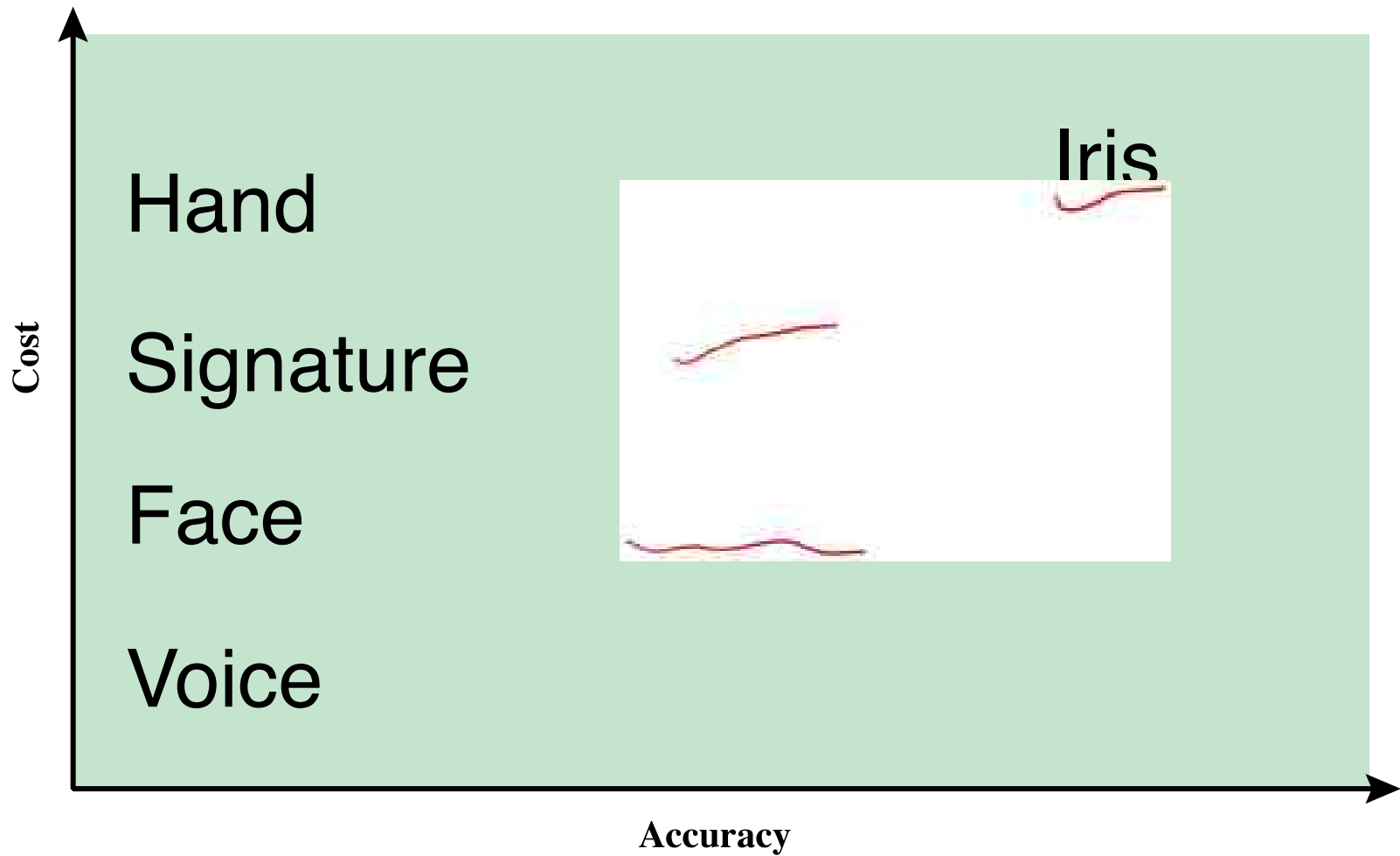
Something the individual does (dynamic biometrics)

- Voice pattern, handwriting, typing rhythm

Biometric Authentication

- Attempts to authenticate an individual based on unique physical characteristics
- Based on pattern recognition
- This is technically complex and expensive when compared to passwords and tokens
- Physical characteristics used include:
 - o Facial characteristics





Name (PIN)

U

I

U

U

Biometric Authentication

Pros

- Difficult to forge
- Convenience
- More secure and non-transferable*

Cons

- Costly
- Complex
- False Acceptance Rate (FAR) and False Rejection Rate (FRR)
- Rigid
- Attacker can fool the system



Multi factor

Authentication

Recall

The four means of authenticating user identity are based on:

Something
you
know

- Password, PIN, answers to prearranged questions

Something
you
have

- Smartcard, electronic keycard, physical key

Something
you
are

- Fingerprint, retina, face

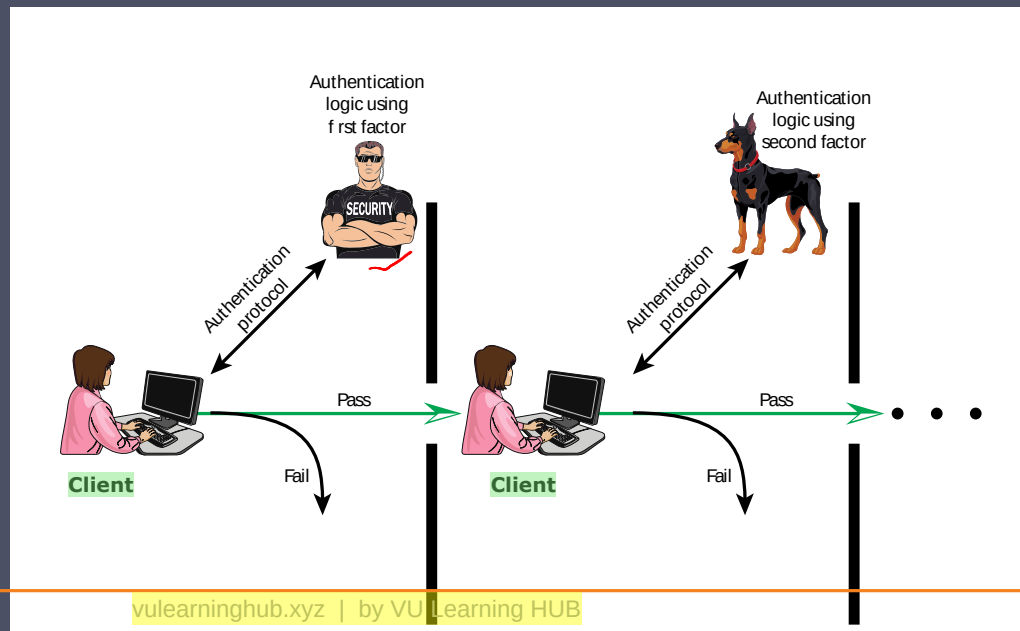
Something
the
individual
does

- Voice pattern, handwriting, typing rhythm

Multifactor Authentication

compromised passwords, according to Verizon's 2019 Data Breach Investigations Report

- Multi-factor authentication (MFA) is the practice of requiring at least one additional form of user authentication—besides a password—when accessing a remote network.



Mul

factor Authentication

- **Most Common Method for MFA**

- o When logging in to a system remotely, the user first enters the regular password and is then prompted to enter the one-time password or passcode.
- o This is also commonly known as 2FA



SFA vs. 2FA vs. MFA

- Simplest authentication method.
- Matches credentials with person on the other end of the line.
- The most common example is a password (credentials) and a username.

It uses a combination of the following factors:
• Something you know,
• Something you have,
• Something you are

It is a combination of

Eavesdropping

Adversary attempts to learn the password by some sort of attack that involves the physical proximity of user and adversary

Denial-of-Service

Attempts to disable a user authentication service by flooding the service with numerous authentication attempts

Host Attacks

Directed at the user file at the host where passwords, token passcodes, or biometric templates are stored

AUTHENTICATION SECURITY ISSUES

Trojan Horse

An application or physical device masquerades as an authentic application or device for the purpose of capturing a user password, passcode, or biometric

Client Attacks

Adversary attempts to achieve user authentication without access to the remote host or the intervening communications path

Replay

Adversary repeats a previously captured user response



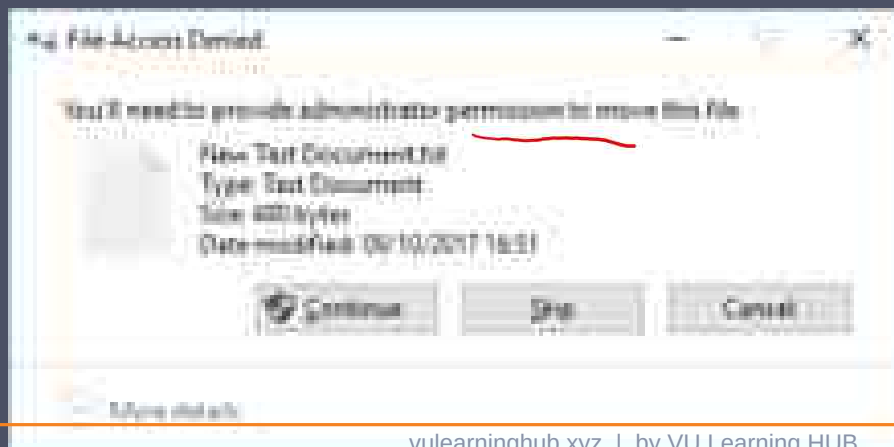
Access Control

Recap



Access Control

"The process of granting or denying specific requests for (1) obtain and use information and related information processing services and (2) enter specific physical facilities"





Subjects, Objects and Access Rights





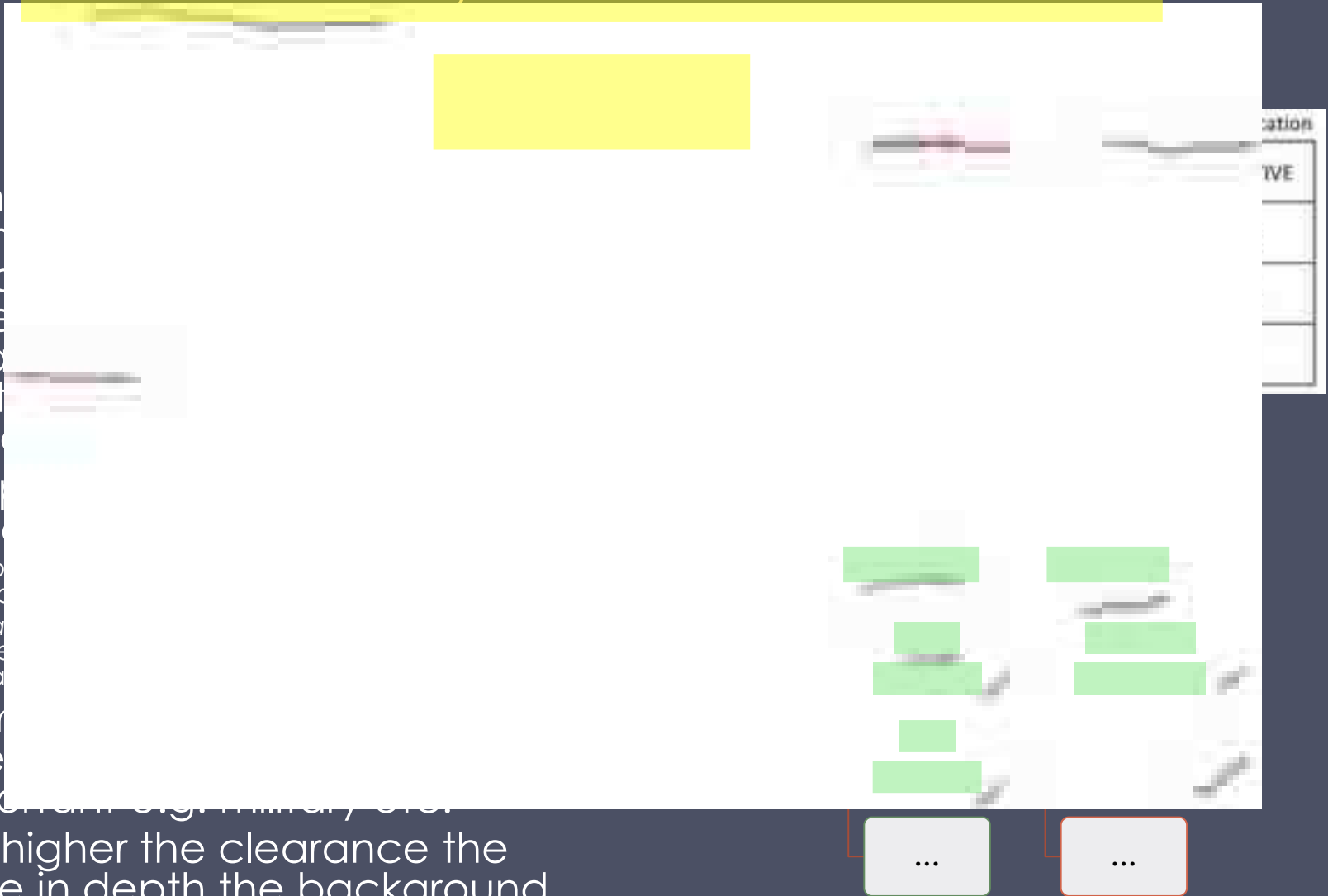
Access Control Policies

Access Control Policies

- Mandatory access control (MAC)
- Discretionary access control (DAC)
- Role-based access control (RBAC)
- Attribute-based access control (ABAC)

Mandatory Access Control

- Confidentiality
compliance
indications
system
clearance
entirely
certified
- This process
becomes
 - performance
for
 - additional
recovery
and
- Confidentiality
when
important information, etc.
- The higher the clearance the
more in depth the background
checks should be.



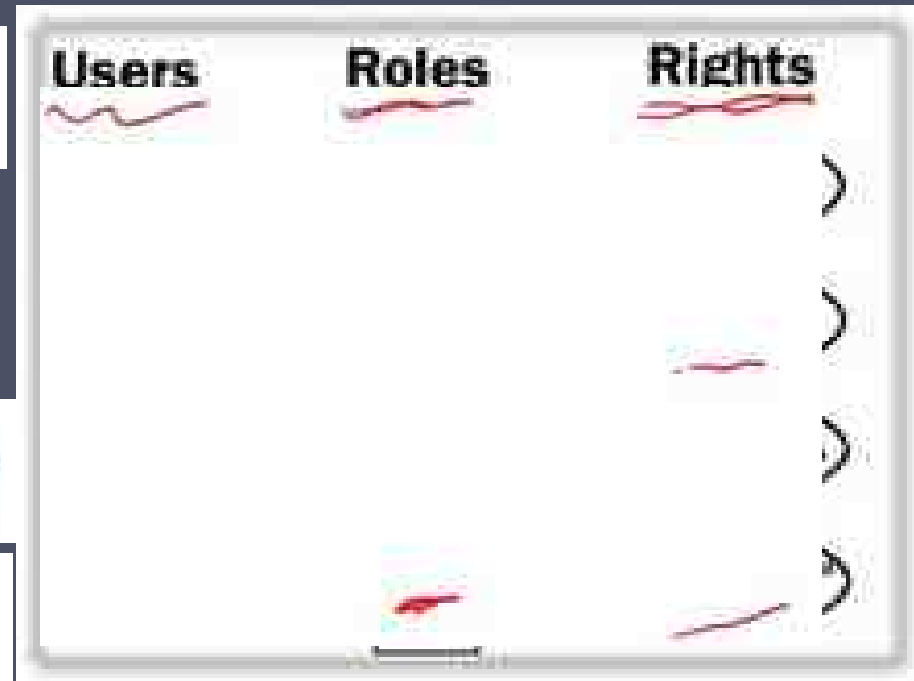
Discretionary Access Control

Useful for small size organizations...

Access Matrix

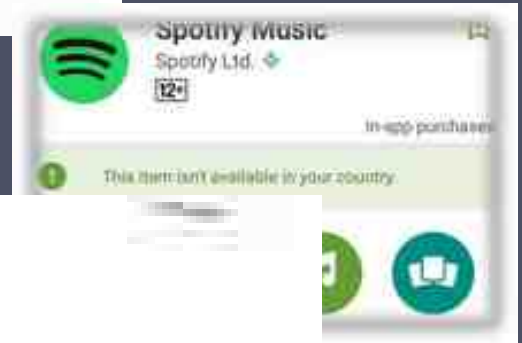
Role-based Access Control (RBAC)

- DAC is not feasible for large size organizations...
 - Something better and easy to manage is needed
- Among such solutions is **RBAC**
- Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.



Attribute-based Access Control (ABAC)

- Controls access based on attributes of the user, the resource to be accessed and current environmental conditions and policies.



Summary

- Mandatory access control (MAC)

- o Controls access based on the classification of the data and the classification of the user, stating what accesses are allowed to users in given roles

- Discretionary access control (DAC)

- o Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do

- Attribute-based access control (ABAC)

- o Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions



Cryptography

vulearninghub.xyz | by VU Learning HUB

<https://www.fortinet.com/resources/cyberglossary/what-is-cryptography>

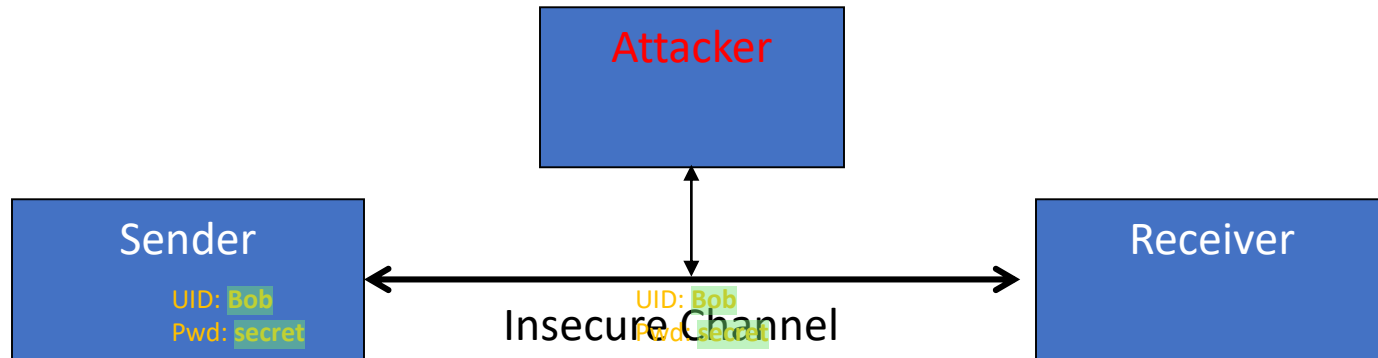
Cryptography

What is cryptography?

- **Cryptography**
 - o The art of **secret writing**
 - o Cryptography is the making
- **Cryptanalysis**
 - o Cryptanalysis is the breaking

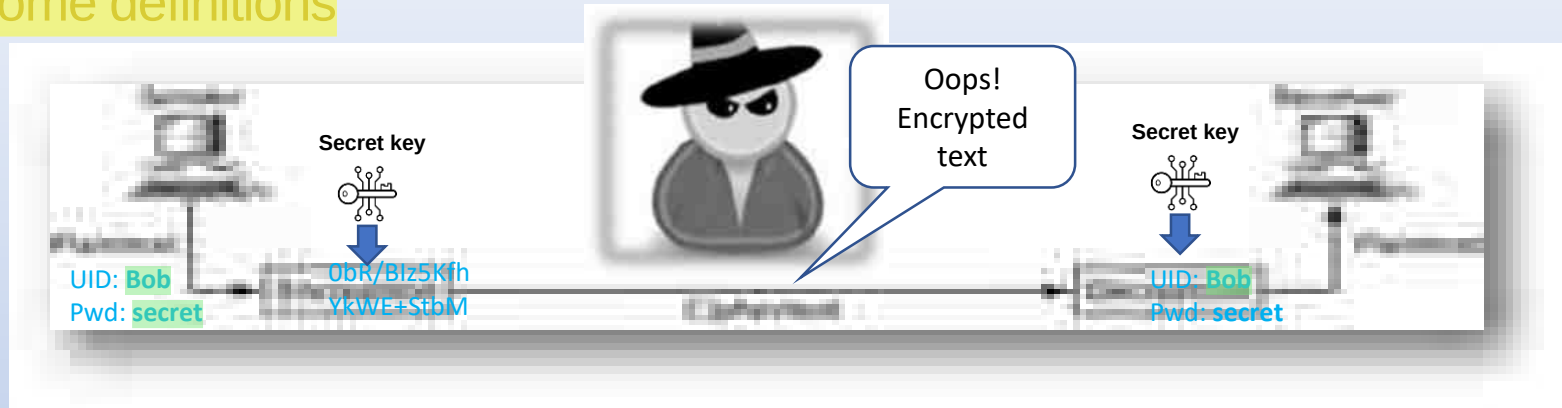
- **Why Cryptography?**

- Cryptography aims to provide secure communications in the presence of an **adversary/attacker**.



Cryptography

Some definitions



Plaintext: This is the original message or data that is to be secured.

Encryption algorithm: This is the mechanism of securing the message and data. The encryption algorithm performs various substitutions and transformations on the plaintext.

Secret key: The secret key is also input to the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.

Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.

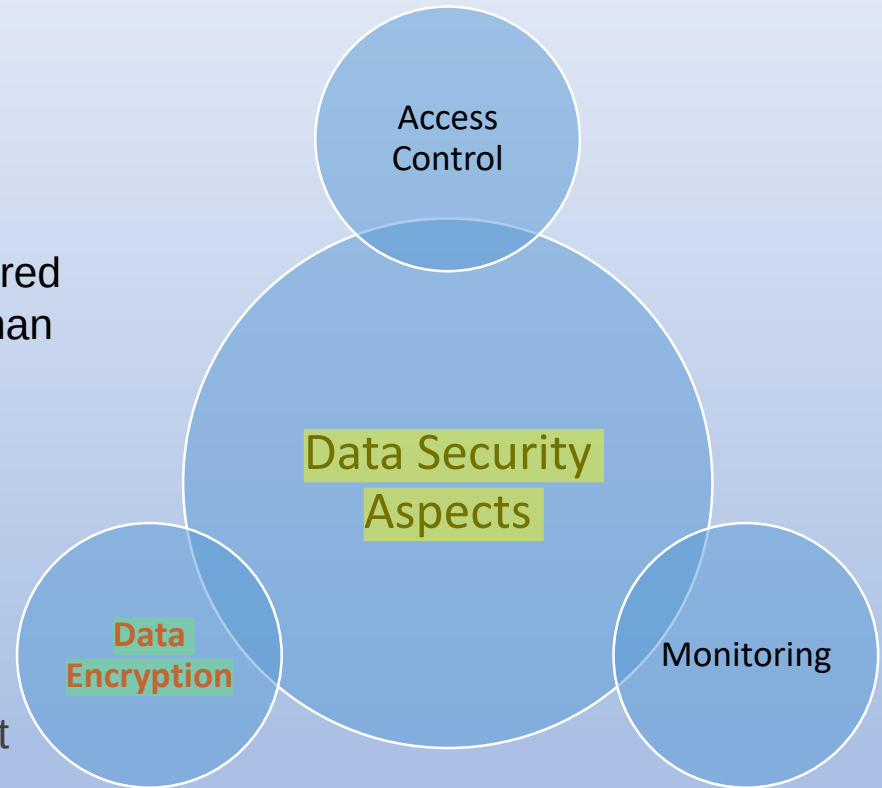
Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the same secret key and produces the original plaintext.

Data Security Aspects

Data Security

Data Security Aspects

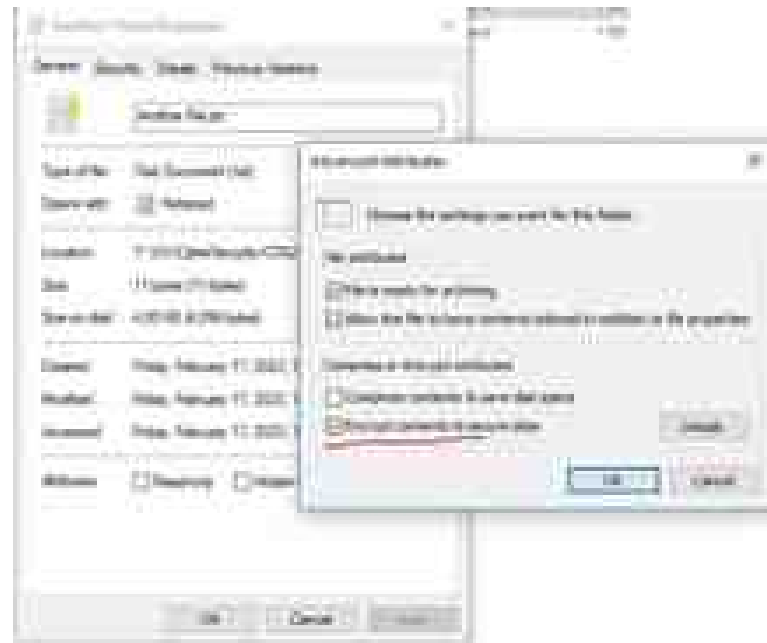
- **Access Control** who can access the data
- **Monitoring** who is using the data and how
- **Data Encryption** strong encryption is required to transform the data from plaintext (or human readable format) to cipher text
- **Stages of Data**
 - Data at rest
 - Data in transit
 - Data in use
- **Cryptographic algorithms** helps to protect the data in all stages from un-authorized access and alteration



Data Security

Is it good to encrypt your files always?

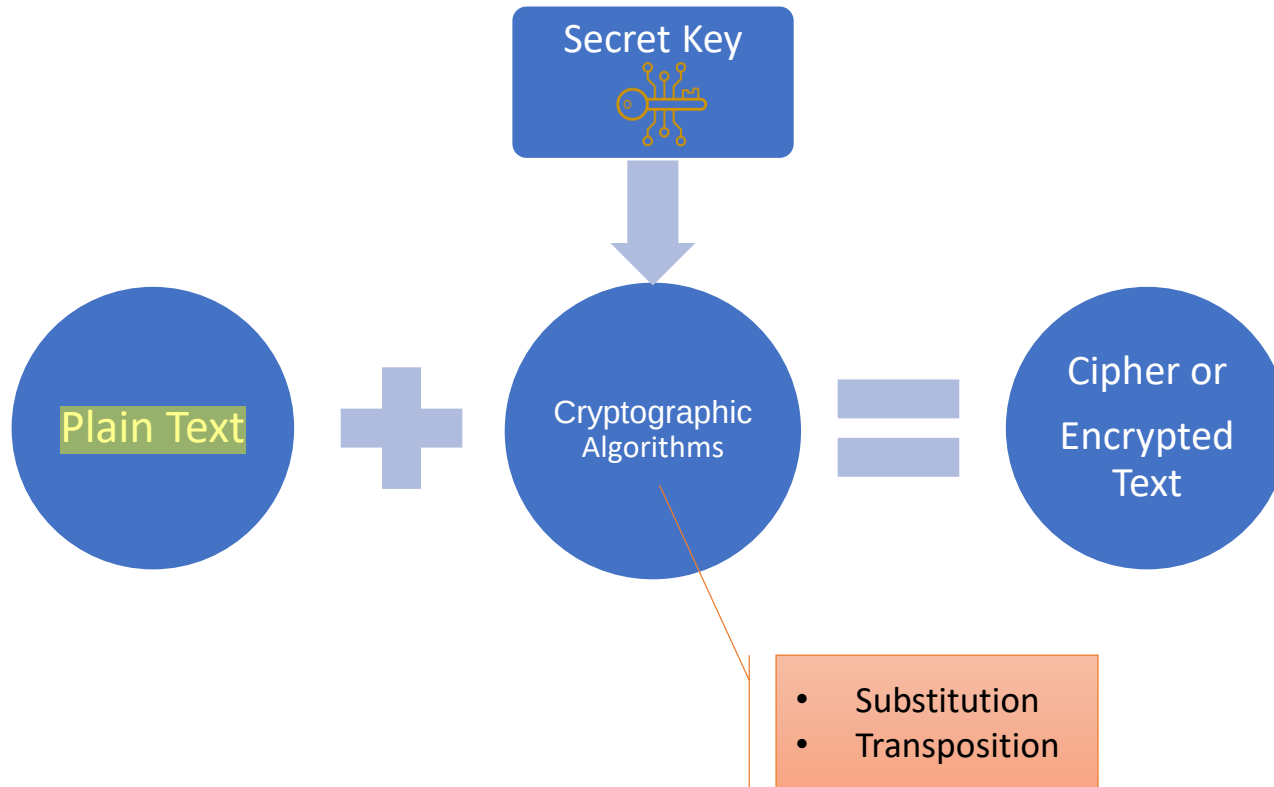
- Encrypt when its needed...
- Be careful with Keys when encrypted...
- Windows files security
 - Access rights
 - Encryption



Cryptographic Algorithms and Kerchoff's Principle

Cryptographic Algorithms

also referred as Ciphers or Encryption Algorithms

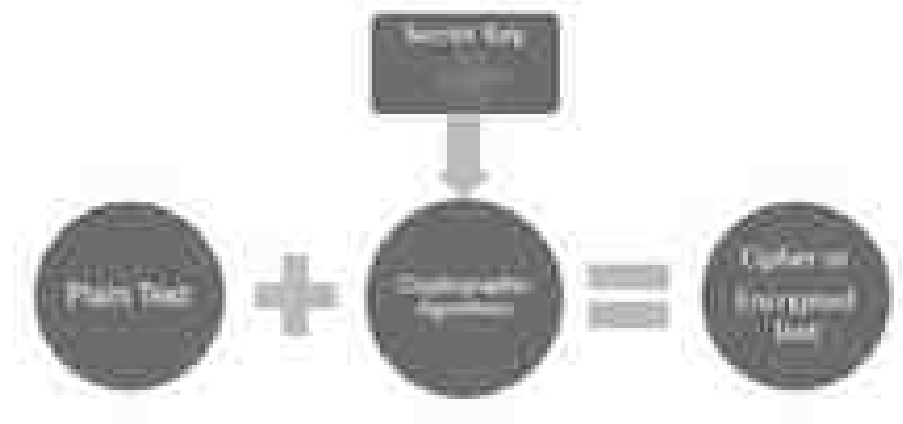


Feistel network consisting multiple rounds of processing of the plaintext, each round consisting of a “substitution” step followed by a permutation step.

Kerchoff's Principle

Kerckhoffs's principle of cryptography was stated by Dutch-born cryptographer Auguste Kerckhoffs in the 19th century.

- Kerckhoff's principle is the concept that a Cryptographic system should be designed to be secure, even if all its details, except for the key, are publicly known.



- In other words,
 - Secrecy of the cryptographic system should rely on the secret keys
 - No need to hide the procedure or algorithm for encryption
 - Rather, its better if procedure or algorithm for encryption are made public as this will help in identification and removing the flaws/loopholes

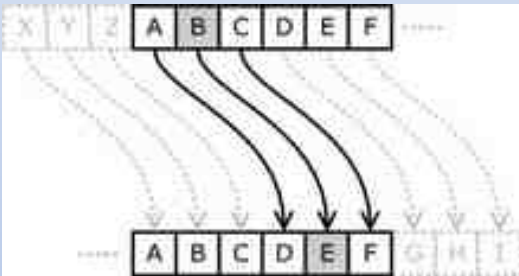
Classical Ciphers

The Caesar Cipher

Classical Ciphers

The Caesar Cipher

The Caesar cipher is one of the earliest and simplest methods of encryption technique and is based on substitution and involves shifting each letter of the plaintext message by a certain number of letters,



- **Caesars cipher**

- o Replace every 'A' in the message with a 'E'
- o Replace every 'B' in the message with a 'F'
- o Replace every 'C' in the message with a 'G', etc.

- **Considerations**

- o Algorithms are public (Kerchoff's Principle)
- o Encrypt/decrypt depends on a key
- o The only secret is the key
- o For Caesars cipher, key is ***n***, since shift forward ***n*** to encrypt, shift backward ***n*** to decrypt
- o Encryption: $C_i = (P_i + n) \bmod 26$
- o Decryption: $P_i = (C_i - n) \bmod 26$

Text : **ATTACKATONCE**

Shift: **4**

Cipher: **EXXEGOEXSRGI**

Caesar Cipher

Cryptanalysis of Caesar Cipher – Brute force

- Ciphertext = “GRR MGAR OY JOBOJKJ OT ZNXKK VGXZY”
- Perform decryption with each possible key:
- Plaintext with $n=1$
 - FQQ LFZQ NX INANIJI NS YMWJJ UFWYX
- Plaintext with $n=2$
 - EPP KEYP MW HMZMHIH MR XLVII TEVXW
- Plaintext with $n=3$
 - DOO JDXO LV GLYLGHG LQ WKUHH SDUWV
- Plaintext with $n=4$
 - CNN ICWN KU FKXKFGF KP VJTGG RCTVU
- Plaintext with $n=5$
 - BMM HBVM JT EJWJEFE JO UISFF QBSUT
- Plaintext with $n=6$
 - ALL GAUL IS DIVIDED IN THREE PARTS

Classical Ciphers

Vigenere Cipher

Classical Ciphers

Vigenere Cipher

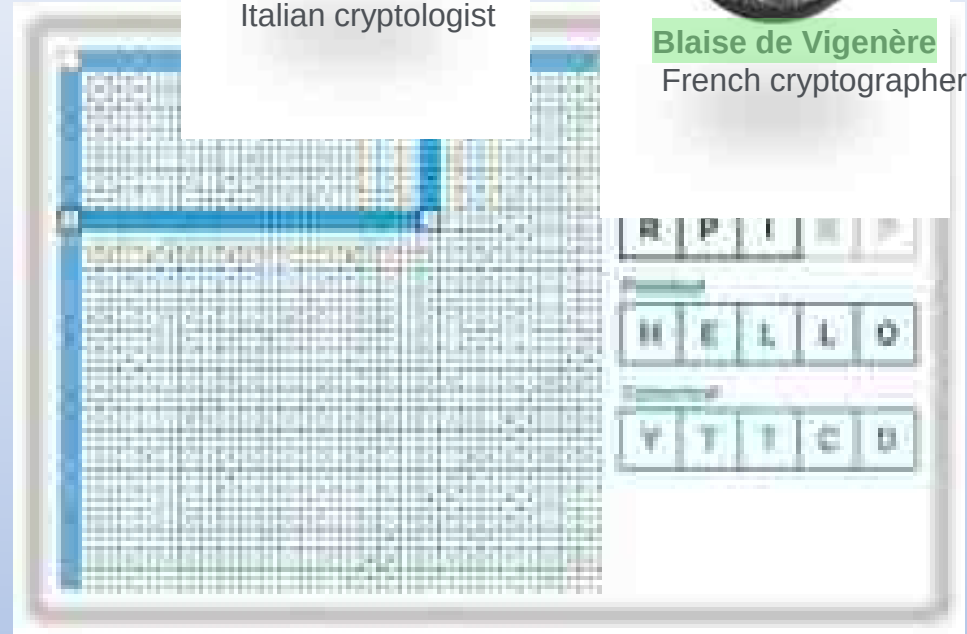


Giovan Battista
Italian cryptologist



Blaise de Vigenère
French cryptographer

- Developed in 1553.
- It is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword.
- Its based on polyalphabetic substitution
- **Key**: A word W of Length M .
- **Plain text** P of length N .
- Repeat the Key until it matches the length of the plain text.
- For each letter P_j of the plain text, apply a Caesar Cipher of length W_j

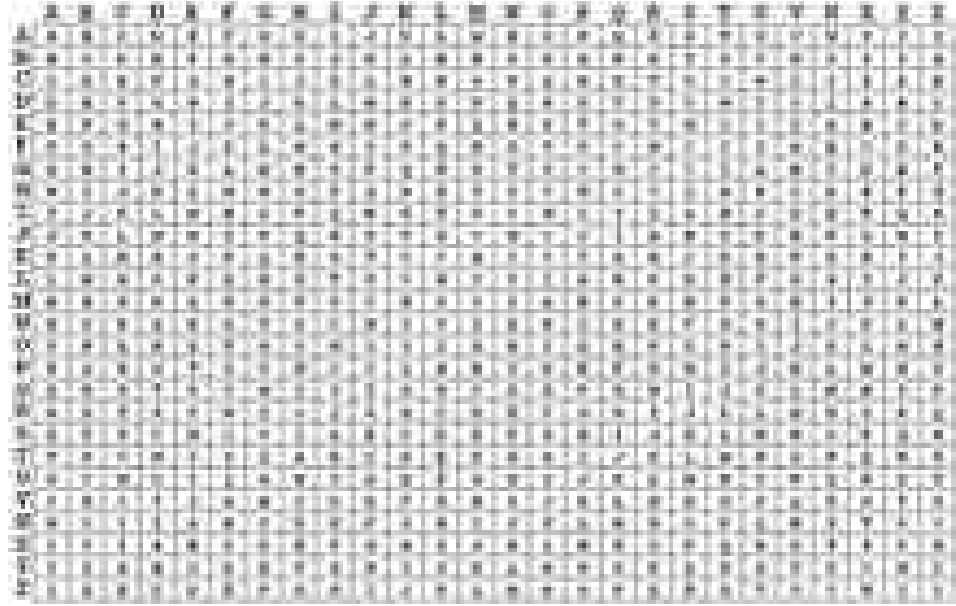


Example

- Key: **RPI**
- Plain Text: HELLO
- Expanded key: RPIRP
- Cipher Text: YTTCD

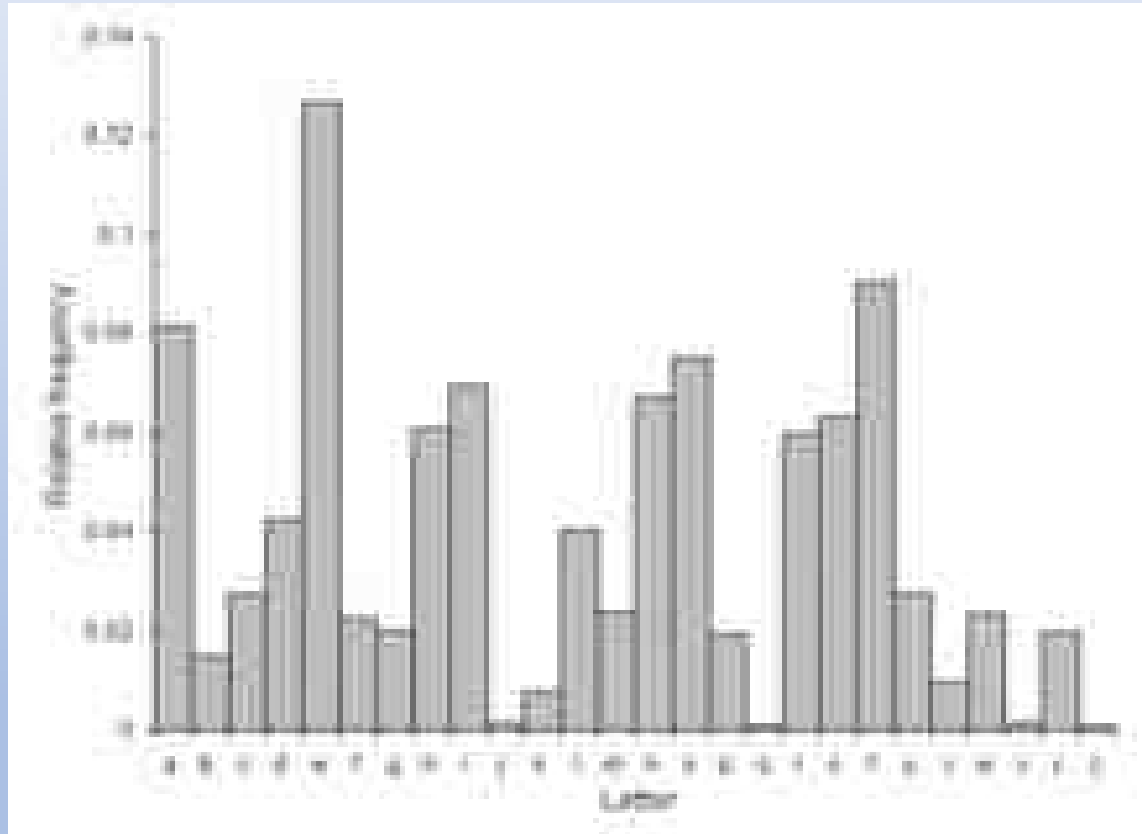
Exercise

Vigenere Cipher



- The apple is in the corner and the pear is there too (*plain*)
- cat (*key*)
- Find the *cipher*?
- the apple is in the corner and the pear is there too (*plain*)
- cat cat cat cat cat cat cat cat cat cat cat cat cat ca (*key*)
- Answer
- Vhx cpi neb uig vhx eok pek cnw vhx ret til vhx tem qo (*cipher*)

Frequency of the letters of the alphabet in English



Caesar Cipher

Cryptanalysis of Caesar Cipher



Frequency analysis of Plain Text



Frequency analysis of Caesar Cipher Text

Vigenere Cipher

Cryptanalysis of Vigenere Cipher



Frequency analysis of Plain Text



Frequency analysis of Vigenere Cipher Text

Vigenere Cipher

Cryptanalysis of Vigenere Cipher

- Three steps
 - Find the length of the key (Kasiski test)
 - **Divide** the message into that many shift cipher encryptions.
 - **Use frequency analysis** to solve the resulting shift ciphers.

Cipher Text

AQRTUVQSTVVXSLMPOR...
AQRTUVQSTVVXSLMPOR...

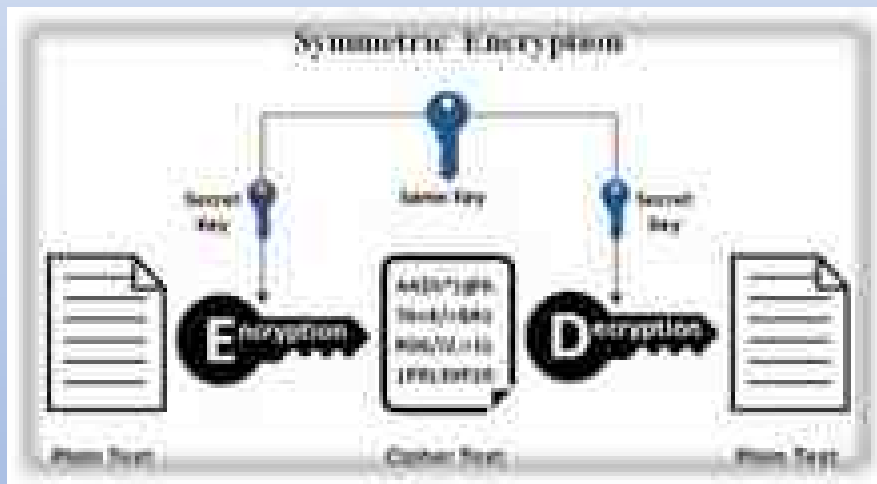


Modern Cryptography Algorithm Types

Symmetric and Asymmetric

Modern Cryptography Algorithm Types

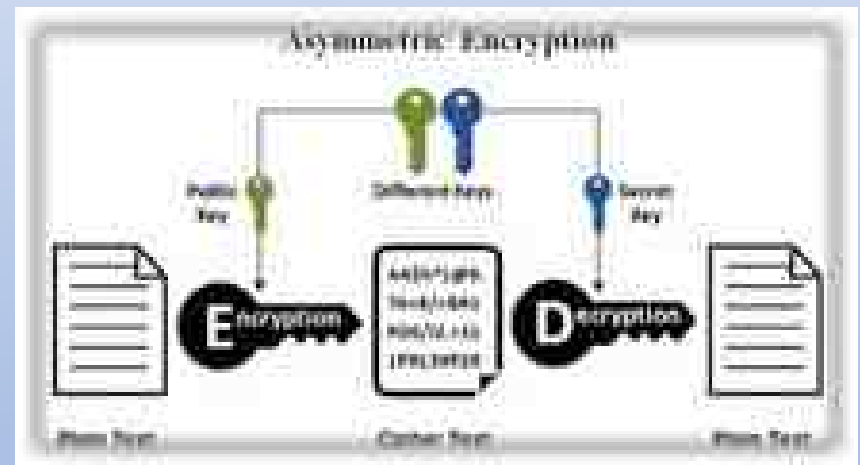
Symmetric Cryptography



- Need a strong encryption algorithm*
- Secure Key Exchange
- Its relatively fast

Asymmetric Cryptography

also known as Public Key Cryptography

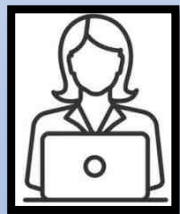


- Public and private keys are mathematically related
- **The private key** is never shared
- Its relatively slow

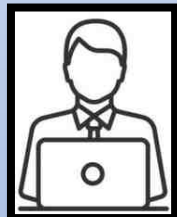
Modern Cryptography Algorithm

Communication Perspective

Symmetric Cryptography

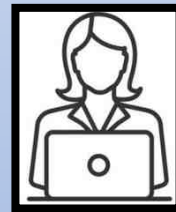


User 1

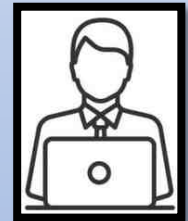


User 2

Asymmetric Cryptography



User 1

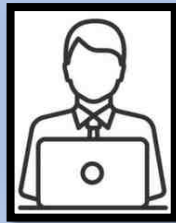


User 2

How Modern Cryptographic Algorithm Are Used?



User 1



User 2

Five Aspects of Security

Five Aspects of Security

Confidentiality

- Assurance that information is not disclosed to unauthorized individuals even they get access to it

Encryption

Integrity

- Information is not tampered by any unauthorized entities, if tampered then receiver must be able to detect that

Hashing

Availability

- Authorized users have timely and easy access to information when needed

IDS and IPS

Authenticity

- Prevents impersonation and enables receiver to **verify the sender of the message is who he claimed to be**

Digital signature

Non-Repudiation

- Sender can't deny after sending the message

Digital signature

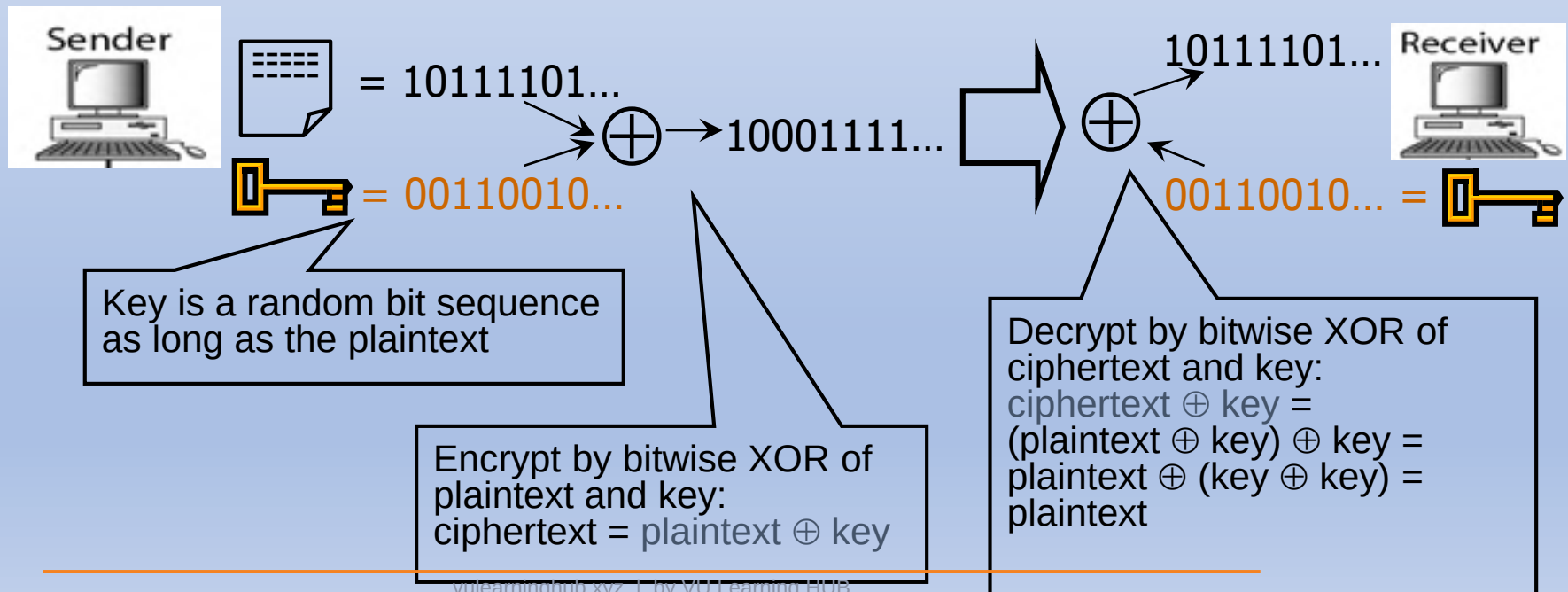
One Time Pad

An Example of Symmetric Encryption

One Time Pad

Example of Symmetric Encryption

- Invented by Gilbert Vernam in the 1920s
- The message is a bitstring $m \in \{0,1\}^n$
- The key is a bitstring as long as the message, $k \in \{0,1\}^n$
- The ciphertext is obtained by XORing each bit of the plaintext with each bit of the key: $c = m \oplus k$.



One Time Pad

Advantages

- **Easy to compute**
 - o Encryption and decryption are the same operation
 - o Bitwise XOR is very cheap to compute
- **As secure as theoretically possible**
 - o Given a ciphertext, all plaintexts are equally likely, regardless of attacker's computational resources
 - o if and only if the key sequence is truly random
 - True randomness is expensive to obtain in large quantities

One Time Pad

Disadvantages

- **Key must be as long as the plaintext**
 - o Impractical in most realistic scenarios
 - o Still used for diplomatic and intelligence traffic
- **Does not guarantee integrity**
 - o One-time pad only guarantees confidentiality
 - o Attacker cannot recover plaintext, but can easily change it to something else
- **Insecure if keys are reused**
 - o Attacker can obtain XOR of plaintexts

ROT13

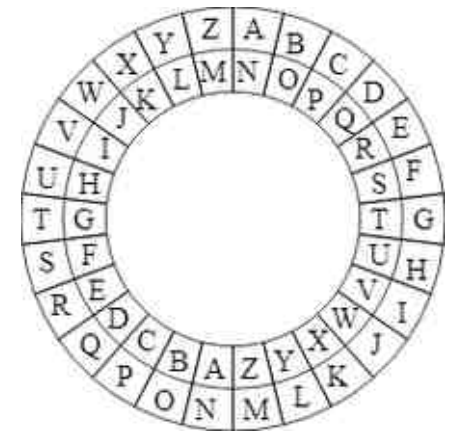
(Rotate by 13 places)

An Example of Symmetric Encrpytion

Symmetric Encryption

ROT13

- ROT13 cipher(read as – “rotate by 13 places”) is a special case of the Ceaser cipher in which the shift is always 13.
- This is an example of substitution **cipher**



Poor Encryption: ROT13

No “key”

Susceptible to frequency analysis

Susceptible to brute forcing

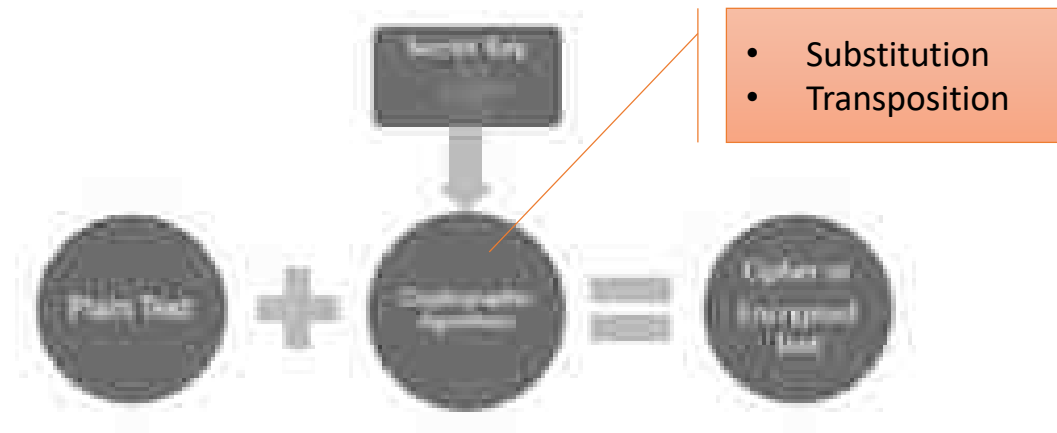
Confusion and Diffusion

Properties of the operation of a secure cipher

Confusion and Diffusion

Properties of the operation of a secure cipher

- Concept was originally presented by Claude Shannon in 1945



- Confusion refers to making the relationship between the Ciphertext and the Key as complex and involved as possible;
 - Make use of Substitution
- Diffusion refers to dissipating the statistical structure of Plaintext over the bulk of Ciphertext
 - Make use of Transposition

Feistel Cipher/Network consisting multiple rounds of processing of the plaintext, each round consisting of a “substitution” step followed by a permutation step.

Operational Modes of Symmetric Encryption

Stream Cipher and Block Cipher

Operational Modes of Symmetric Encryption

Symmetric encryption schemes follow two distinct modes of operation:

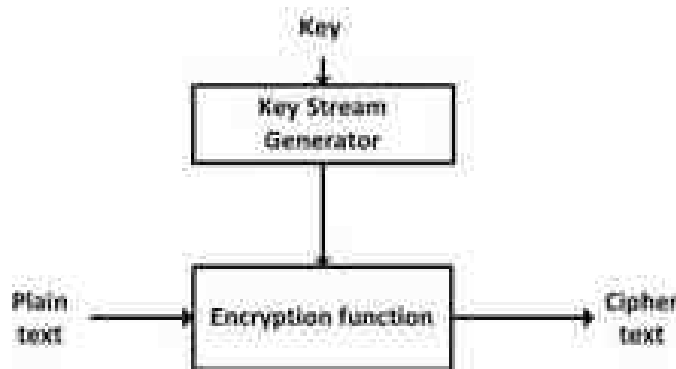
- **Stream Cipher**
 - o Plain text is encrypted bit by bit
 - o Plain text and key are XORed
- **Block Cipher**
 - o Plain text is encrypted block by block
 - o The whole block is encrypted with a key

Stream Ciphers

- Each bit of plaintext is encrypted one by one, with the corresponding bit of the keystream, obtaining a bit of ciphertext.
- To describe a stream cipher, it is enough to describe the key stream generator. Once the key stream is obtained, it works like the one-time pad.
- The key stream must be generated from a random seed



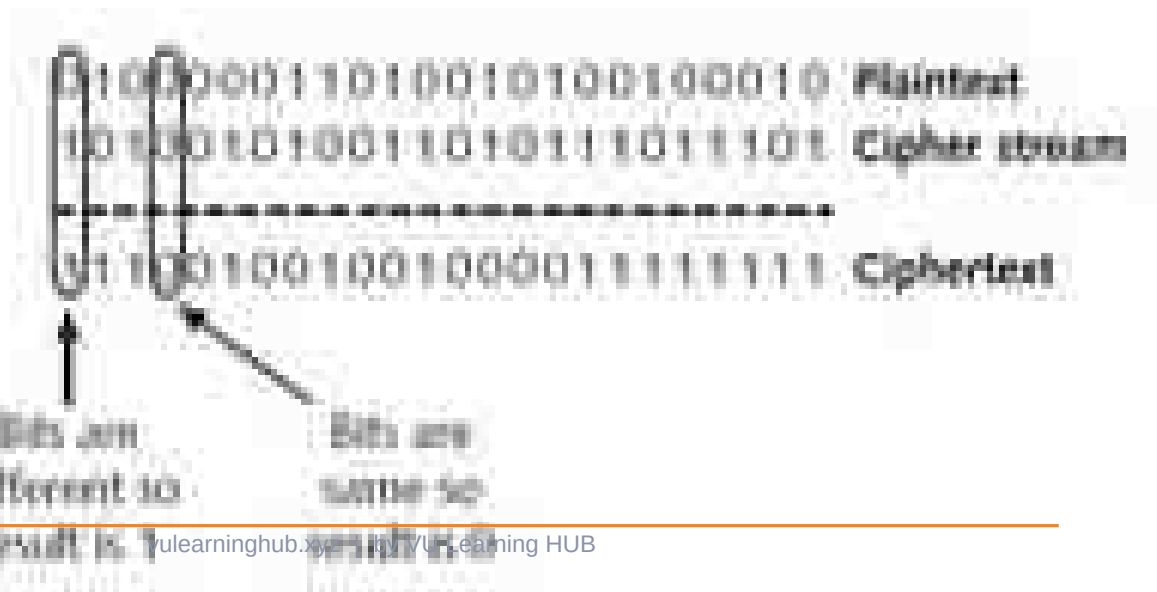
One Time Pad



Stream Ciphers

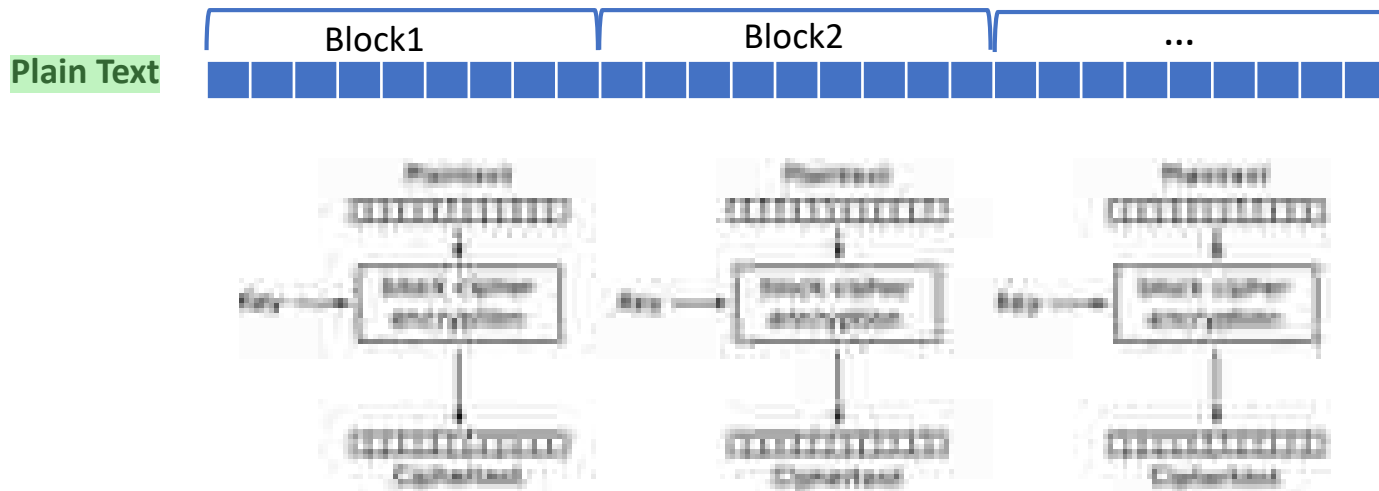
Stream Encryption

XOR GATE Truth Table



Block Ciphers

- Block ciphers operate on blocks of plaintext one at a time to produce blocks of ciphertext.
- The encryption of a bit in a plaintext will depend on the other bits in the block.
- The block sizes are usually reasonably large e.g. 64 bits, 128 bits, even more.

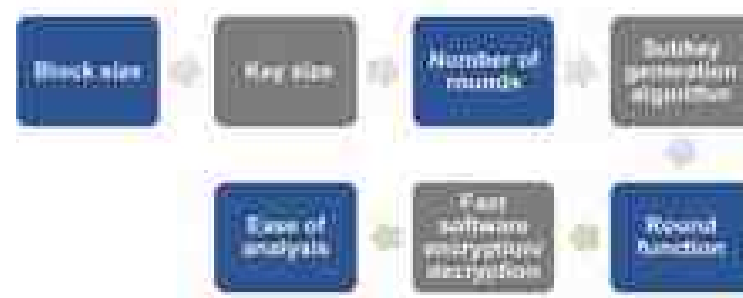
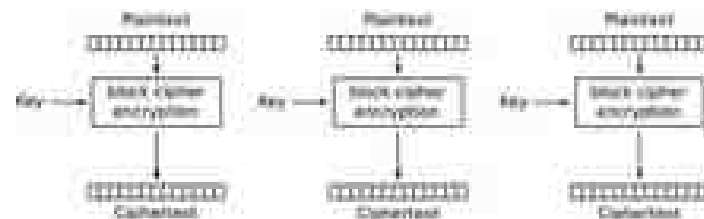


- The most famous block cipher is DES (Data Encryption Standard).
- Since DES is the most studied scheme and the design principles of DES have inspired a lot of ciphers used nowadays, we will have a slight view of **DES**.

Block Ciphers Design Considerations

Block Ciphers Design Considerations

- Processes the input one block of elements at a time
- Produces an output block for each input block
- Block size:** Larger block sizes mean greater security (all other things being equal) but reduced encryption/decryption speed. block size of 128 bits is a reasonable trade-off.
- Key size:** Larger key size means greater security but may decrease encryption/ decryption speed. The most common key length in modern algorithms is 128 bits.
- Number of rounds:** The essence of a symmetric block cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. A typical size is 16 rounds.
- Subkey generation algorithm:** Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.
- Round function:** Again, greater complexity generally means greater resistance to cryptanalysis.
- Fast software encryption/decryption:** In many cases, encryption is embedded in applications or utility functions and the speed of execution of the algorithm becomes a concern.
- Ease of analysis:** Although we would like to make our algorithm as difficult as possible to cryptanalyze, there is great benefit in making the algorithm easy to analyze vulnerabilities.



	128b	Triple 128b	256b
Plaintext block size (bits)	128	128	128
Ciphertext block size (bits)	128	128	128
Key size (bits)	128	112 or 168	256, 192, or 128

128b = Data Encryption Standard
 168b = Advanced Encryption Standard

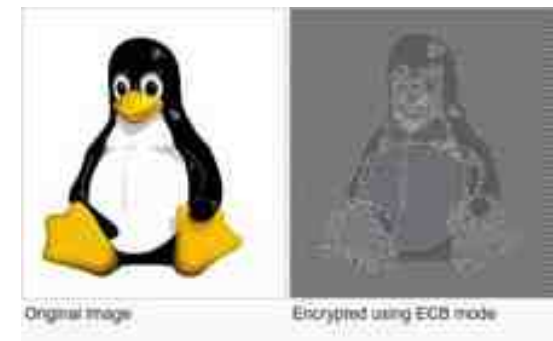
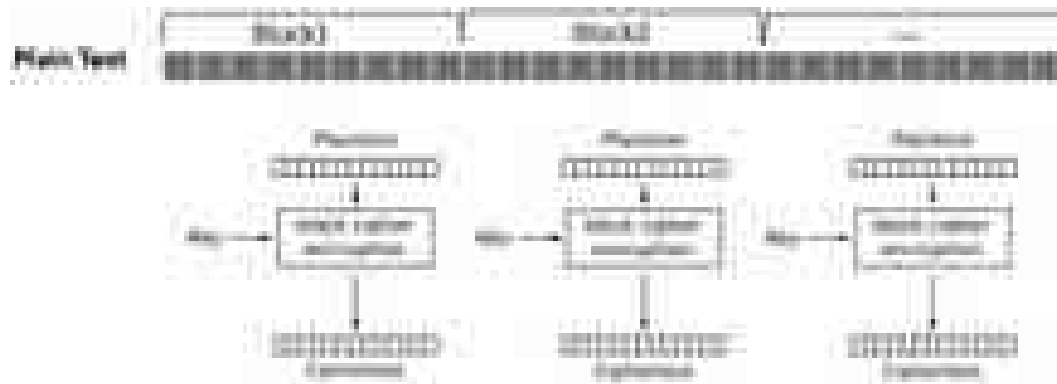
Block Cipher Modes

Symmetric Encryption

Block Cipher Modes - Symmetric Encryption

Practical Security Issues

- Typically, symmetric encryption is applied to a unit of data larger than a single 64-bit or 128-bit block.
- The simplest approach to multiple-block encryption:
 - Each block of plaintext is encrypted using the same key
 - Cryptanalysts may be able to exploit regularities in the plaintext
 - This is commonly known as **Electronic Code Book (ECB) mode**



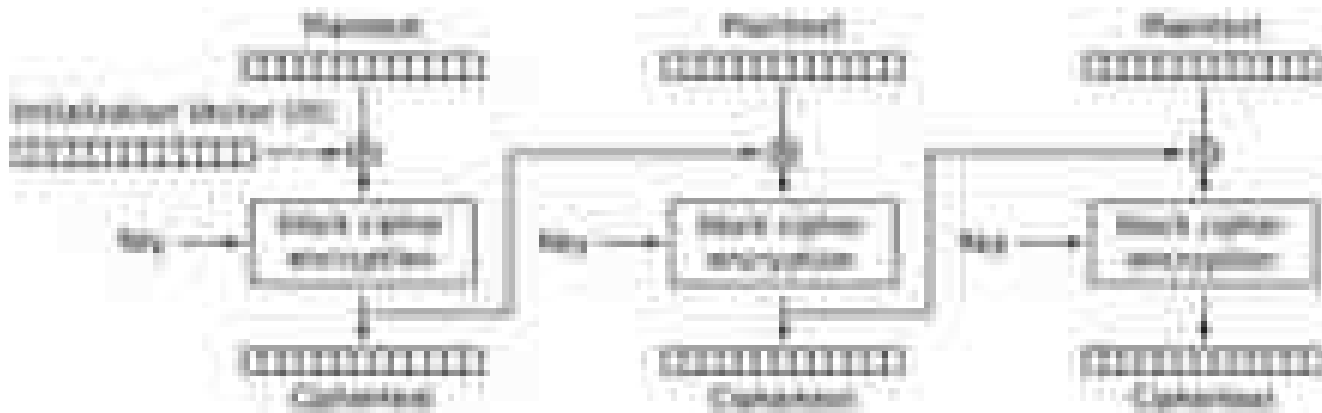
- Alternative techniques developed to increase the security of symmetric block encryption for large sequences
- Overcomes the weaknesses of ECB
- Consequently...different Block cipher modes were designed

- **Electronic Code Book (ECB) Mode**
- Cipher Block Chaining (CBC) Mode
- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFM)
- Counter mode (CTR)

Cipher Block Chaining Mode

- Electronic Code Book (ECB) Mode
- **Cipher Block Chaining (CBC) Mode**
- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFM)
- Counter mode (CTR)

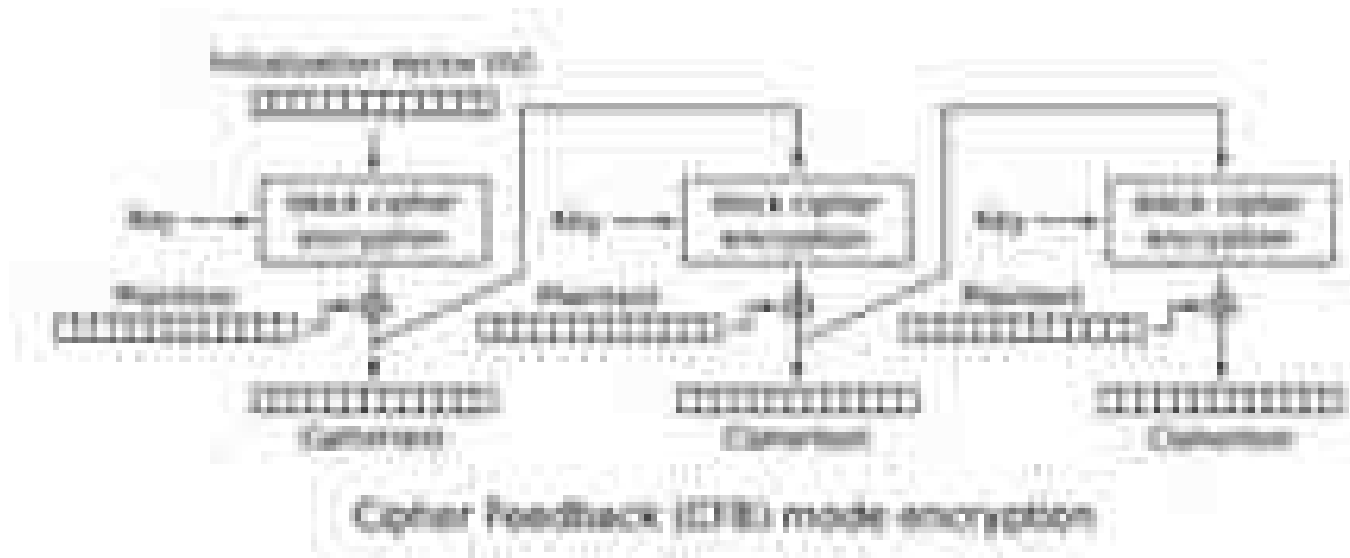
- Input to encryption algorithm is XOR of next 64-bits plaintext and preceding 64-bits ciphertext
- Typical applications: General-purpose block-oriented transmission; authentication
- Initialization Vector (IV) must be known by sender/receiver, but secret from attacker



Cipher Feedback Mode

- Electronic Code Book (ECB) Mode
- Cipher Block Chaining (CBC) Mode
- **Cipher Feedback Mode (CFB)**
- Output Feedback Mode (OFM)
- Counter mode (CTR)

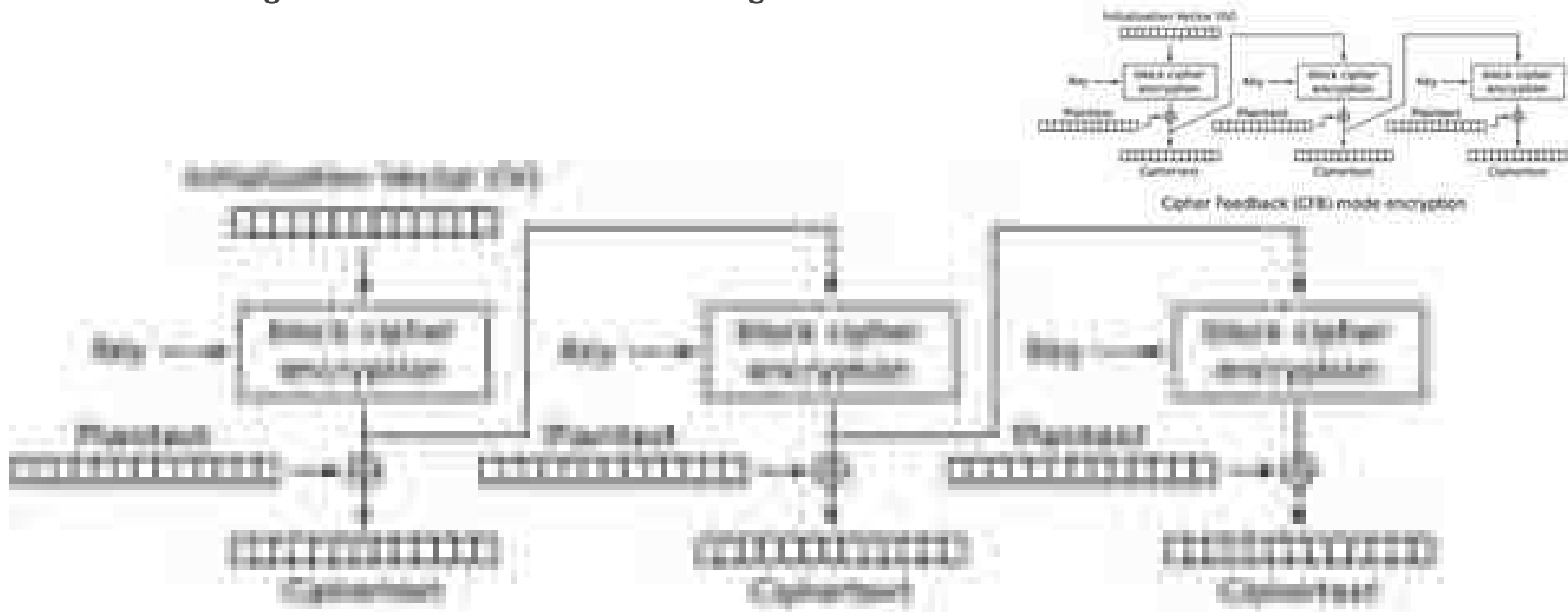
- Converts block cipher into stream cipher
- No need to pad message to integral number of blocks
- Operate in real-time: each character encrypted and transmitted immediately
- Input processed s bits at a time
- Preceding ciphertext used as input to cipher to produce pseudo-random output
- XOR output with plaintext to produce ciphertext
- Typical applications: General-purpose stream-oriented transmission; authentication



Output Feedback Mode

- Electronic Code Book (ECB) Mode
- Cipher Block Chaining (CBC) Mode
- Cipher Feedback Mode (CFB)
- **Output Feedback Mode (OFM)**
- Counter mode (CTR)

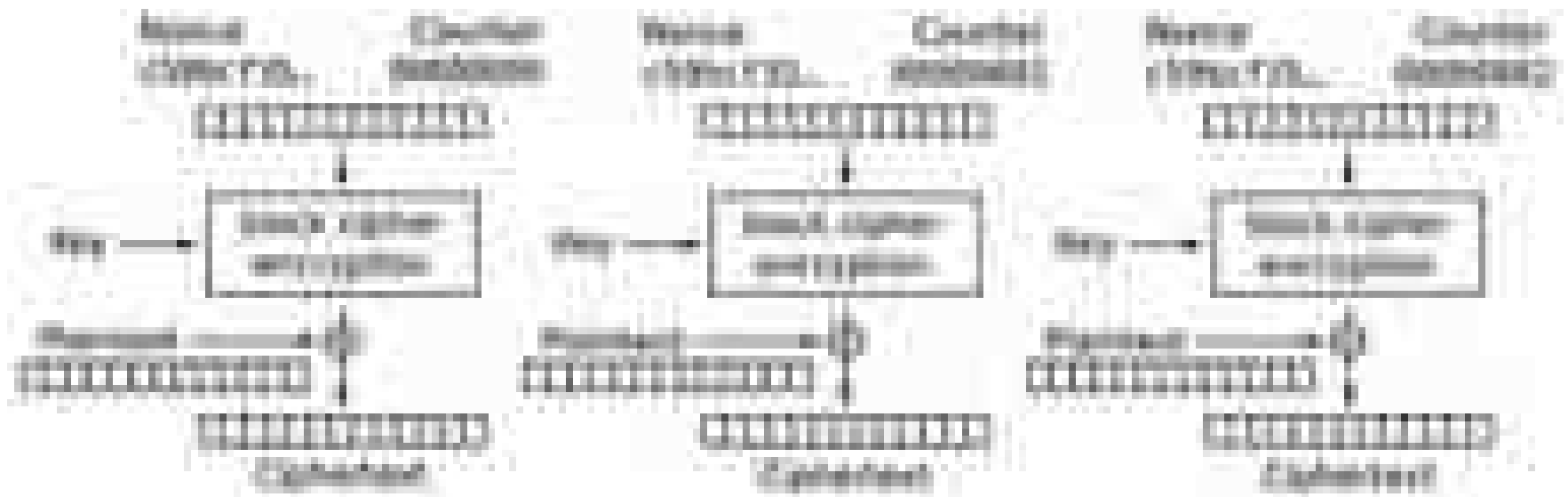
- Converts block cipher into stream cipher
- Similar to CFB, except input to encryption algorithm is preceding encryption output
- Typical applications: stream-oriented transmission over noisy channels (e.g. satellite communications)
- Advantage compared to OFB: bit errors do not propagate
- Disadvantage: more vulnerable to message stream modification attack



Counter Mode

- Electronic Code Book (ECB) Mode
- Cipher Block Chaining (CBC) Mode
- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFM)
- **Counter Mode (CTR)**

- Converts block cipher into stream cipher
- Each block of plaintext XORed with encrypted counter
- Typical applications: General-purpose block-oriented transmission; useful for high speed requirements
- Efficient hardware and software implementations
- Simple and secure



Block Cipher Modes - Symmetric Encryption

Summary

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	•General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	Input is processed s bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	•General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	•General-purpose block-oriented transmission •Useful for high-speed requirements

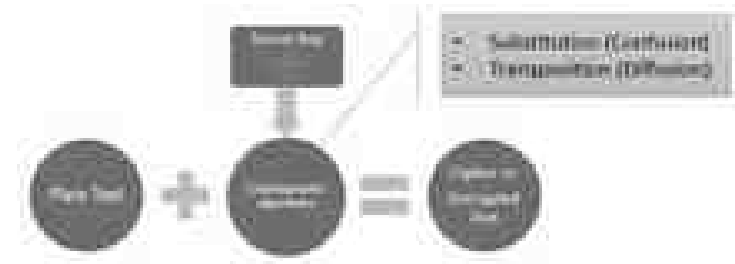
Attack Strategies on Symmetric Encryption

Brute-force Attacks

- Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
- On average half of all possible keys must be tried to achieve success
- Number of Keys are dictated by the key size.

Cryptanalytic Attacks

- Rely on:
 - Nature of the algorithm
 - Some knowledge of the general characteristics of the plaintext
 - Some sample plaintext-ciphertext pairs
- Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
 - If successful, all future and past messages encrypted with that key are compromised

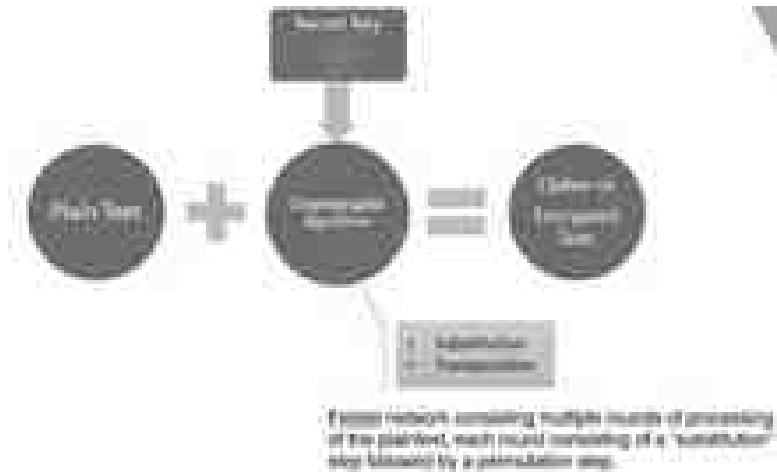


Feistel Network

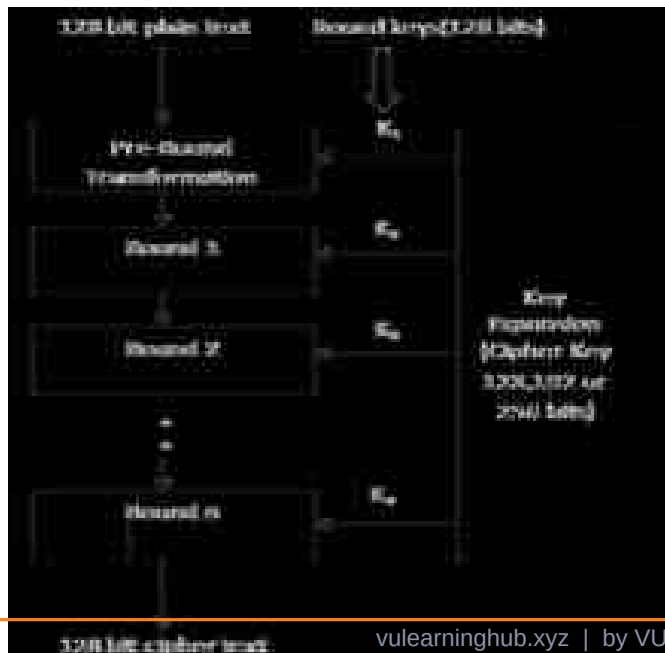
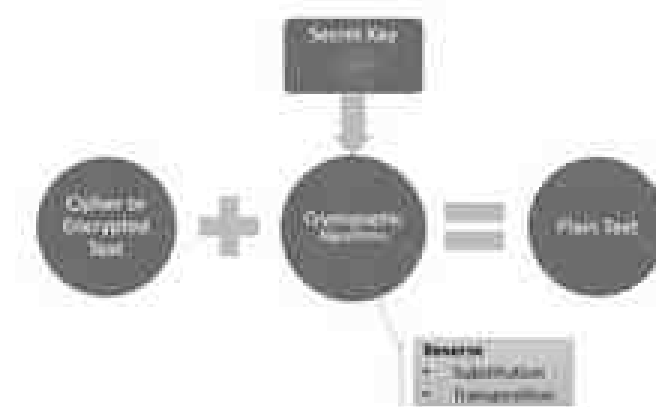
Symmetric Encryption

Encryption/Decryption Process

Encryption Process



Decryption Process



We want to make encryption process hard for attacker to break our algorithm...How?

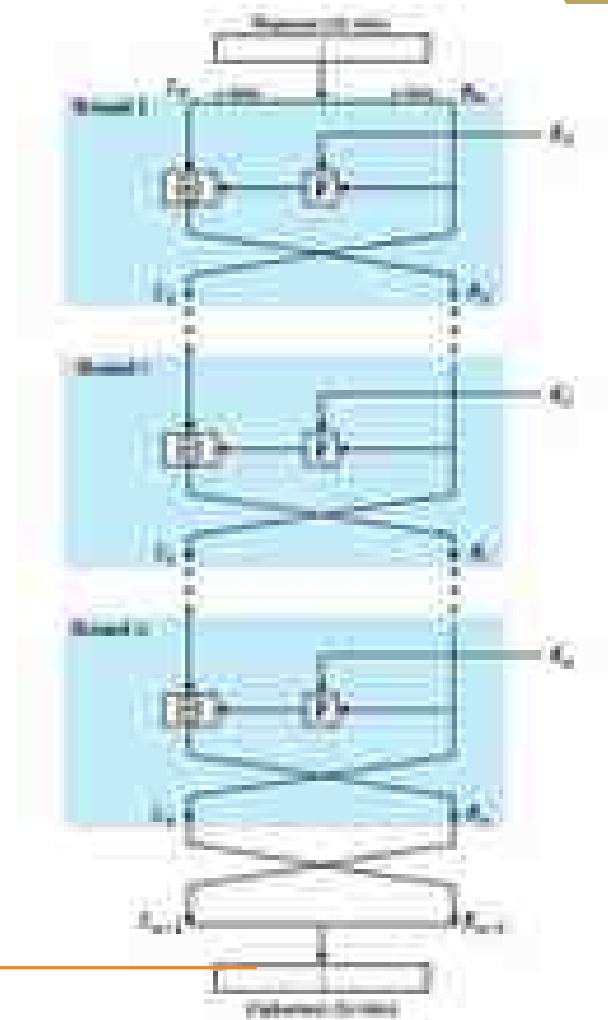
More rounds, complex substitution and transposition...

But, users with the K_e should be able to decrypt it easily...How?

Feistel Network

Feistel Network - Symmetric Encryption

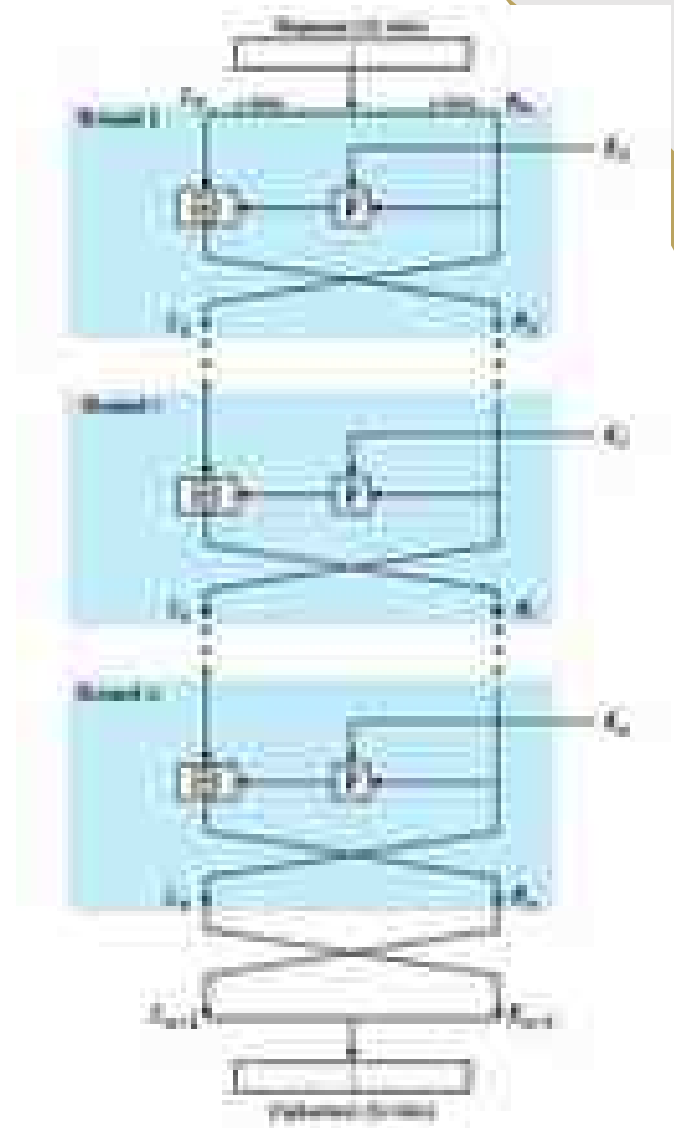
- Many encryption algorithms incorporate a structure first proposed by Horst Feistel of IBM (1973); a **Feistel Network**.
- Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a “substitution” step followed by a permutation step.
- Many advance encryption algorithms are designed using this Feistel structure
 - This includes the DES standard.



Feistel Network

Brief explanation

- The inputs to the encryption algorithm are a plaintext block of length $2w$ bits and a key K .
- The plaintext block is divided into two halves, L^0 and R^0 .
- The two halves of the data pass through n rounds of processing and then combine to produce the ciphertext block.
- Each round i has as inputs L^{i-1} and R^{i-1} , derived from the previous round, as well as a subkey K^i , derived from the overall K .
- In general, the subkeys K^i are different from K and from each other and are generated from the key by a subkey generation algorithm.



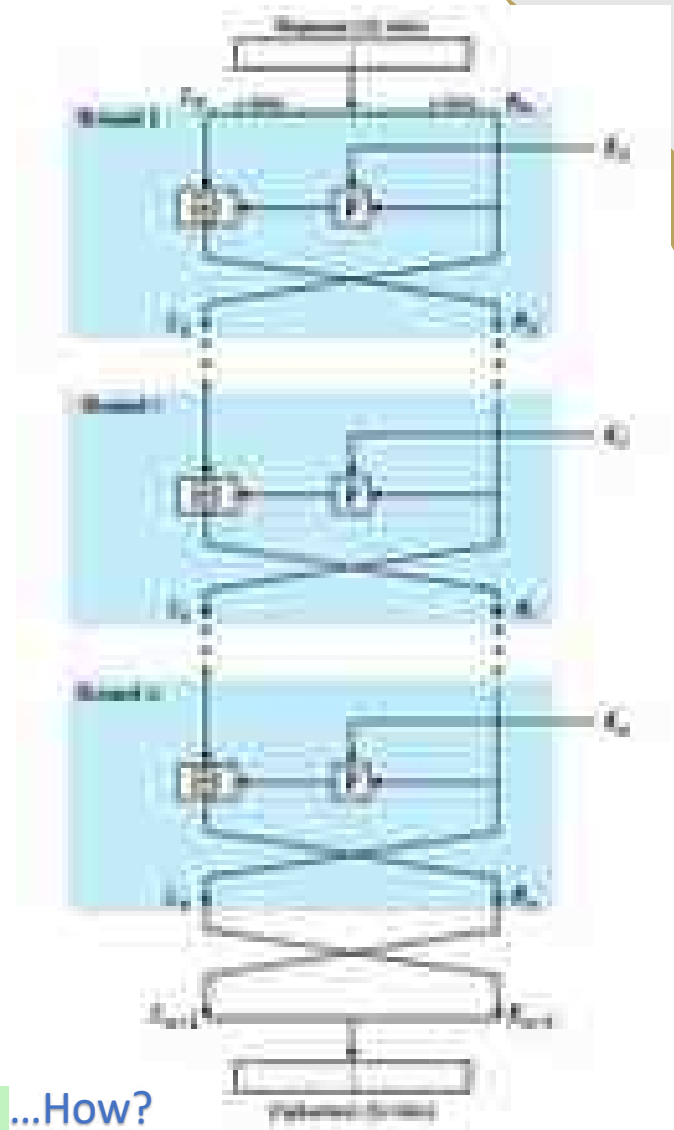
Feistel Network

Brief explanation

- All rounds have the same structure. A substitution is performed on the left half of the data.
- This is done by applying a round function F to the right half of the data and then taking the exclusive-OR (XOR) of the output of that function and the left half of the data.
- The round function has the same general structure for each round but is parameterized by the round subkey K^i .
- Following this substitution, a permutation is performed that consists of the interchange of the two halves of the data.

What's happening inside round function "F"?

Users with the Key should be able to decrypt it easily...How?



Feistel Network

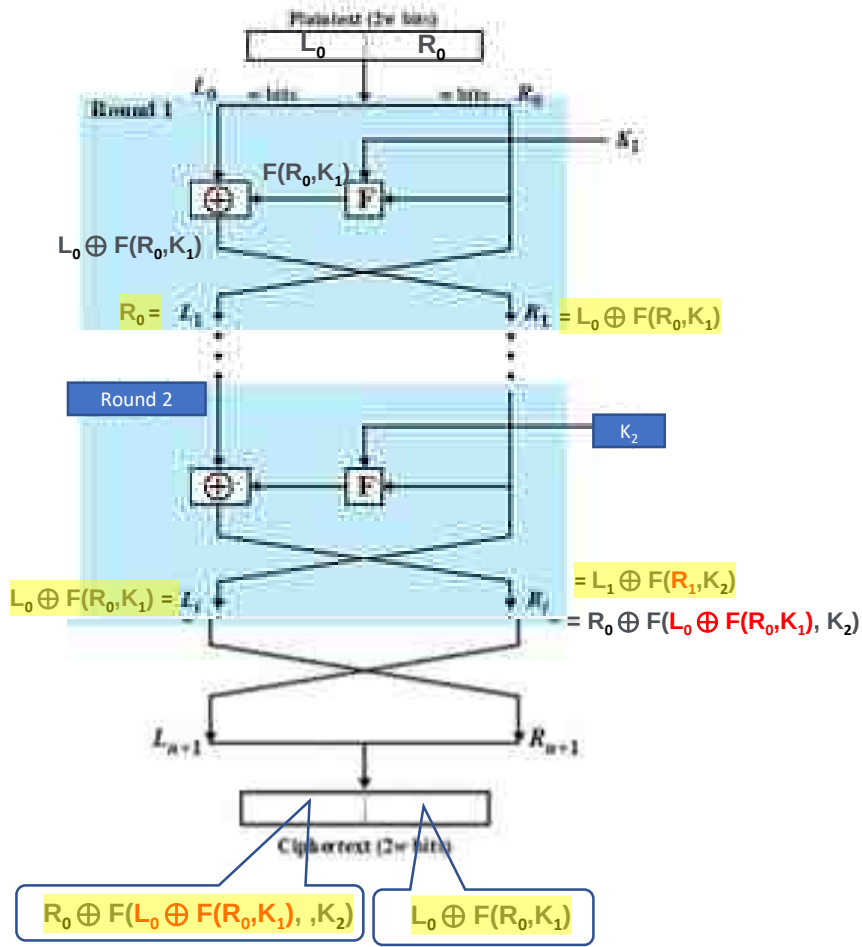
Encryption/Decryption Process

What's happenin inside round function "F"?

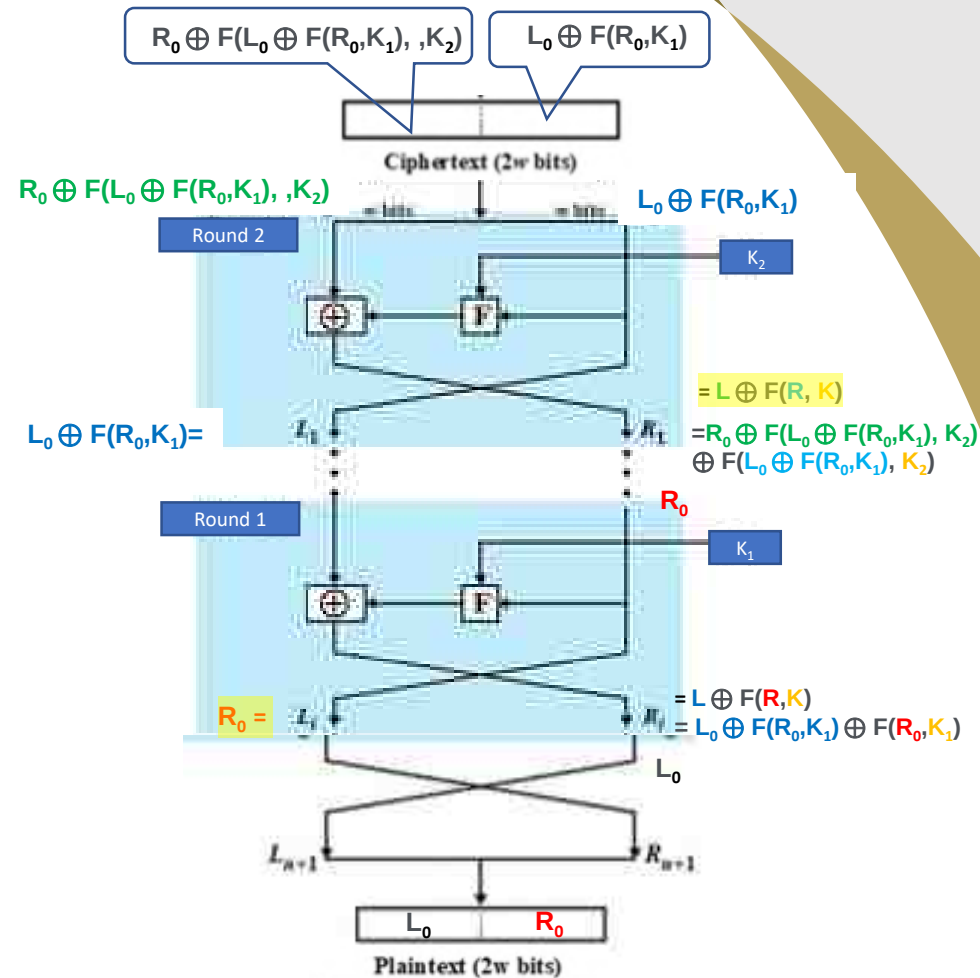
Users with the Ke should be able decrypt it
easi ...How?

Feistel Network

Encryption Process



Decryption Process



Data Encryption Standard (DES)

Symmetric Encryption Algorithm

Data Encryption Standard (DES)

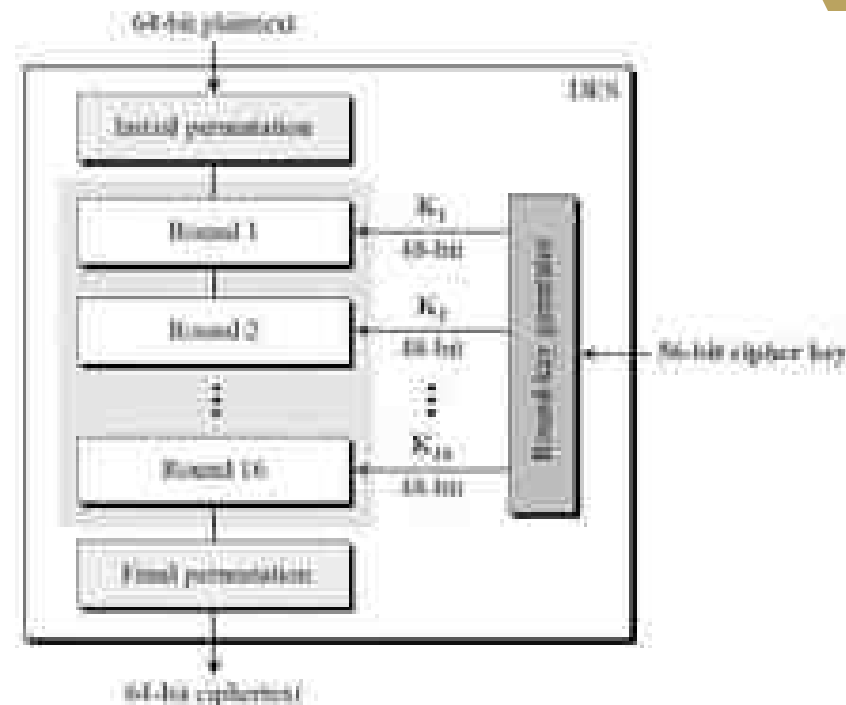
Symmetric Encryption Algorithm

Until recently was the most widely used encryption scheme

- Federal Information Processing Standards FIPS PUB 46
- Referred to as the Data Encryption Algorithm (DEA)
- DES is the most studied encryption algorithm
- DES is a Feistel Cipher.

Working

- 64 bit plaintext block
- 56 bit key
- to produce a 64 bit ciphertext block
- Total 16 rounds
- Concerns about the use of a 56-bit key
 - Prone to brute-force attack...



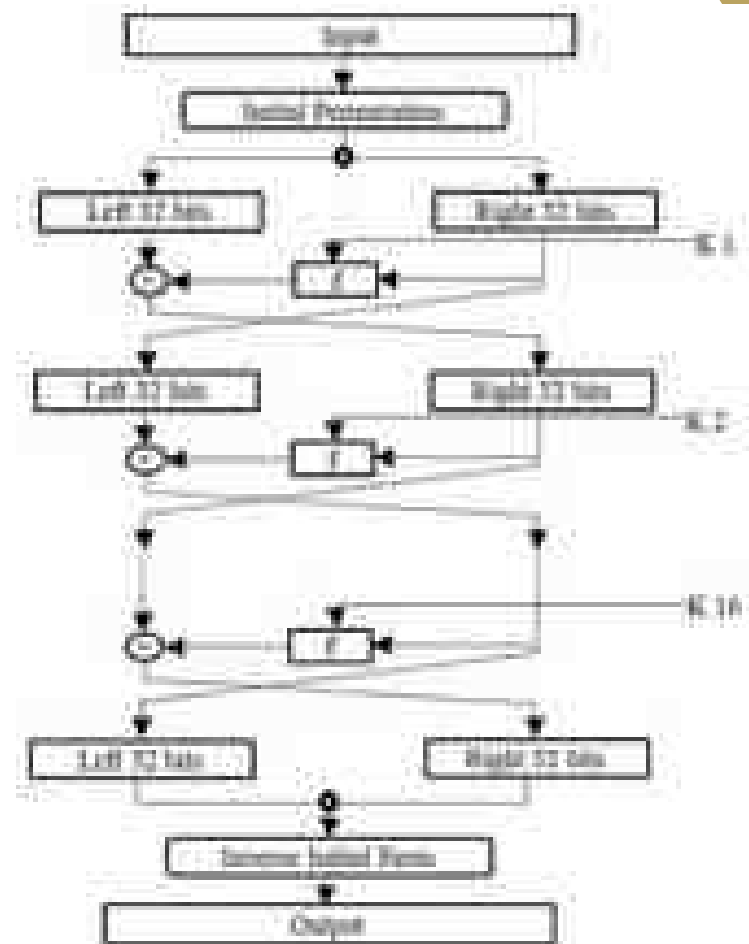
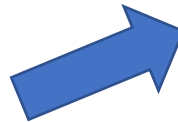
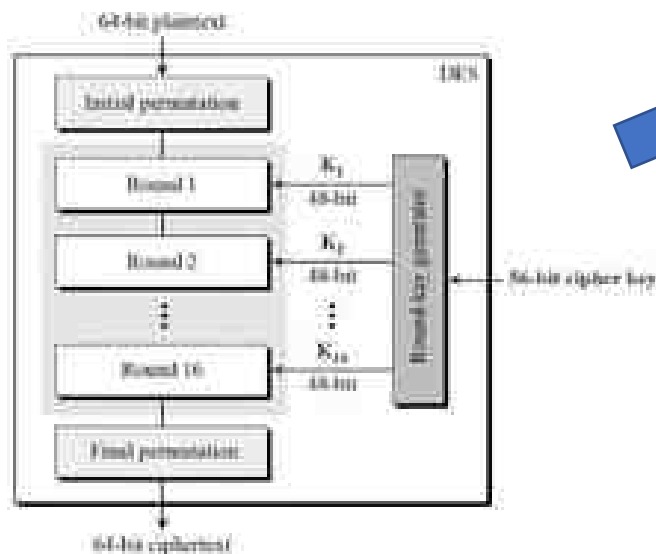
Data Encryption Standard (DES)

Symmetric Encryption Algorithm

- DES is the most studied encryption algorithm
- DES is a Feistel Cipher.

Working

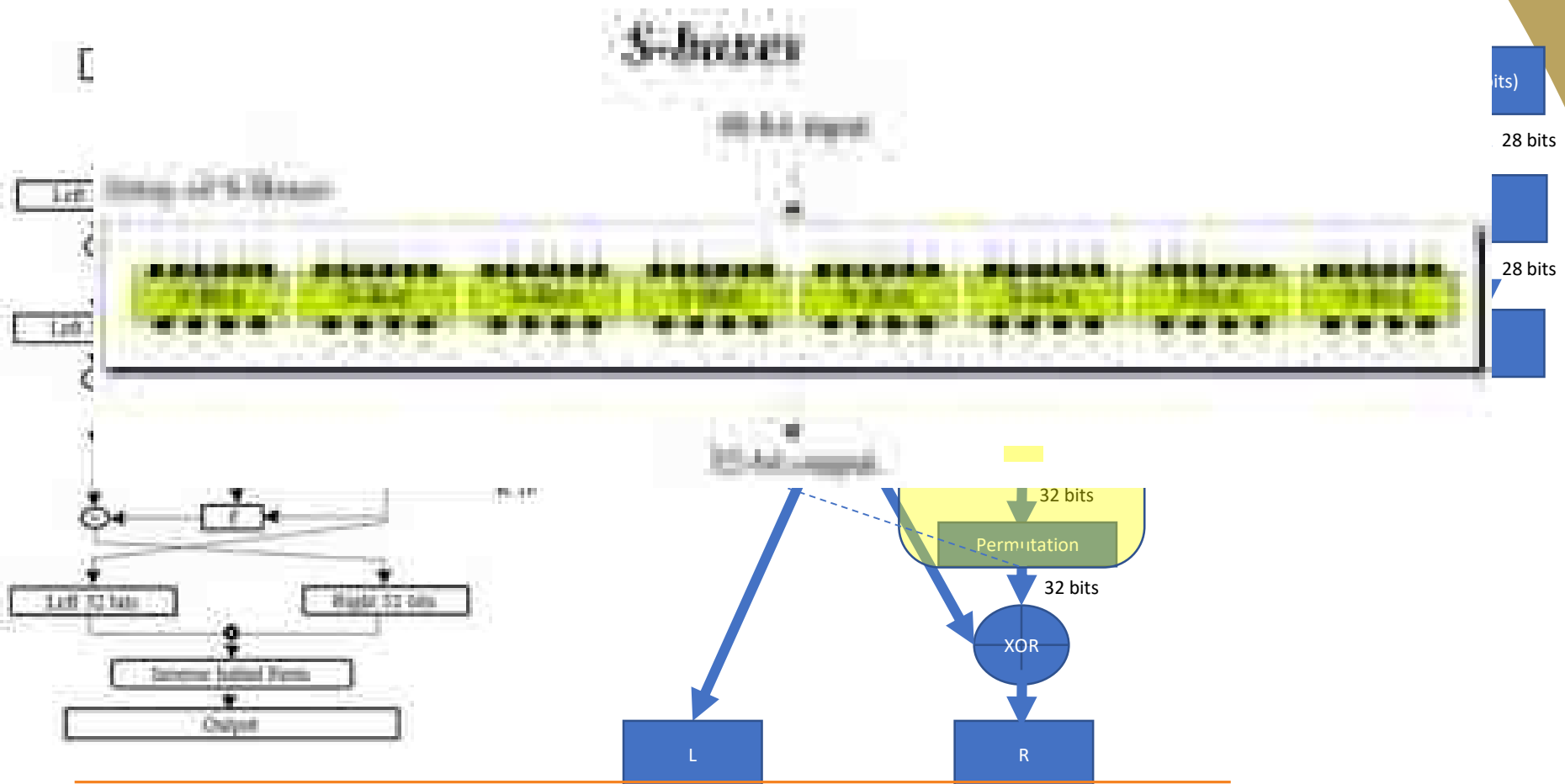
- 64 bit plaintext block
- 56 bit key
- to produce a 64 bit ciphertext block
- Total 16 rounds



Data Encryption Standard (DES)

What happens in each round?

- 16 Rounds.
- In each round we apply:
 - Expansion Box.
 - Substitution Box.
 - XOR with the round key.



Data Encryption Standard (DES)

How strong?

Concerns about the use of a 56-bit key

Brute-force attacks

- Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
- On average *half of all possible keys must be tried* to achieve success
- Number of Keys are dictated by the key size.

Key size (bits)	Ciphertext (bits)	Number of Encryptions Keys	Time Required at 10 ⁹ Encryptions/s	Time Required at 10 ¹¹ Encryptions/s
56	64	$2^{56} \approx 7.2 \times 10^{16}$	27 sec = 1.221 hours	1.2 days

Think...what can you do to make it strong??

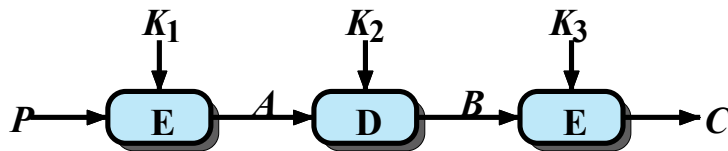
Triple DES (3DES)

Symmetric Encryption Algorithm

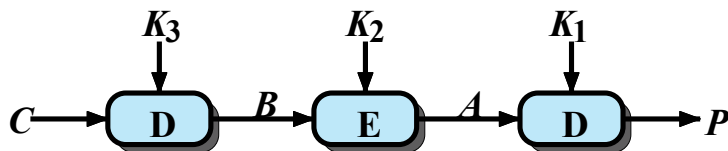
Triple DES (3DES)

Symmetric Encryption Algorithm

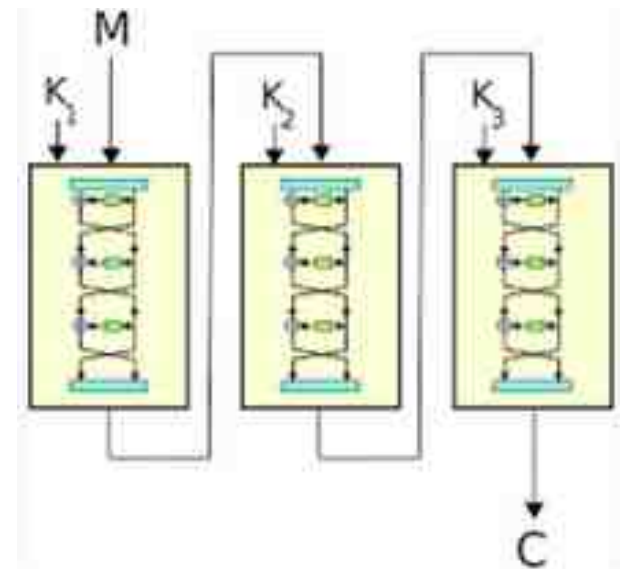
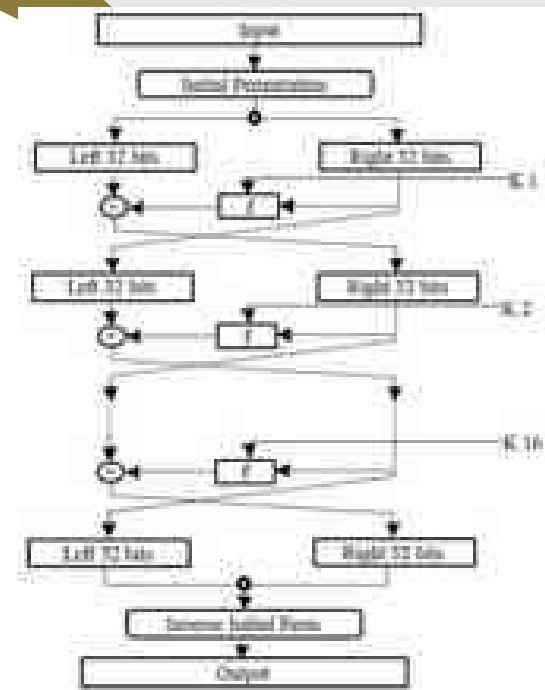
- Designed to address security concerns over DES
 - Original DES soon become prone to brute-force attack
- Need more secure encryption algorithms
- Repeats basic DES algorithm three times using either two or three unique keys
- First standardized for use in financial applications in ANSI standard X9.17 in 1985



(a) Encryption



(b) Decryption



Triple DES (3DES)

Symmetric Encryption Algorithm

Attractions:

- With three distinct keys, 3DES has an effective key length of 168 bits.
- 168-bit key length overcomes the vulnerability to brute-force attack of DES
- Underlying encryption algorithm is the same as in DES

Key Size (bits)	Cipher	Number of Encryption Steps	Time Required to 10 ⁹ Encryptions	Time Required to 10 ¹¹ Encryptions
56	DES	$2^{16} \approx 6.5 \times 10^4$	27 sec ≈ 0.001 min	1 hour
168	Triple DES	$2^{168} \approx 3.4 \times 10^{50}$	2^{168} sec $\approx 6.8 \times 10^{47}$ min	4.3×10^{47} years

Drawbacks:

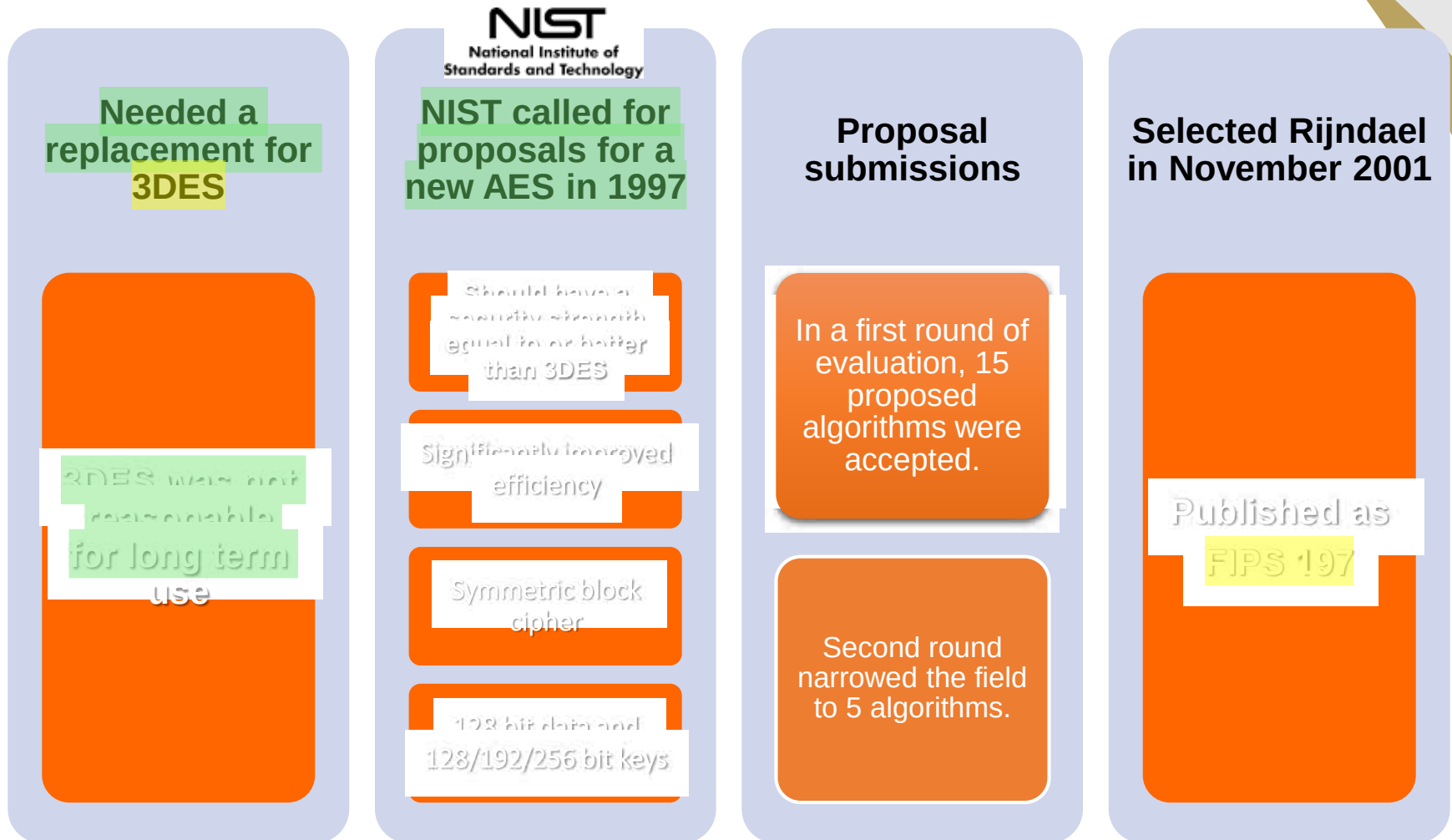
- Algorithm is sluggish in software
- Uses a 64-bit block size

Advanced Encryption Standard (AES)

Symmetric Encryption Algorithm

Advanced Encryption Standard (AES)

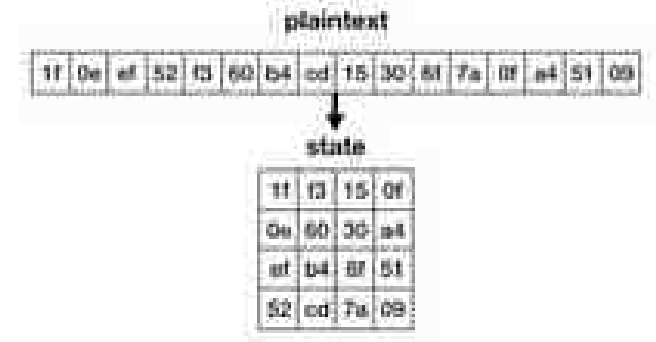
Symmetric Encryption Algorithm



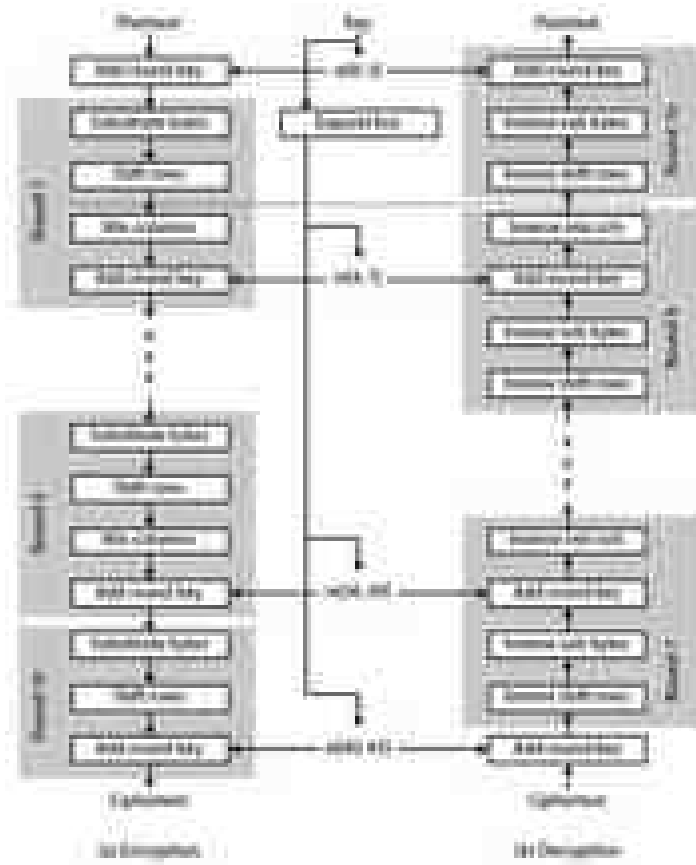
Advanced Encryption Standard (AES)

Symmetric Encryption Algorithm

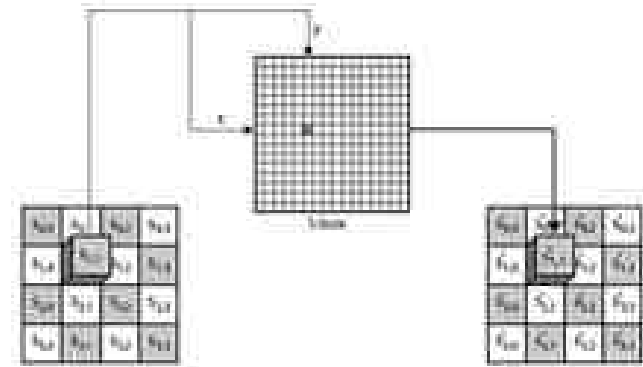
- An **iterative** rather than **Feistel** cipher
 - Processes data as block of 4 columns of 4 bytes
 - Operates on entire data block in every round
- Designed to be:
 - Resistant against known attacks
 - Speed and code compactness on many CPUs
 - Design simplicity
- Data block viewed as 4-by-4 table of bytes
 - Such a table is called the **current state**
- Key is expanded to array of words
- Has 10 rounds in which state the following transformations (called 'layers'):
 - BS- byte substitution (1 S-box used on every byte)
 - SR- shift rows (permute bytes between groups/columns)
 - MC- mix columns (uses matrix multiplication in GF(2⁸))
 - ARK- add round key (XOR state with round key)
- First and last round are a little different



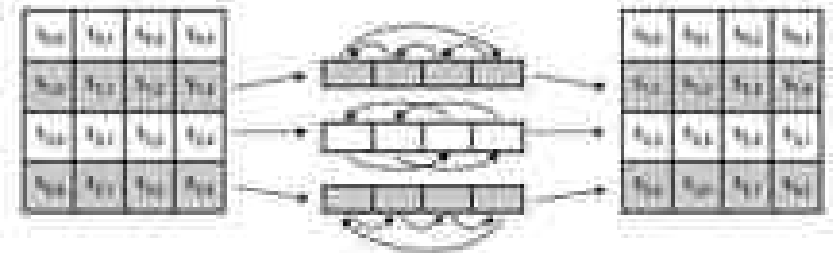
AES Working



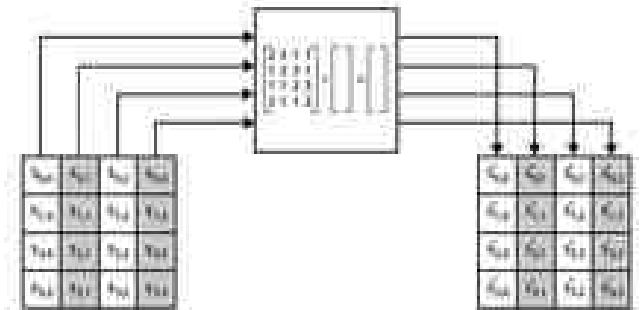
BS



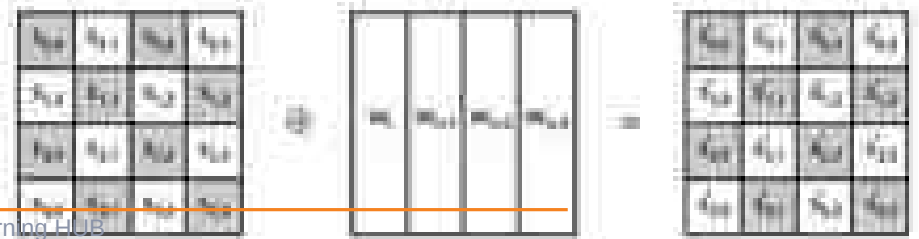
SR



MC

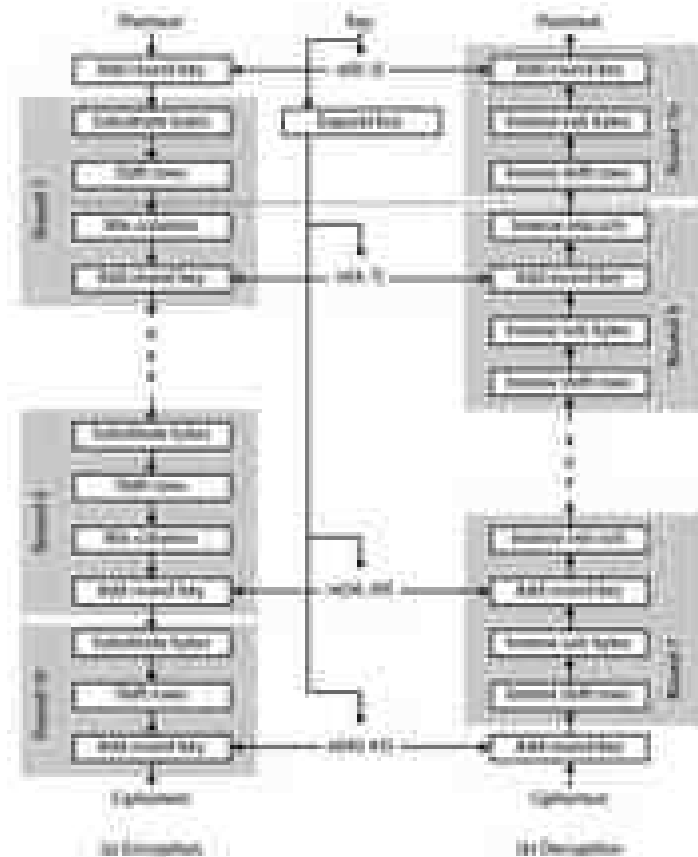


ARK



AES Working

Byte Substitution



BS



	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	64	5b	91	2b	75	ff	60	72	4d	03	76	ad	54	65	ce	95
1	27	80	74	21	1a	84	02	5c	4e	67	96	8b	4f	1b	62	90
2	49	7d	33	bc	15	70	3f	4a	50	12	63	57	7e	32	36	81
3	82	99	3a	2c	18	af	08	52	71	19	20	35	6d	40	88	2d
4	5d	45	98	14	7c	9e	05	46	86	bd	31	16	74	17	8a	2e
5	28	eb	6b	48	53	07	13	42	24	34	85	44	68	94	9d	83
6	94	1c	43	28	5a	22	25	af	9a	78	26	ae	80	38	79	72
7	51	00	8c	bf	81	11	71	99	3e	47	87	93	73	10	4b	41
8	09	26	5e	66	4c	61	51	23	8d	6c	27	bb	3d	0b	fb	86
9	88	77	47	16	85	40	39	70	0f	dc	62	8e	37	92	44	7a
a	53	01	10	7b	30	fb	8f	9b	32	1a	5b	04	7a	2e	9a	96
b	17	14	23	ea	cc	58	06	42	69	97	28	11	41	9c	40	7d
c	38	16	0d	7f	54	63	87	31	15	29	48	04	74	22	64	55
d	02	08	4f	1b	62	90	81	93	73	10	4b	41	7a	2e	9a	96
e	4e	3b	61	51	23	8d	6c	27	bb	3d	0b	fb	86	2d	83	2f
f	8b	4f	1b	62	90	81	93	73	10	4b	41	7a	2e	9a	96	2f

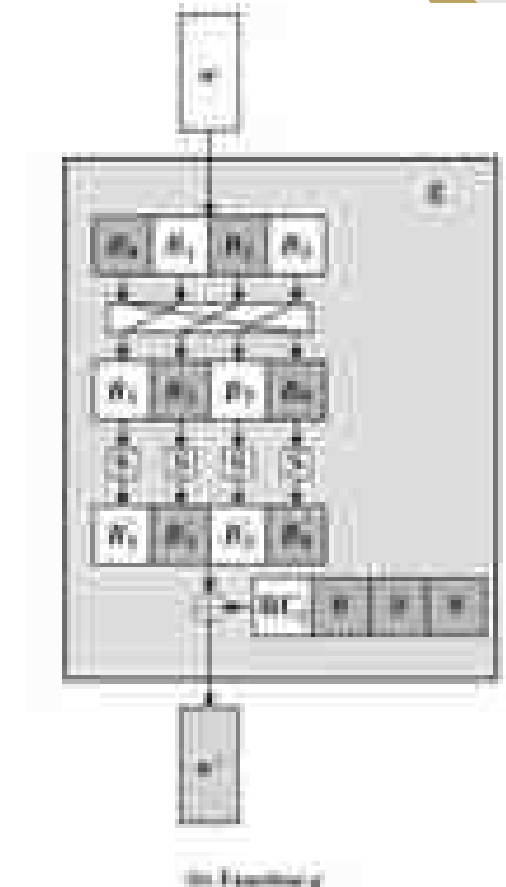
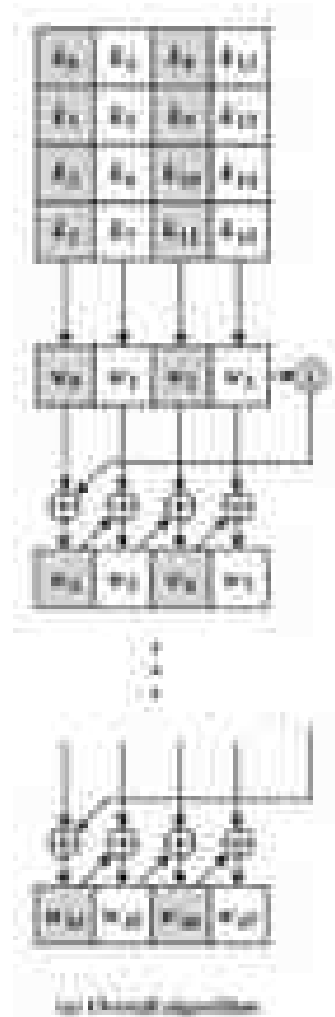
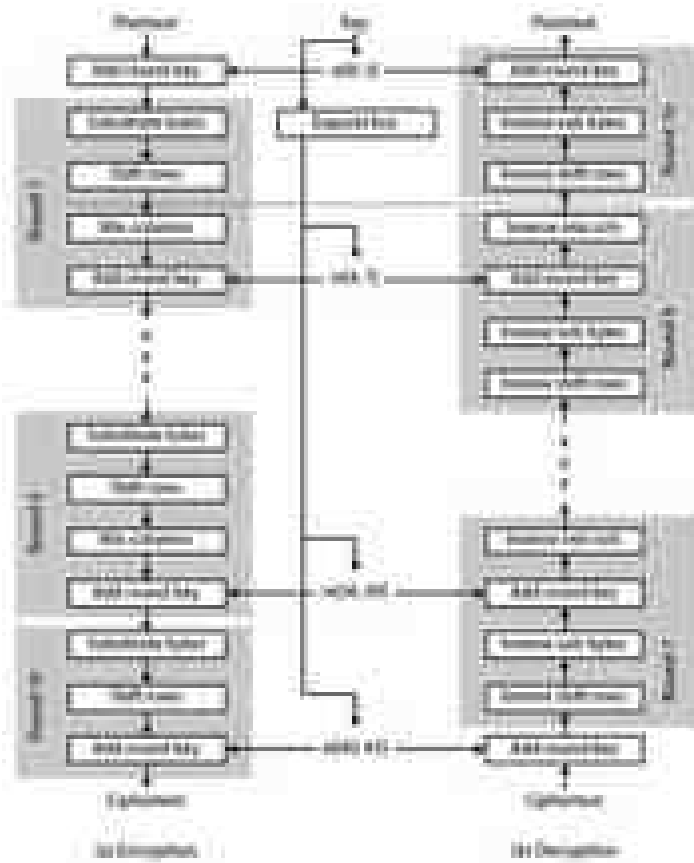
AES S-box

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	64	5b	91	2b	75	ff	60	72	4d	03	76	ad	54	65	ce	95
1	27	80	74	21	1a	84	02	5c	4e	67	96	8b	4f	1b	62	90
2	49	7d	33	bc	15	70	3f	4a	50	12	63	57	7e	32	36	81
3	82	99	3a	2c	18	af	08	52	71	19	20	35	6d	40	88	2d
4	5d	45	98	14	7c	9e	05	46	86	bd	31	16	74	17	8a	2e
5	28	eb	6b	48	53	07	13	42	24	34	85	44	68	94	9d	83
6	94	1c	43	28	5a	22	25	af	9a	78	26	ae	80	38	79	72
7	51	00	8c	bf	81	11	71	99	3e	47	87	93	73	10	4b	41
8	09	26	5e	66	4c	61	51	23	8d	6c	27	bb	3d	0b	fb	86
9	88	77	47	16	85	40	39	70	0f	dc	62	8e	37	92	44	7a
a	53	01	10	7b	30	fb	8f	9b	32	1a	5b	04	7a	2e	9a	96
b	17	14	23	ea	cc	58	06	42	69	97	28	11	41	9c	40	7d
c	38	16	0d	7f	54	63	87	31	15	29	48	04	74	22	64	55
d	02	08	4f	1b	62	90	81	93	73	10	4b	41	7a	2e	9a	96
e	4e	3b	61	51	23	8d	6c	27	bb	3d	0b	fb	86	2d	83	2f
f	8b	4f	1b	62	90	81	93	73	10	4b	41	7a	2e	9a	96	2f

AES Inverse S-box

AES Sub-Key Generation

Key Expansion



Public-Key Cryptography

Asymmetric Encryption

Public-Key Cryptography

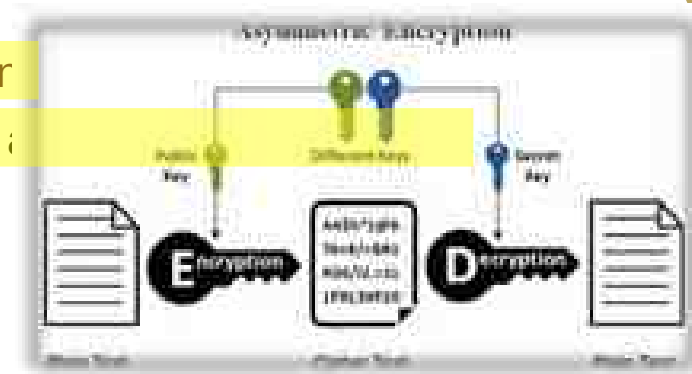
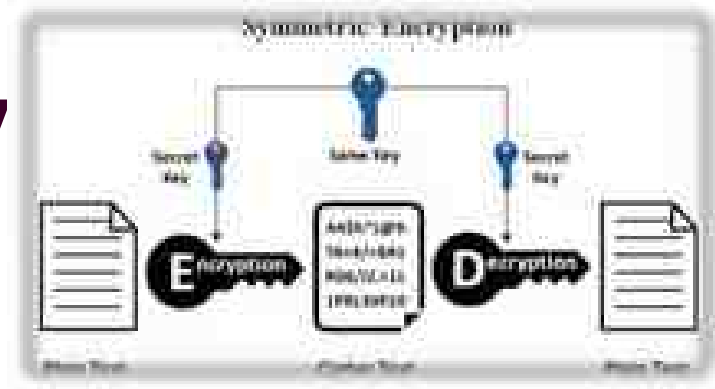
Asymmetric Encryption

Why Public-Key?

- Developed to address two major issues:
 - **key distribution** – how to have secure key exchange among communicating parties
 - **digital signatures** – how to verify a message comes intact from the claimed sender

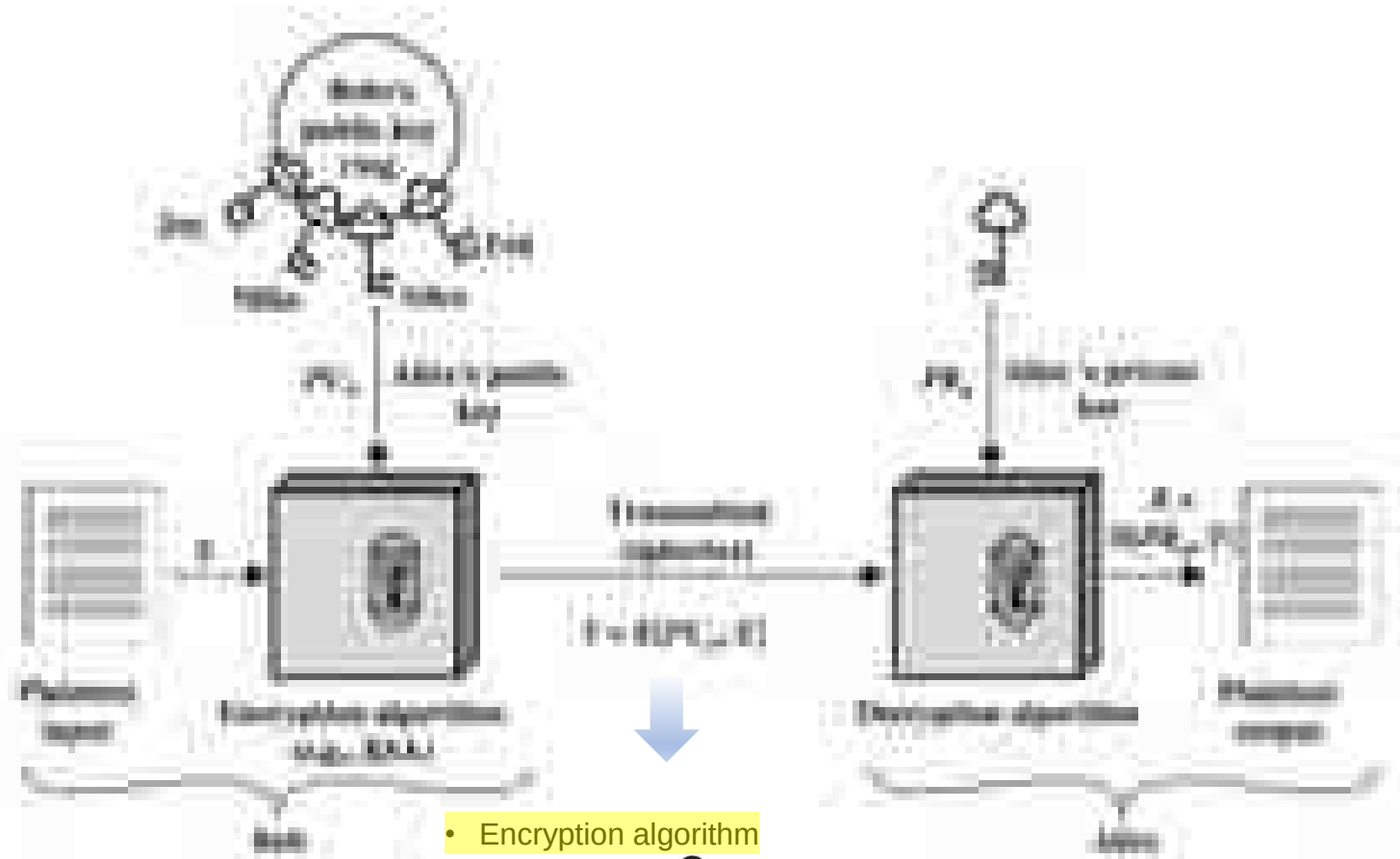
- Public-Key Cryptography was designed to address these concerns
- Public invention due to Whitfield Diffie & Martin Hellman
 - known earlier in classified community

- Probably most significant advancement in the history of cryptography
- Uses two keys – a public & a private key
- Asymmetric since different keys are used for encryption and decryption
- Uses clever application of number theoretic concepts to function
- This is not meant to replace Symmetric Encryption (private key crypto) but rather to complement...



Public-Key Cryptography

How public and private keys are used?



- Encryption algorithm
- Public Key
- Ciphertext

Private Key??
Plaintext??

Public-Key Cryptography

Example of public and private keys



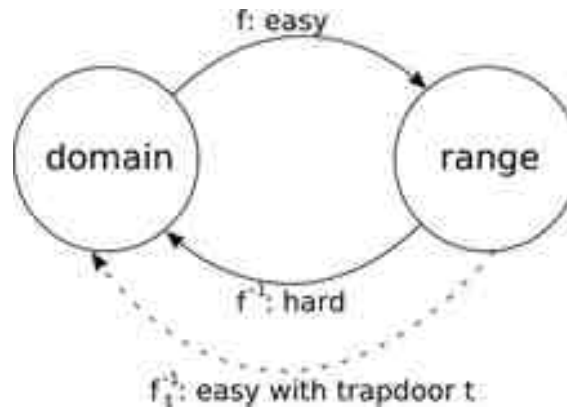
One-way Functions

Base for Modern Cryptography

One-way Functions

Base for Modern Cryptography

- A **one-way function** is “easy” to compute and “difficult” to reverse.



- The process of **exponentiation** means raising numbers to a power.
- Raising **2** to the power **3**, normally denoted 2^3 just means multiplying **2** by itself **3** times. In other words:
 - $2^3 = (2 \times 2 \times 2)$
 - $a^x = a \times a \times a \times \dots \times a$
- Modular exponentiation** means computing $a^x \bmod n$.
 - $a^x \bmod n$.
- In other words, given a number **a** and a prime number **n**, the function $f(x) = a^x \bmod n$ is a one-way function.

For $x=b$, we can easily compute $y=f(b)=a^b \bmod n$.
But its reverse is :(

For a particular $y=c$, it's difficult to get respective x such that $c=f(b)=a^x \bmod n$.

One-way Functions

Base for Modern Cryptography

Another Example

- It is easy to take two prime numbers and multiply them together.
- If the numbers are small, we can do this in our heads, on a piece of paper.
- What if numbers get bigger and bigger?
- Multiplication of two **big** prime numbers is **believed** to be a one-way function.
- Check Wikipedia for RSA Numbers
- https://en.wikipedia.org/wiki/RSA_numbers#:~:text=In%20mathematics%2C%20the%20RSA%20numbers,prime%20factors%20of%20each%20number.
- One of the modern asymmetric algorithm RSA is based on this idea

RSA Algorithm

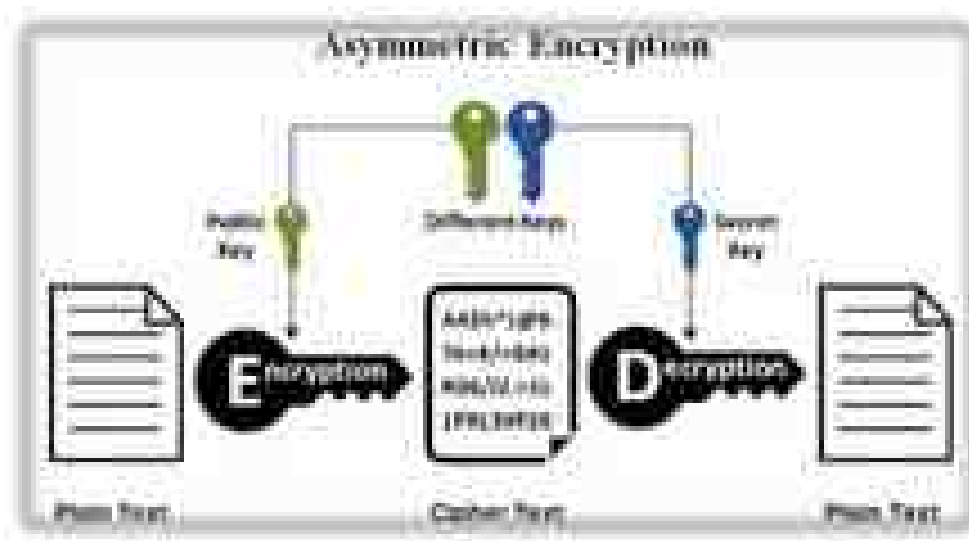
Asymmetric Encryption Algorithm

RSA Algorithm

Asymmetric Encryption Algorithm



- The **RSA** algorithm was the first practical implementation of public key encryption.
- It is named after the three researchers Ron Rivest, Adi Shamir and Len Adleman



RSA Algorithm

How the public and private keys are selected?

- Let **n** be the product of two large primes **p** and **q** (i.e. $n=p \times q$)
 - o at least 512 bits.
- Select a special number **e**
 - o greater than 1 and less than $(p-1)(q-1)$. The precise mathematical property that **e** must have is that there must be no numbers that divide neatly into **e** and into $(p-1)(q-1)$, except for 1.
- Publish the pair of numbers **(n,e)**
- Compute the private key **d** from **p**, **q** and **e**
- The private key **d** is computed to be the unique inverse of **e** modulo $(p-1)(q-1)$.
- In other words, **d** is the unique number less than $(p-1)(q-1)$ that when multiplied by **e** gives you 1 modulo $(p-1)(q-1)$.
 - o $ed = 1 \text{ mod } (p-1)(q-1)$

Public key: **(e, n)**
Private key: **(d, n)**

RSA Algorithm

How the message is encrypted and decrypted?

Encryption

Given a message M , $0 < M < n$ $M \in \mathbb{Z}_n - \{0\}$

use public key (e, n)

compute $C = M^e \bmod n$ $C \in \mathbb{Z}_n - \{0\}$

Decryption

Given a ciphertext C , use private key (d)

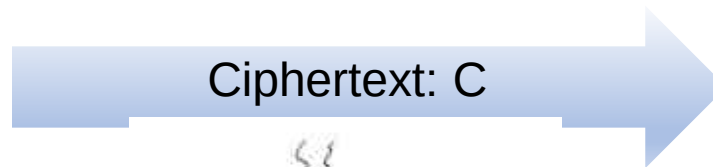
Compute $C^d \bmod n = (M^e \bmod n)^d \bmod n = M^{ed} \bmod n = M$

Sender Side

Plaintext: M

Encryption

$C = M^e \bmod (n=pq)$



Receiver Side

Ciphertext: C

Plaintext: $M = C^d \bmod n$



From n , difficult to figure out p, q

From (n, e) , difficult to figure d .

From (n, e) and C , difficult to figure out M s.t. $C = M^e$

RSA Algorithm

Can we see the public and private keys?

- Let **n** be the product of two large primes **p** and **q** (i.e. $n=pq$)
 - o at least 512 bits.
- Select a special number **e**
 - o greater than 1 and less than $(p-1)(q-1)$. The precise mathematical property that **e** must have is that there must be no numbers that divide neatly into **e** and into $(p-1)(q-1)$, except for 1.
- Publish the pair of numbers (**n**,**e**)
- Compute the private key **d** from **p**, **q** and **e**
- The private key **d** is computed to be the unique inverse of **e** modulo $(p-1)(q-1)$.
- In other words, **d** is the unique number less than $(p-1)(q-1)$ that when multiplied by **e** gives you 1 modulo $(p-1)(q-1)$.
 - o $ed = 1 \text{ mod } (p-1)(q-1)$

Public key: (**e**, **n**)
Private key: (**d**, **n**)

A Digital Certificate is an electronic file that is tied to a cryptographic key pair and authenticates the identity of a website, individual, organization, user, device or server. It is also known as a public key certificate or identity certificate.

<https://www.boxentriq.com/code-breaking/hex-to-decimal-converter>

RSA Algorithm - Working Example

Asymmetric Encryption Algorithm

RSA Algorithm Example

How are the public and private keys generated?

- Assume we have generated the RSA public-private key pair:
- Choose two “big” primes $p=11$ and $q=13$
- Compute the number $n = p \cdot q = 143$
- Number $e=? \in [1, (p-1)(q-1)] = [1, 120]$
 - Relative prime with $(p-1)(q-1)$
- $e=7$
- private exponent $d = ?$
 - $ed = 1 \bmod (p-1)(q-1)$
- $d=103$

Public key: (e, n)

Private key: (d, n)

- Let n be the product of two large primes p and q (i.e. $n=p \cdot q$)
 - o at least 512 bits.
 - Select a special number e
 - o greater than 1 and less than $(p-1)(q-1)$. The precise mathematical property that e must have is that there must be no numbers that divide neatly into e and into $(p-1)(q-1)$, except for 1.
 - Publish the pair of numbers (n, e)
 - Compute the private key d from p, q and e
 - The private key d is computed to be the unique inverse of e modulo $(p-1)(q-1)$.
 - In other words, d is the unique number less than $(p-1)(q-1)$ that when multiplied by e gives you 1 modulo $(p-1)(q-1)$.
 - o $ed = 1 \bmod (p-1)(q-1)$
- Public key:** (e, n)
Private key: (d, n)

RSA Algorithm Example

How the message is encrypted and decrypted?

- number **n** say 143
- **e=7**
- **d=103**

Public key: (e, n)
Private key: (d, n)

- Let's **encrypt** a secret message **msg = 83**

Encryption
 $C = M^e \bmod (n=pq)$

- Let's now try **decryption** of the secret message **C=8**

Plaintext: $M = C^d \bmod n$

Diffie-Hellman Key Exchange Protocol

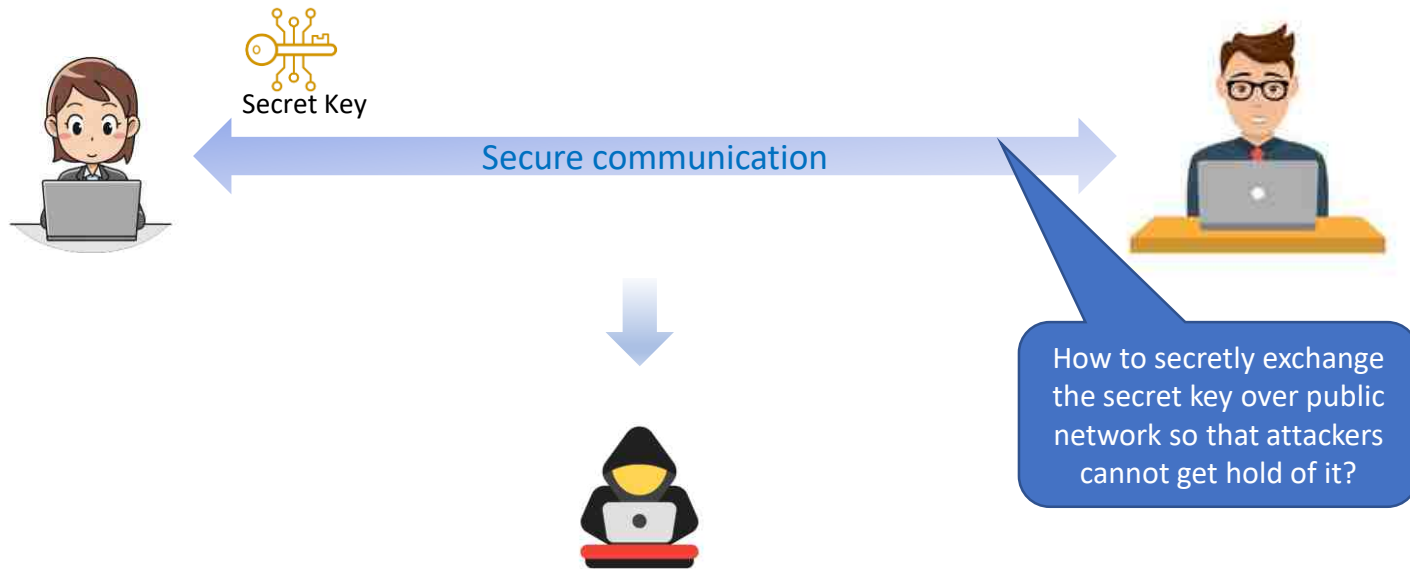
For Secure Key Exchange

Diffie-Hellman Key Exchange Protocol

For Secure Key Exchange

Two major issues with symmetric encryptions algorithms:

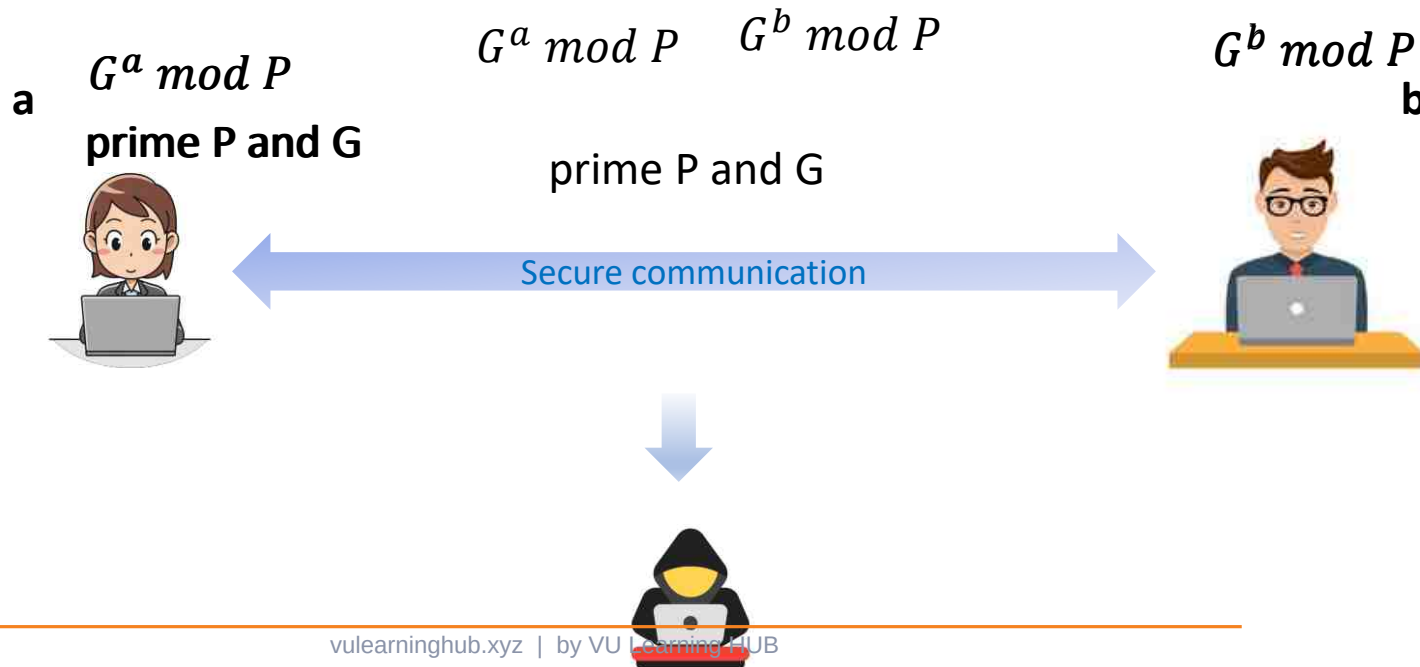
- **key distribution** – how to have secure key exchange among communicating parties
- **digital signatures** – how to verify a message comes intact from the claimed sender



Diffie-Hellman Key Exchange Protocol

How Keys are secretly exchanged?

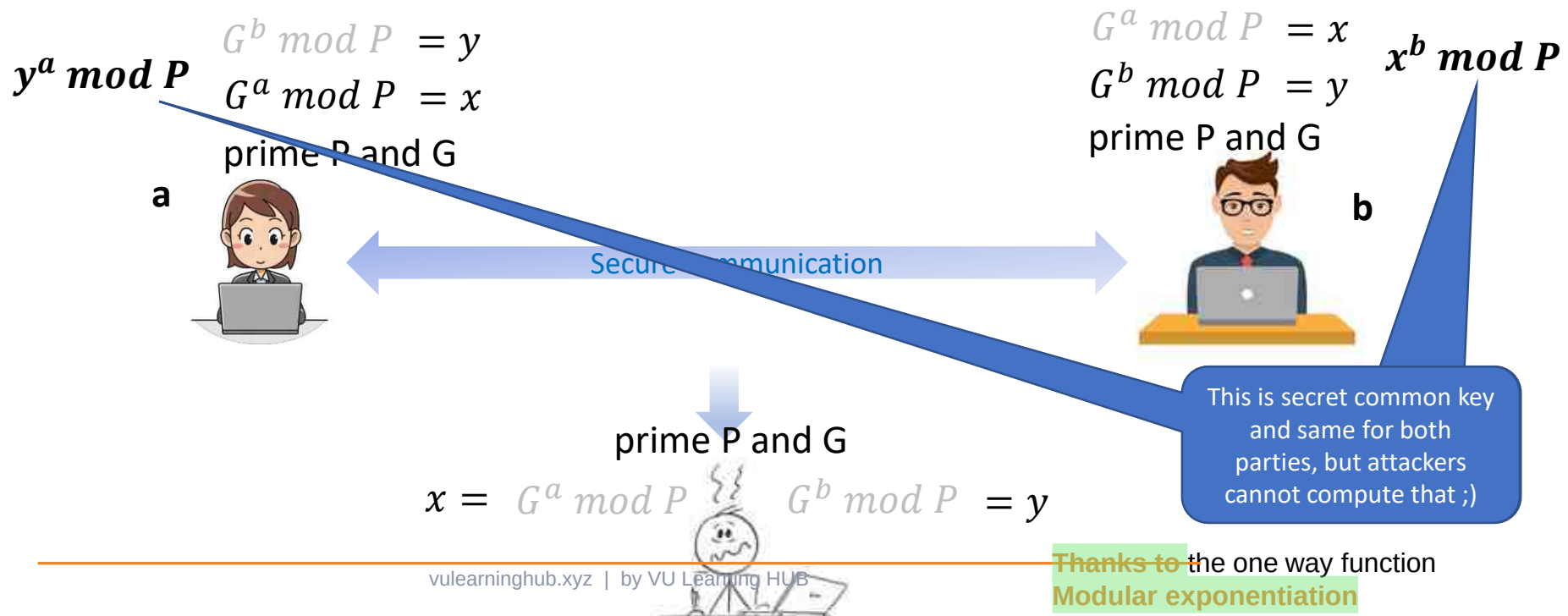
- Lets see, how two users can secretly exchange the key in presence of attacker
- Either party can choose one prime P and G (a primitive root of P) and exchange with the other...attacker can also see that
- Next, each party choose their private values
 - lets say, user-1 choose "**a**" and user-2 choose "**b**".
- Afterwards, both parties compute a number $G^x \bmod P$ and send it to the other
- Finally, both parties can generate the common secret key



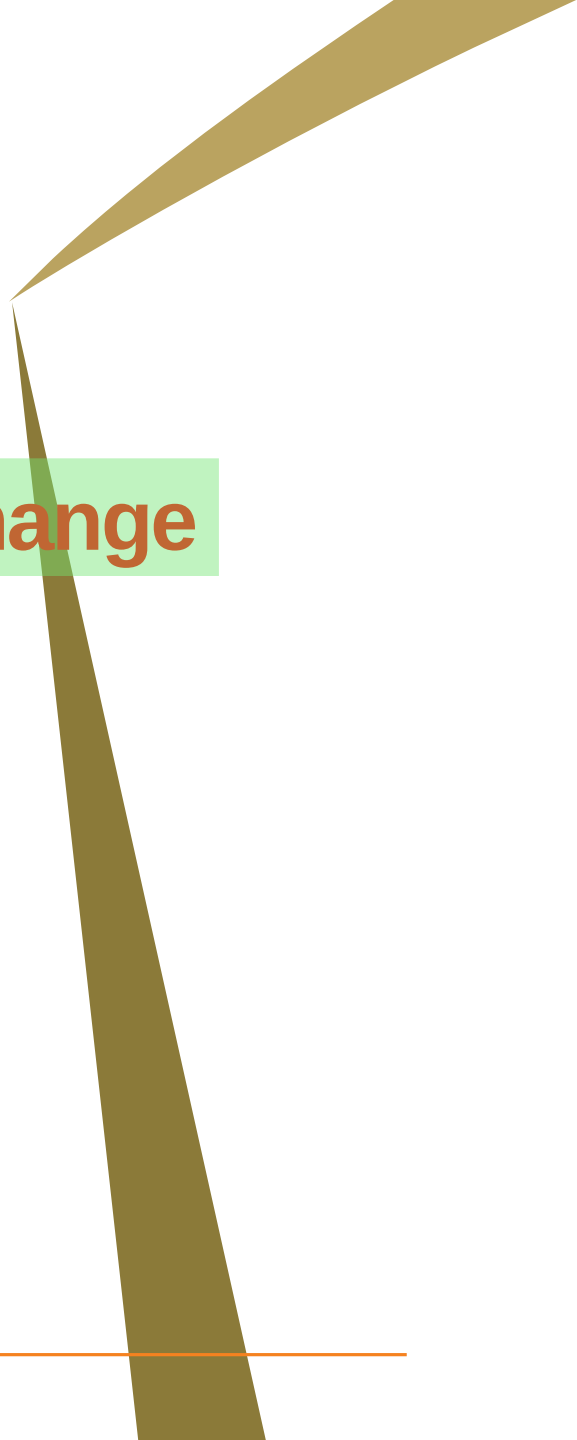
Diffie-Hellman Key Exchange Protocol

How Keys are secretly exchanged?

- Lets see, how two users can secretly exchange the key in presence of attacker
- Either party can choose one prime P and G (a primitive root of P) and exchange with the other...attacker can also see that
- Next, each party choose their private values
 - lets say, user-1 choose " a " and user-2 choose " b ".
- Afterwards, both parties compute a number $G^x \bmod P$ and send it to the other
- Finally, both parties can generate the common secret key



Thanks to the one way function
Modular exponentiation



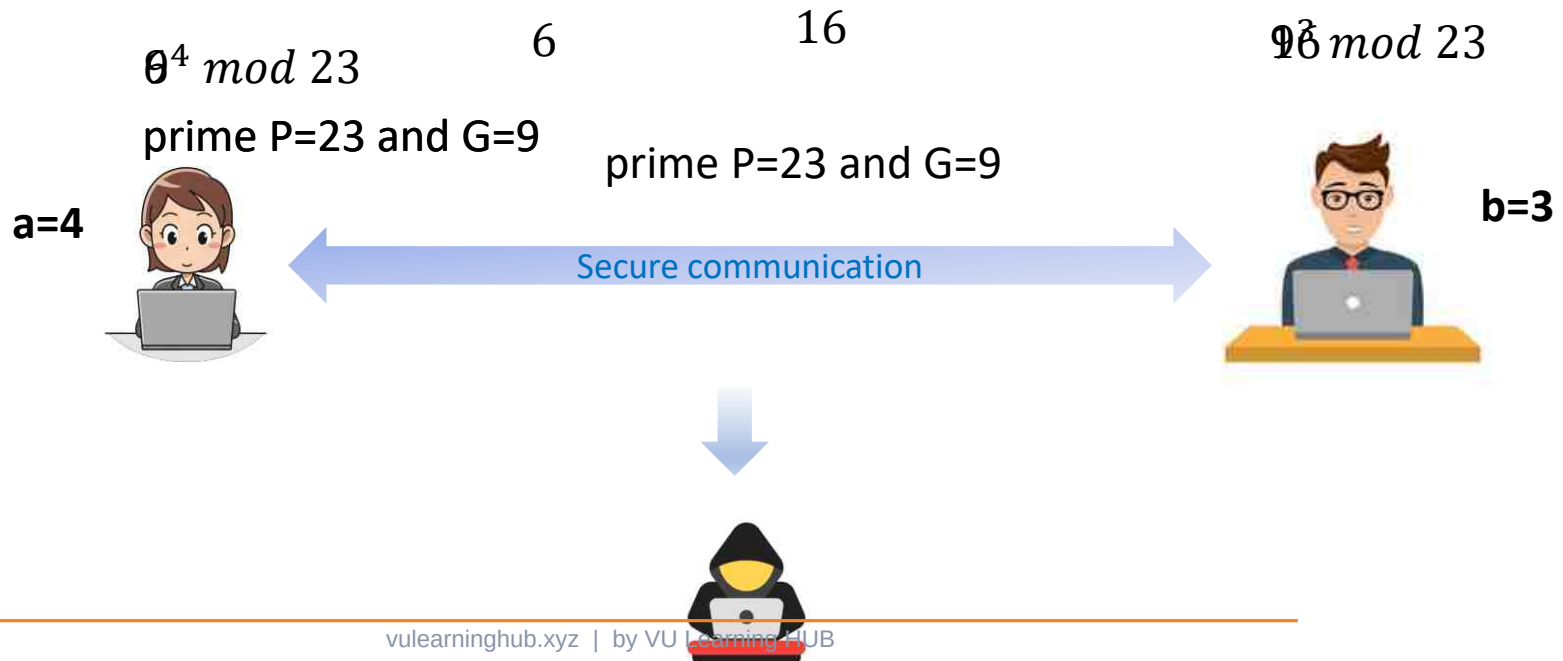
Diffie-Hellman Key Exchange Working Example

Secure Key Exchange

Diffie-Hellman Key Exchange - Example

How Keys are secretly exchanged?

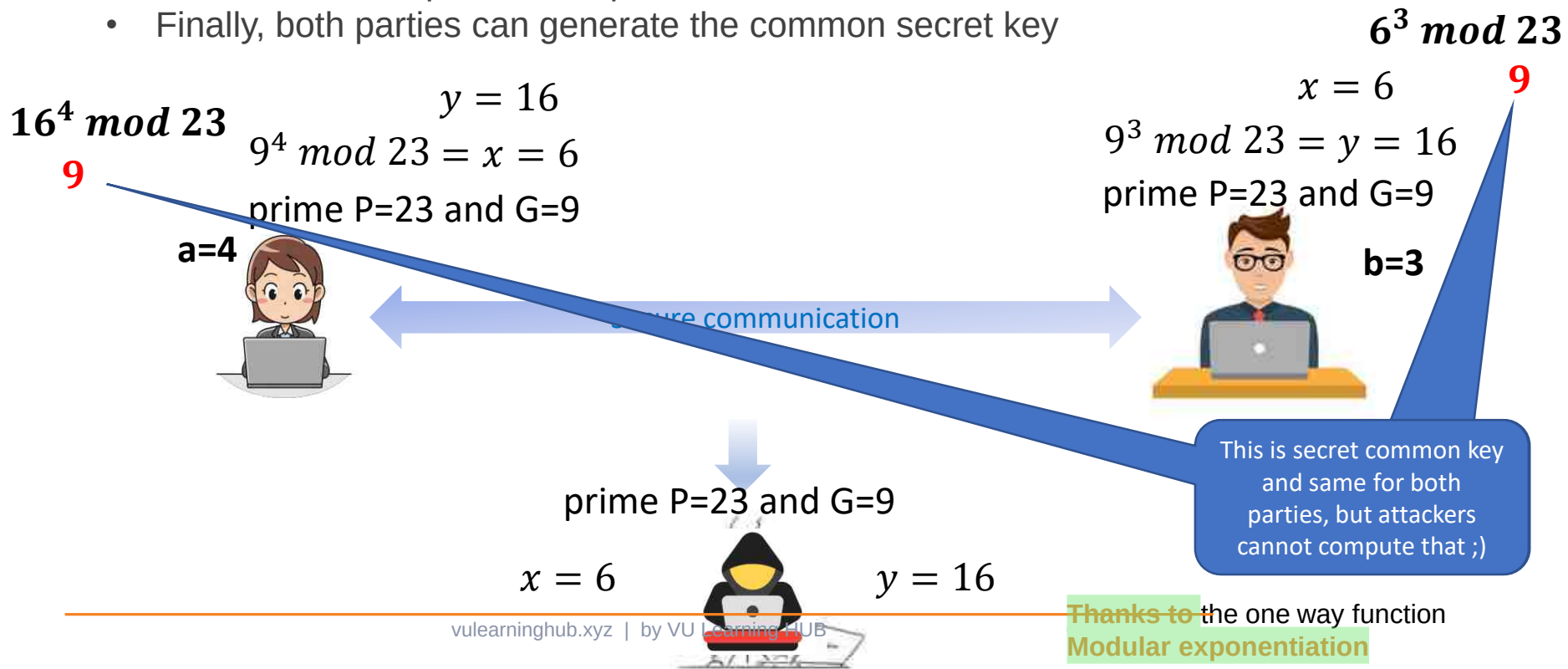
- Lets see, how two users can secretly exchange the key in presence of attacker
- Either party can choose one prime $P=23$ and $G=9$ (a primitive root of P) and exchange with the other...attacker can also see that
- Next, each party choose their private values
 - lets say, user-1 choose "**a=4**" and user-2 choose "**b=3**".
- Afterwards, both parties compute a number $G^x \bmod P$ and send it to the other
- Finally, both parties can generate the common secret key



Diffie-Hellman Key Exchange - Example

How Keys are secretly exchanged?

- Lets see, how two users can secretly exchange the key in presence of attacker
- Either party can choose one prime P and G (a primitive root of P) and exchange with the other...attacker can also see that
- Next, each party choose their private values
 - lets say, user-1 choose "a" and user-2 choose "b".
- Afterwards, both parties compute a number $G^x \bmod P$ and send it to the other
- Finally, both parties can generate the common secret key



Security Issue in the Diffie-Hellman

Can we trust the Diffie-Hellman Algorithm?

Security Issue in the Diffie-Hellman

Can we trust the Diffie-Hellman Algorithm for secure Key exchange?

- Diffie-Hellman Algorithm is safe against sniffing attack...interception



- But what if attacker sits in the middle?



Network Devices

Introduction

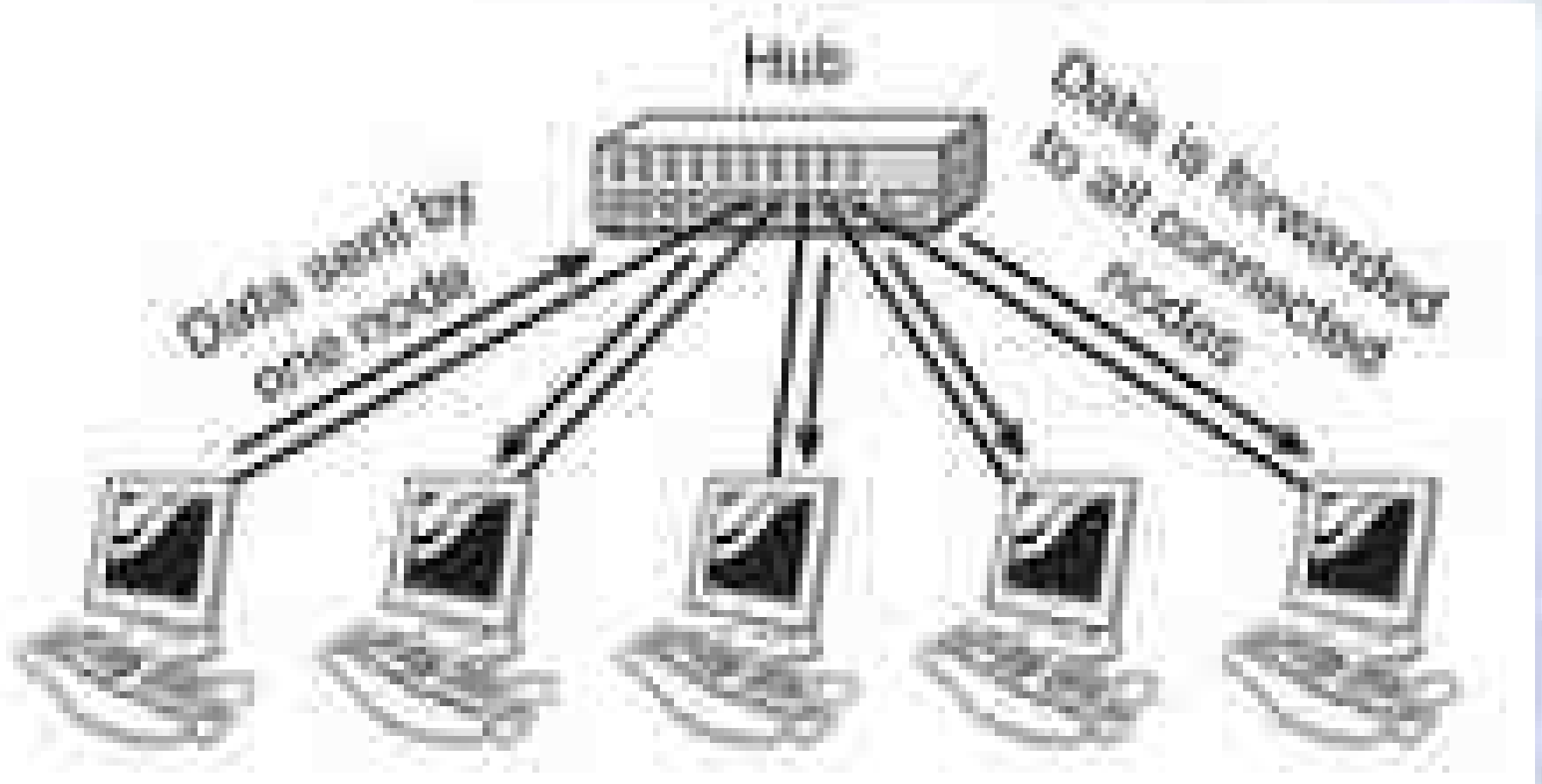
- In this topic we will cover the basics of network devices and their functions.
- We will discuss different types of network devices, including routers, switches, firewalls, and more.

Hub

- A network hub is a device that broadcasts data to every computer or Ethernet-based device connected to it.
- Network hubs are best suited for small, simple local area network (LAN) environments.



Working of Hub

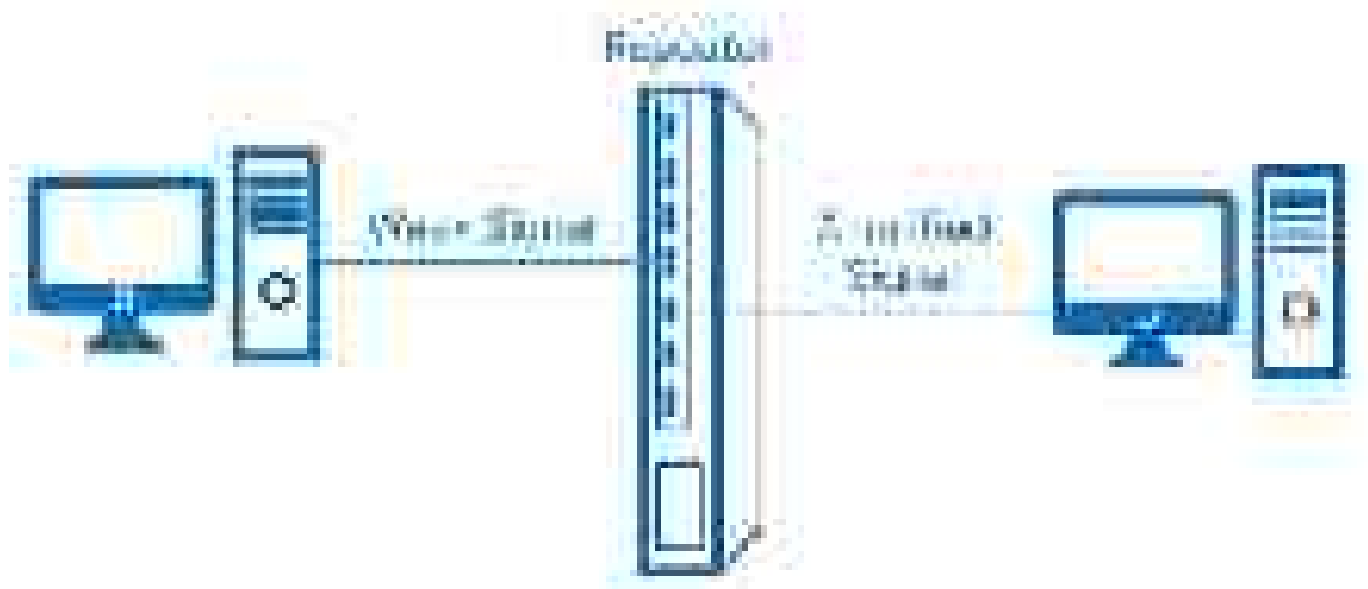


Repeater

- Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it.
- They are incorporated in networks to expand its coverage area. They are also known as signal boosters.



Working of Repeater

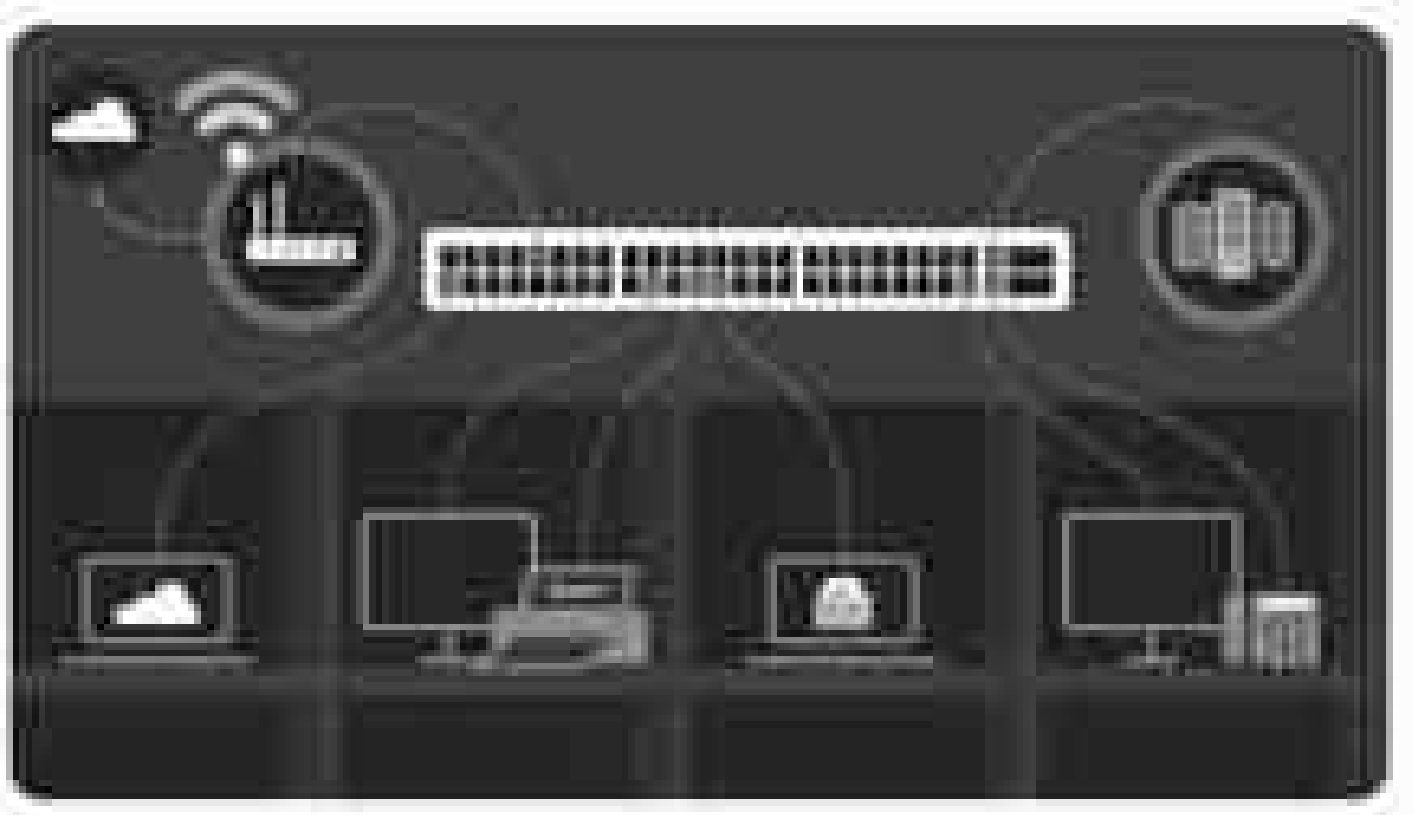


Switch

- A switch is a network device that connects devices on a local area network (LAN).
- It operates at the data link layer of the OSI model and uses MAC addresses to direct traffic to the appropriate device.

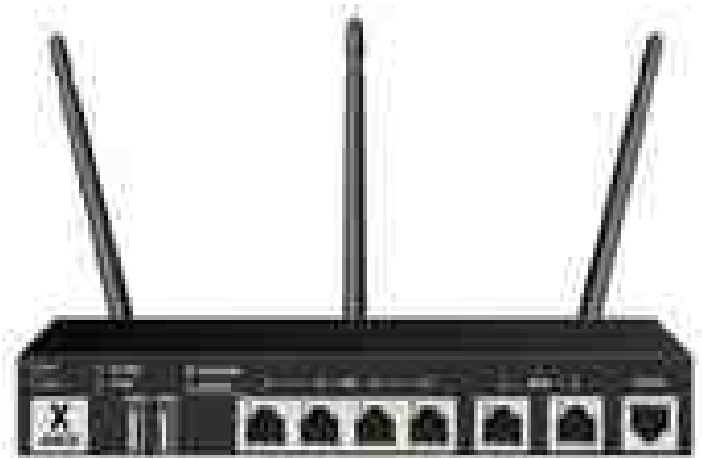


Switch's working

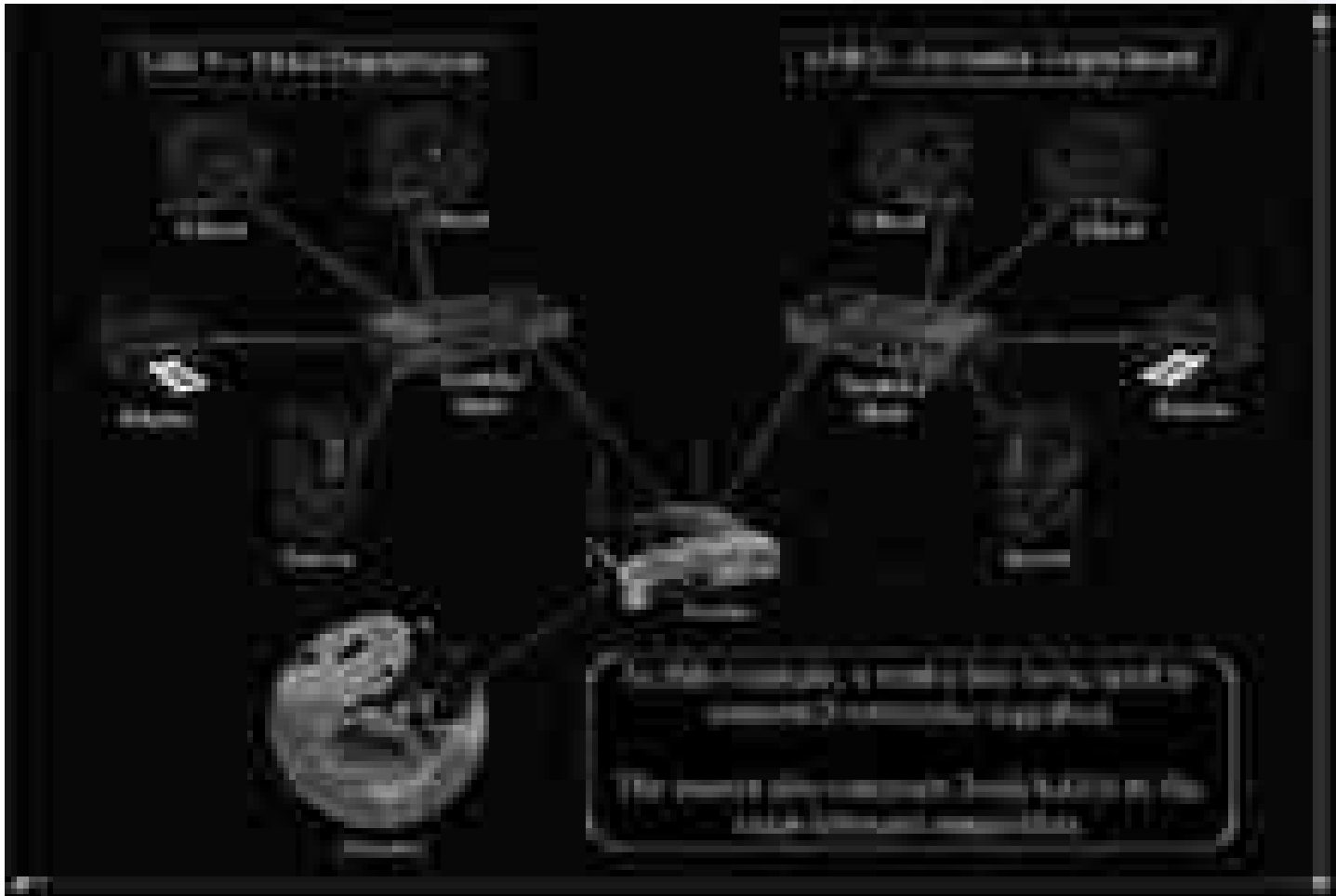


Routers

- A router is a network device that connects multiple networks and routes traffic between them.
- It operates at the network layer of the OSI model and uses routing tables to determine the best path for data to travel.



Router's working



Firewalls

- A firewall is a network security device that monitors and controls incoming and outgoing network traffic.
- It can block unauthorized access to a network and prevent malicious traffic from entering or leaving the network.

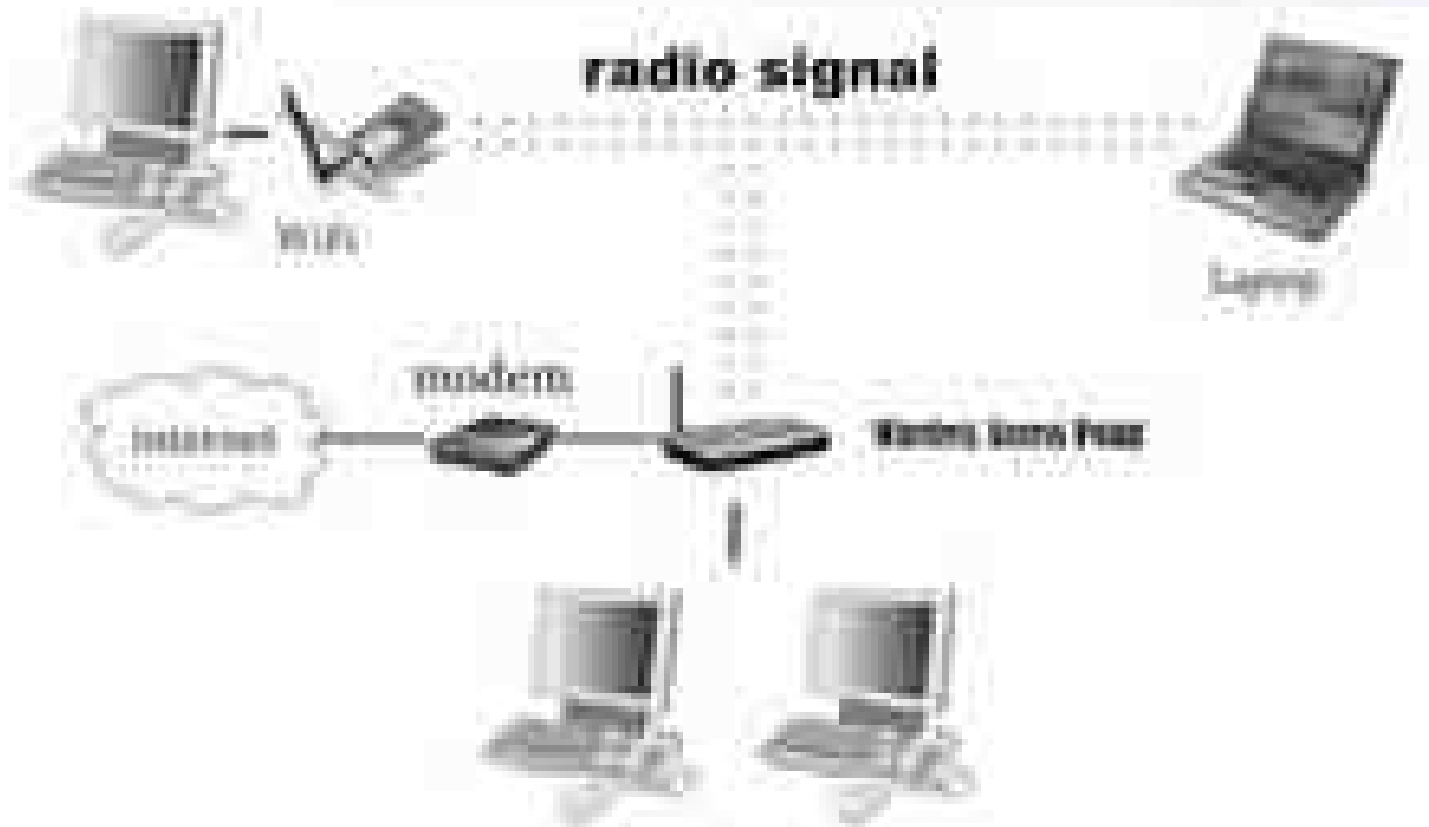


Wireless Access Points

- A wireless access point (WAP) is a network device that allows wireless devices to connect to a wired network.
- It provides a wireless signal for devices to connect to and can support multiple wireless devices simultaneously.



Wireless Access Point's working

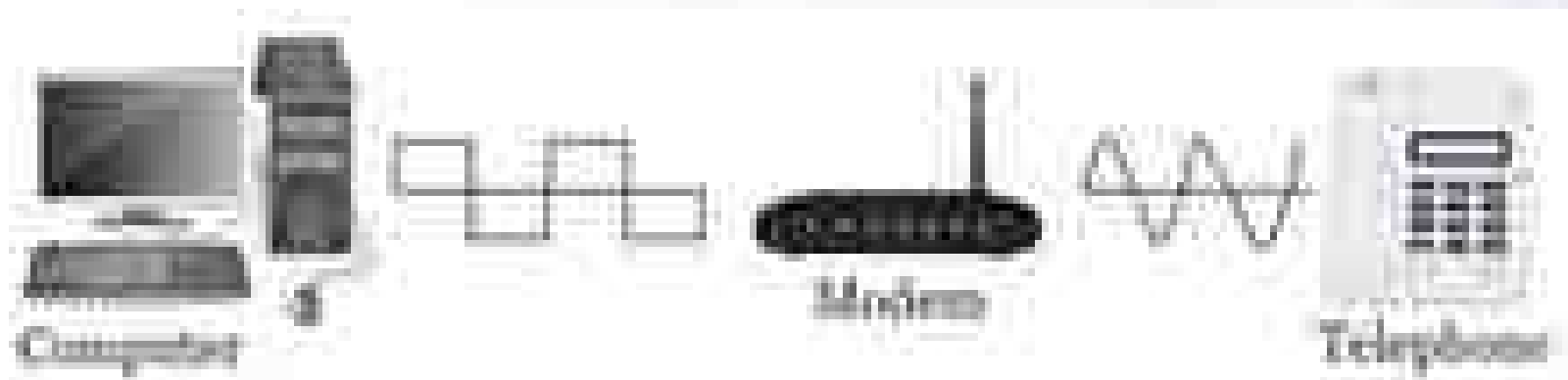


Modems

- A modem is a network device that modulates and demodulates signals between a computer and the internet service provider (ISP).
- It converts digital signals from a computer into analog signals that can travel over phone lines or cable lines, and vice versa.



Working of Modem

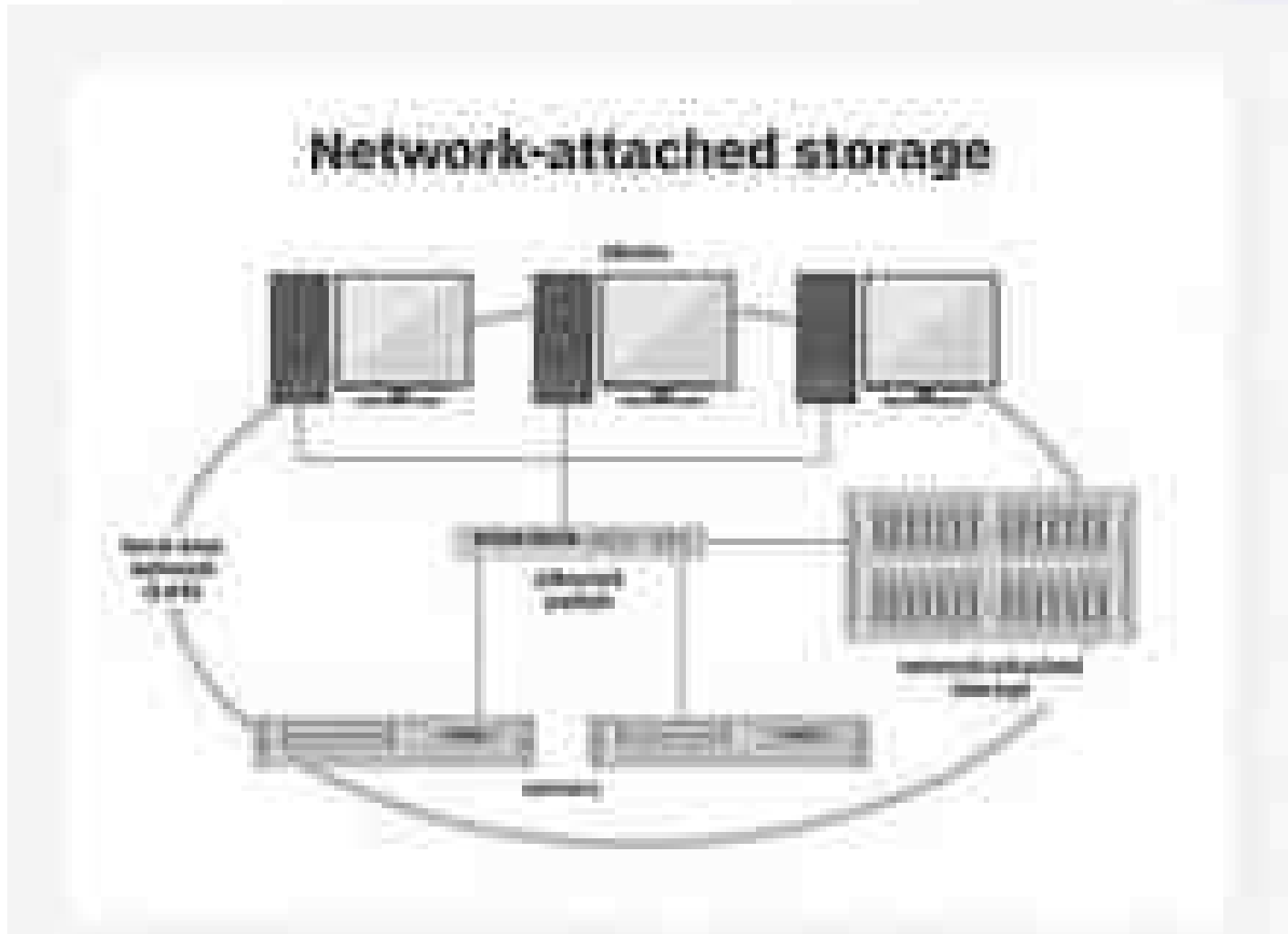


Network Attached Storage (NAS)

- **Network Attached Storage (NAS)** is a network device that allows multiple devices to share and access files from a central location.
- **It can provide data redundancy, backup, and storage capabilities for a network.**



Network Attached Storage working



Conclusion

- In conclusion, network devices are essential components of a computer network.
- Understanding the functions and capabilities of each device can help network administrators design, configure, and maintain a secure and efficient network infrastructure.

Perimeter Security

Introduction

- In this topic we will cover the basics of perimeter security and its importance in protecting a network.
- We will discuss different types of perimeter security, including physical and logical measures.

Physical Perimeter Security

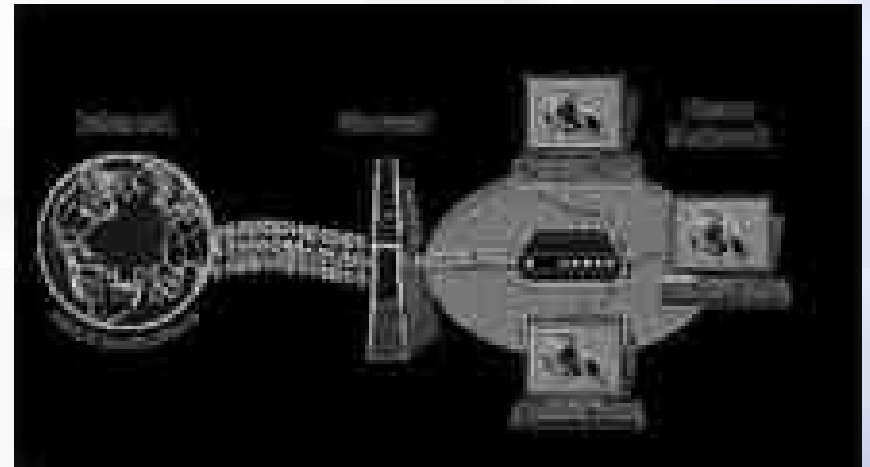
- Physical perimeter security includes measures such as fences, gates, walls, and security cameras.
- These measures restrict access to a physical location and can prevent unauthorized entry.

Logical Perimeter Security

- Logical perimeter security includes measures such as firewalls, intrusion detection systems, and virtual private networks (VPNs).
- These measures control access to a network and can prevent unauthorized access.

Firewalls

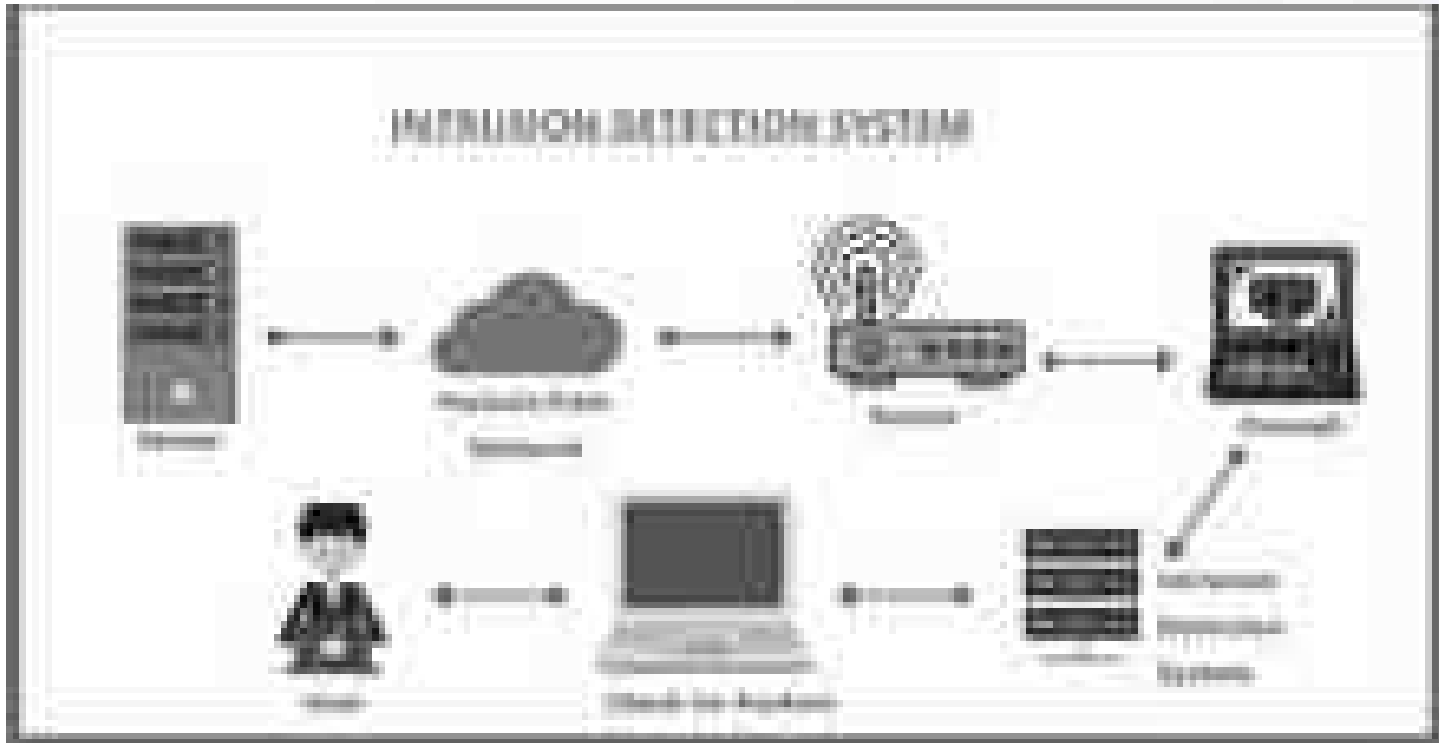
- A firewall is a logical perimeter security device that monitors and controls incoming and outgoing network traffic.
- It can block unauthorized access to a network and prevent malicious traffic from entering or leaving the network.



Intrusion Detection Systems (IDS)

- An intrusion detection system (IDS) is a logical perimeter security device that monitors a network for suspicious activity.
- It can detect and alert network administrators of potential security breaches.

Working of Intrusion Detection Systems (IDS)

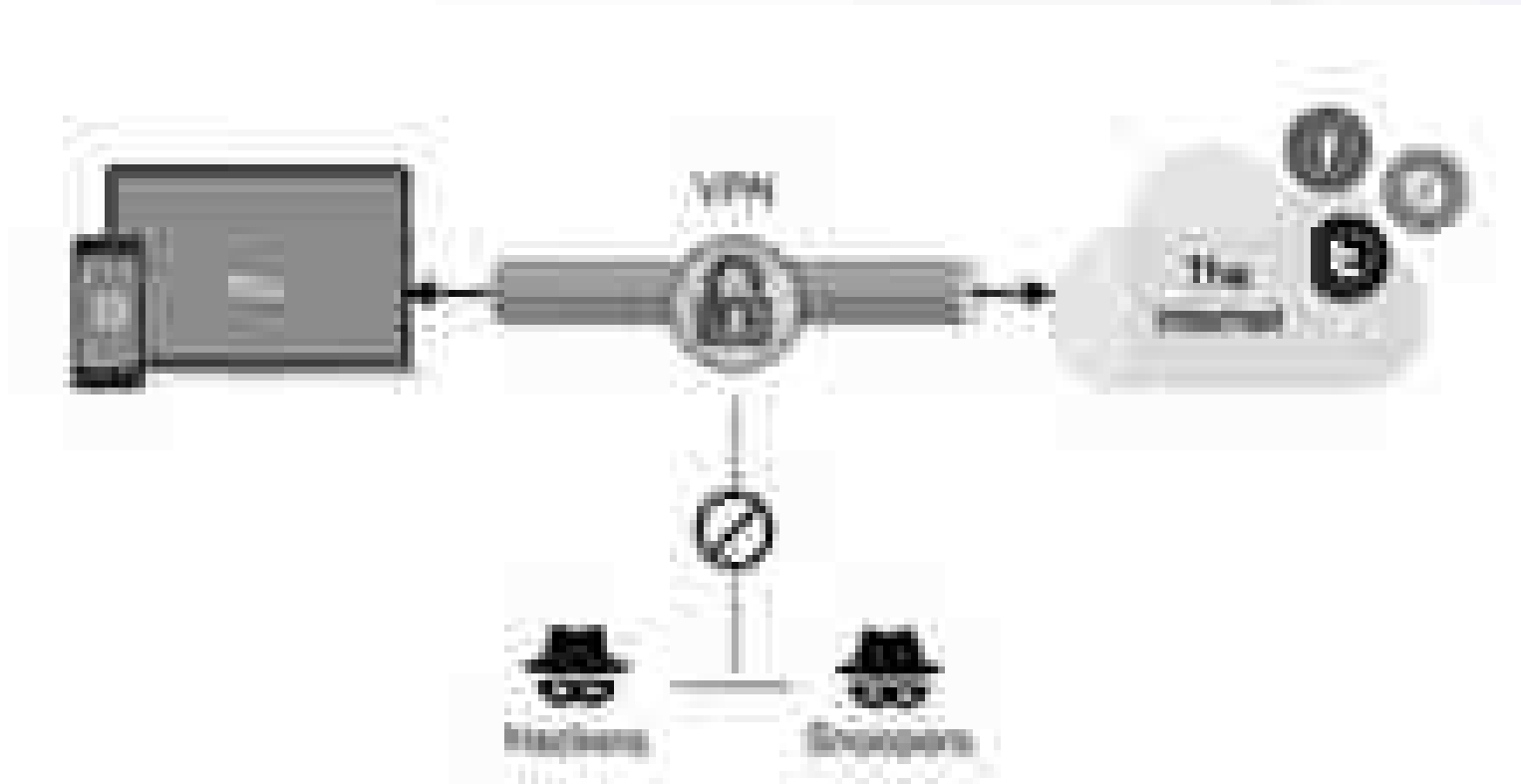


Virtual Private Networks (VPNs)

- A virtual private network (VPN) is a logical perimeter security measure that allows remote users to securely connect to a network.
- It encrypts traffic between the remote user and the network, providing secure access to network resources.



Working of VPN



Access Control

- Access control is a logical perimeter security measure that restricts access to network resources based on user credentials and permissions.
- It ensures that only authorized users have access to sensitive information.

Access Control List



Conclusion

- In conclusion, perimeter security is a critical component of network security.
- Physical and logical measures can be used to protect a network from unauthorized access and malicious attacks.
- Understanding the various types of perimeter security measures and their functions can help network administrators design, configure, and maintain a secure network infrastructure.

What is an intrusion?

Introduction

- In this topic we will cover the basics of intrusion and its impact on a network.
- We will discuss what an intrusion is, types of intrusions, and how to prevent them.

What is an intrusion?

- An intrusion is an unauthorized attempt to access, use, or modify a network, system, or device.
- It can occur through various means, including malware, phishing attacks, and brute-force attacks.

Types of Intrusions

There are different types of intrusions, including:

- **External Intrusion:** when an attacker attempts to gain access to a network from outside.
- **Internal Intrusion:** when an attacker gains access to a network from within, such as an employee with malicious intent.
- **Insider Threat:** when an employee or contractor intentionally or unintentionally causes harm to a network.
- **Distributed Denial of Service (DDoS):** when an attacker floods a network with traffic to disrupt normal operations.

Impact of Intrusions

Intrusions can have severe impacts on a network, including:

- ☐ Data theft or loss
- ☐ Financial loss
- ☐ Reputation damage
- ☐ Disruption of operations

Prevention Measures

To prevent intrusions, organizations can implement various measures, including:

- Firewalls and intrusion detection/prevention systems
- Regular software updates and patching
- Strong password policies
- Employee training on phishing and social engineering attacks
- Access control policies

Incident Response

- Despite preventative measures, intrusions can still occur.
- Organizations should have an incident response plan in place to quickly and effectively respond to a security breach.

Conclusion

- In conclusion, intrusions are unauthorized attempts to access, use, or modify a network, system, or device.
- They can have severe impacts on an organization, but prevention measures and incident response plans can help mitigate the risks.

Examples of Intrusion

Introduction

- In this topic we will cover some common examples of intrusions.
- We will discuss the types of attacks used in each example and the impact on the affected network.

Malware Infection

- Malware is a type of software designed to harm a computer system or network.
- Examples of malware include viruses, worms, and Trojan horses.
- A malware infection can result in stolen data, financial loss, and network downtime.



Phishing Attacks

- Phishing attacks are attempts to trick individuals into revealing sensitive information.
- Attackers often use email or social media to deceive victims into clicking a malicious link or providing personal information.
- A successful phishing attack can result in stolen login credentials or sensitive data.



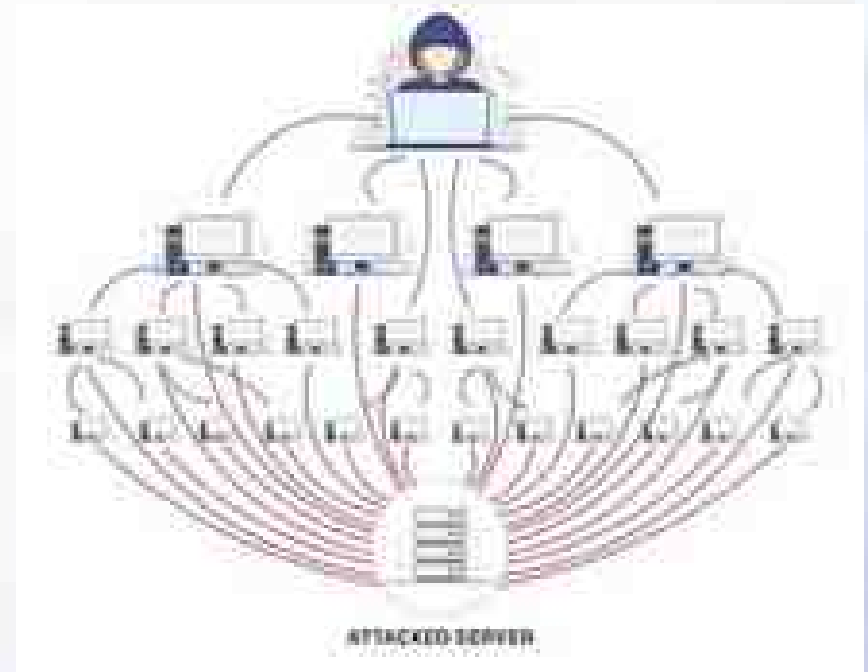
Brute-Force Attacks

- A brute-force attack is an attempt to gain unauthorized access to a system or network by guessing passwords.
- Attackers use automated tools to try multiple password combinations until they find the correct one.
- A successful brute-force attack can result in unauthorized access to sensitive data.



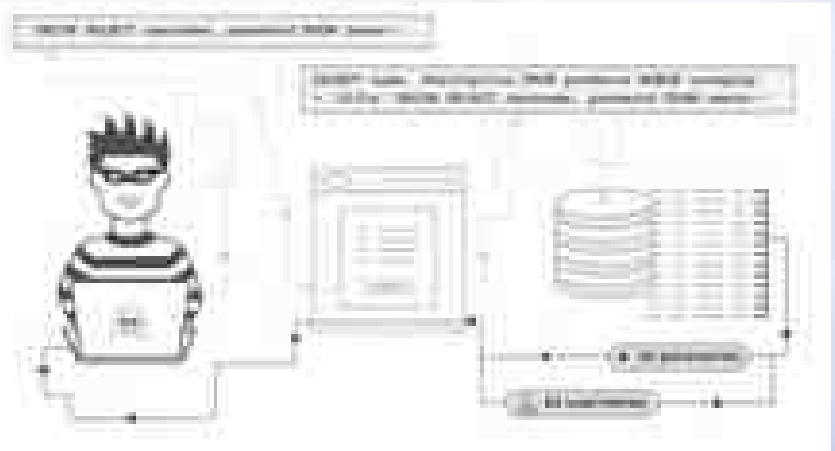
Distributed Denial of Service (DDoS)

- A DDoS attack is an attempt to disrupt normal network operations by overwhelming the network with traffic.
- Attackers use a botnet, a group of compromised devices, to flood the network with traffic.
- A successful DDoS attack can result in network downtime and financial loss.



SQL Injection

- An SQL injection is an attack that targets the database of a web application.
- Attackers input malicious SQL code into a web form to access or modify sensitive information stored in the database.
- A successful SQL injection can result in unauthorized access to sensitive data.



Conclusion

- In conclusion, there are various examples of intrusions that can impact a network.
- Attackers use different types of attacks, including malware infections, phishing attacks, brute-force attacks, DDoS attacks, and SQL injections.
- Organizations must implement strong security measures, such as firewalls, intrusion detection systems, and access control policies, to prevent and mitigate the impact of intrusions.

Intruder Behavior

Introduction

- In this topic we will cover intruder behavior and how it can impact a network.
- We will discuss the different types of intruders and their motivations for attacking a network.

Types of Intruders

There are different types of intruders, including:

Script Kiddies: inexperienced attackers who use pre-written scripts to launch attacks.

- **Hacktivists:** attackers who target a network to promote a political or social cause.
- **Insiders:** employees or contractors who intentionally or unintentionally cause harm to a network.
- **Cybercriminals:** attackers who target a network for financial gain.
- **Nation-state Actors:** attackers who are sponsored by a government to gain access to sensitive information.

Motivations for Intruder Behavior

Intruders may have various motivations for attacking a network, including:

- Financial gain
- Political or social reasons
- Espionage
- Personal challenge
- Revenge

Intruder Methods

Intruders use various methods to gain access to a network, including:

- Exploiting vulnerabilities in software or hardware
- Social engineering, such as phishing attacks
- Brute-force attacks
- Distributed denial of service (DDoS) attacks
- Insider threats

Impact of Intruder Behavior

Intruder behavior can have severe impacts on a network, including:

- Data loss or theft
- Financial loss
- Reputation damage
- Disruption of operations
- Legal consequences

Prevention and Mitigation

To prevent and mitigate the impact of intruder behavior, organizations can implement various measures, including:

- [?] Strong passwords and access control policies
- [?] Regular software updates and patching
- [?] Employee training on social engineering attacks
- [?] Firewalls and intrusion detection/prevention systems
- [?] Incident response plans

Conclusion

- In conclusion, intruder behavior can have severe impacts on a network, and there are different types of intruders with varying motivations for attacking a network.
- Organizations must implement strong security measures to prevent and mitigate the impact of intruder behavior, including strong passwords, access control policies, regular software updates, employee training, and incident response plans.

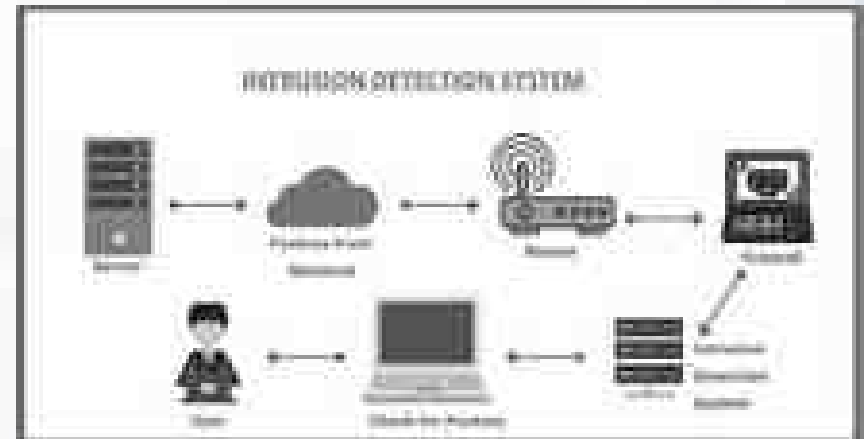
Intrusion Detection System (IDS)

Introduction

- In this topic we will cover Intrusion Detection System (IDS) and its importance in network security.
- We will discuss the types of IDS and how they work to detect intrusions.

What is an IDS?

- An IDS is a security tool designed to detect and alert on malicious activity on a network.
- IDS can detect unauthorized access, malware infections, phishing attacks, and other types of intrusions.



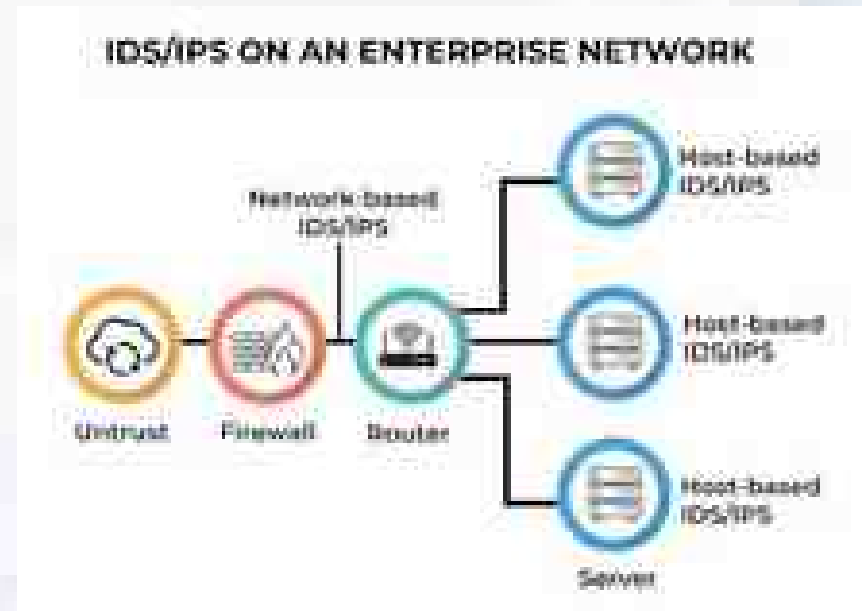
Types of IDS

There are two types of IDS:

- **Network-based IDS (NIDS):** These monitor network traffic for suspicious activity, such as unusual traffic patterns or known attack signatures.
- **Host-based IDS (HIDS):** These monitor activity on individual devices, such as servers or workstations, to detect unauthorized access or system-level attacks.

How IDS Works?

- IDS works by comparing network traffic or system activity against known attack signatures, behavior patterns, or other indicators of compromise (IoCs).
- IDS can detect intrusions by analyzing packet headers and payloads, system logs, and other data sources.
- IDS alerts security teams or generates automated responses, such as blocking traffic or quarantining affected devices.



Benefits of IDS

IDS provides several benefits, including:

- Early detection and alerting of intrusions, reducing the impact of an attack.
- Faster incident response by identifying the affected devices and the scope of the attack.
- Improved visibility into network traffic and activity, allowing security teams to identify vulnerabilities and potential attack vectors.

Limitations of IDS

IDS has some limitations, including:

- IDS may generate false positives or false negatives, leading to unnecessary alerts or missed intrusions.
- IDS requires maintenance and updates to stay current with the latest attack signatures and IoCs.
- IDS may not detect new or unknown attack vectors.

Conclusion

- In conclusion, IDS is an important tool in network security that can detect and alert on intrusions, reducing the impact of an attack.
- Organizations must choose the right type of IDS, NIDS or HIDS, based on their network architecture and security needs.
- IDS has limitations, and organizations must implement complementary security measures, such as firewalls, access control, and endpoint security, to achieve a comprehensive security posture.

IDS Analysis Approaches

Introduction

- In this topic we will cover IDS analysis approaches and how they can be used to detect and respond to network intrusions.
- We will discuss the different types of IDS analysis approaches and how they work.

Types of IDS Analysis Approaches

There are three main types of IDS analysis approaches:

- Signature-based analysis
- Anomaly-based analysis
- Hybrid analysis

Signature-based Analysis

- Signature-based analysis compares network traffic against known attack signatures or patterns.
- IDS with signature-based analysis can identify known attacks with high accuracy but may miss new or unknown attacks.
- Signature-based analysis requires regular updates to stay current with new attack signatures.

Anomaly-based Analysis

- Anomaly-based analysis detects deviations from normal network traffic or user behavior.
- IDS with anomaly-based analysis can identify new or unknown attacks but may generate more false positives than signature-based analysis.
- Anomaly-based analysis requires a baseline of normal network traffic or user behavior to be established and updated regularly.

Hybrid Analysis

- Hybrid analysis combines signature-based and anomaly-based analysis to achieve a more comprehensive detection capability.
- IDS with hybrid analysis can identify known and unknown attacks with fewer false positives but require more resources to operate effectively.

IDS Analysis Approaches in Action

IDS analysis approaches can be applied to detect various types of network intrusions, including:

- Malware infections
- Unauthorized access attempts
- Data exfiltration
- Denial of service attacks

Conclusion

- In conclusion, IDS analysis approaches are essential for detecting and responding to network intrusions effectively.
- Organizations must choose the right type of IDS analysis approach based on their network architecture and security needs.
- IDS analysis approaches require regular maintenance, updates, and baseline establishment to operate effectively.

Host-Based IDS

Introduction

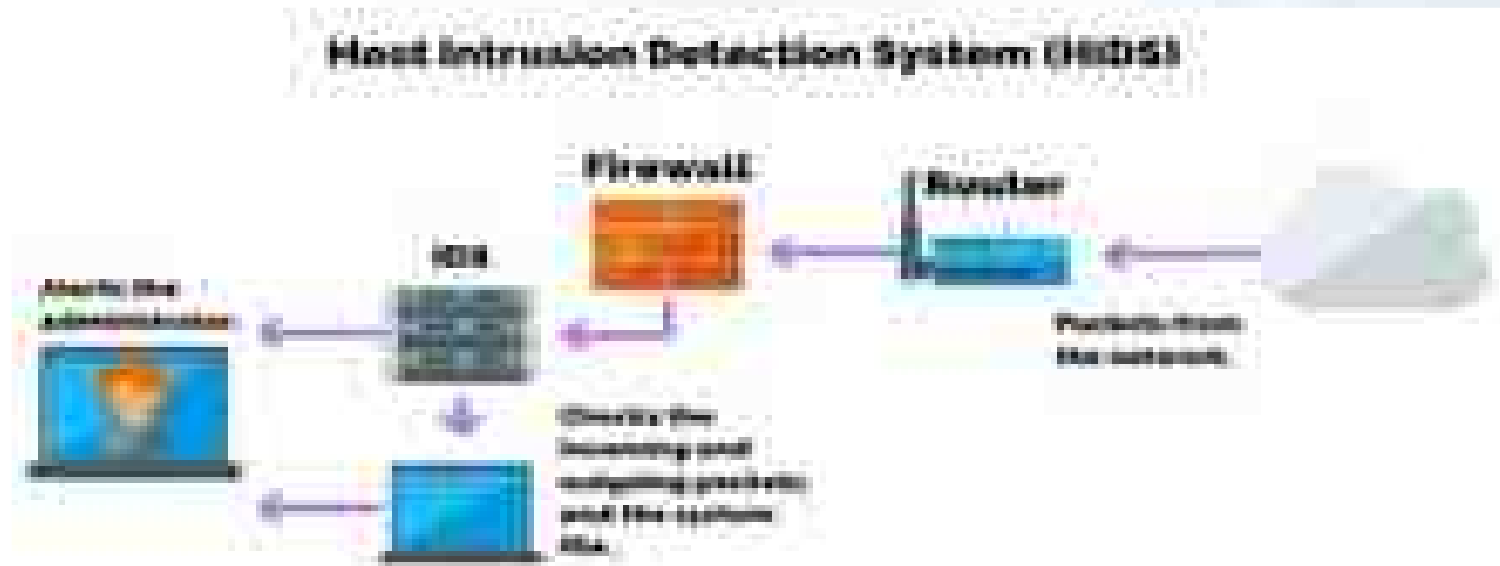
- In this topic we will cover Host-Based Intrusion Detection System (HIDS) and its importance in host-level security.
- We will discuss how HIDS works and its benefits and limitations.

What is HIDS?

- HIDS is an intrusion detection system that monitors activity on individual devices, such as servers or workstations, to detect unauthorized access or system-level attacks.
- HIDS can detect malicious activity that network-based IDS (NIDS) may not capture, such as file modifications or process-level attacks.

How HIDS Works?

- HIDS works by collecting and analyzing system activity logs, file integrity, and system performance metrics to identify suspicious activity.
- HIDS can detect unauthorized access attempts, malware infections, and other types of host-level attacks.
- HIDS alerts security teams or generates automated responses, such as terminating malicious processes or isolating affected devices.



Benefits of HIDS

HIDS provides several benefits, including:

- Granular visibility into host-level activity, allowing for faster incident response and reducing the impact of an attack.
- Detecting threats that may evade NIDS, such as fileless malware or process-level attacks.
- Enhancing compliance by monitoring and reporting on system-level activity.

Limitations of HIDS

HIDS has some limitations, including:

- HIDS can generate a high number of alerts, leading to alert fatigue and missed intrusions.
- HIDS requires maintenance and updates to stay current with the latest attack patterns and IoCs.
- HIDS may not detect sophisticated or zero-day attacks.

HIDS Deployment

HIDS can be deployed in several ways, including:

- **Agent-based:** HIDS agent installed on each monitored device.
- **Agentless:** HIDS uses system logs and network packets for analysis.
- **Hybrid:** HIDS uses a combination of agent-based and agentless approaches.

Conclusion

- In conclusion, HIDS is an essential tool in host-level security that can detect and alert on intrusions, reducing the impact of an attack. 
- Organizations must choose the right type of HIDS deployment based on their network architecture and security needs.
- HIDS has limitations, and organizations must implement complementary security measures, such as firewalls, access control, and endpoint security, to achieve a comprehensive security posture.

Network-Based IDS

Introduction

- Network-based Intrusion Detection Systems (NIDS) are security tools that monitor and analyze network traffic to detect suspicious activity or malicious attacks.
- NIDS is one of the most important security measures in modern-day networks.
- NIDS provides a higher level of security by detecting and alerting the network administrator of potential threats.



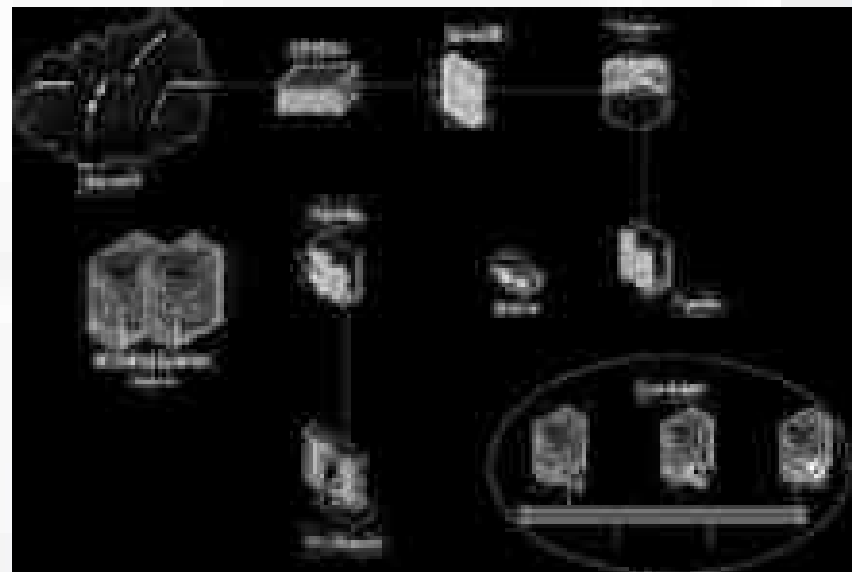
Types of NIDS

- **Signature-based NIDS:** Uses a pre-defined database of known attack patterns, and alerts when a network packet matches a signature in the database.
- **Anomaly-based NIDS:** Analyzes the network traffic for abnormal behavior or traffic patterns, and alerts the administrator when such activity is detected.
- **Hybrid NIDS:** Combines both signature-based and anomaly-based detection methods to provide a more comprehensive approach to intrusion detection.

NIDS Architecture

NIDS architecture includes the following components:

- **Network Taps:** Collect and route network traffic to the NIDS for analysis.
- **Sensors:** Monitor network traffic and analyze packets for malicious activity.
- **Console:** Provides the interface for administrators to configure and manage the NIDS, and review alerts and logs.



NIDS Deployment

NIDS can be deployed in two ways: passive or active.

- **Passive deployment:** Does not alter the network traffic or packets, and only analyzes network traffic.
- **Active deployment:** Alters network traffic or packets, such as dropping or modifying packets, to prevent malicious activity.

Advantages of NIDS

- Provides real-time monitoring of network traffic.
- Detects and alerts the administrator of potential threats, allowing for timely action to be taken.
- Can be deployed on a variety of network architectures and sizes.
- Can be configured to monitor specific types of traffic, such as web traffic or email traffic.

Disadvantages of NIDS

- **False positives:** Alerts generated by NIDS may not always indicate a genuine threat, which can lead to unnecessary investigations.
- **Limited visibility:** NIDS can only monitor network traffic, and may not be able to detect attacks on endpoints or applications.
- **Performance impact:** NIDS can impact network performance, especially if the network traffic is high.

Conclusion

- NIDS is an important tool for network security, providing real-time monitoring and alerting of potential threats.
- NIDS architecture includes sensors, network taps, and a console for management and configuration.
- NIDS can be deployed passively or actively, with advantages and disadvantages for each deployment method.

WIPS - Wireless IPS

Introduction

- Wireless Intrusion Prevention Systems (WIPS) are security tools that detect and prevent unauthorized access to wireless networks.
- WIPS is a crucial security measure for modern-day wireless networks. 
- WIPS provides a higher level of security by detecting and preventing potential threats to wireless networks.

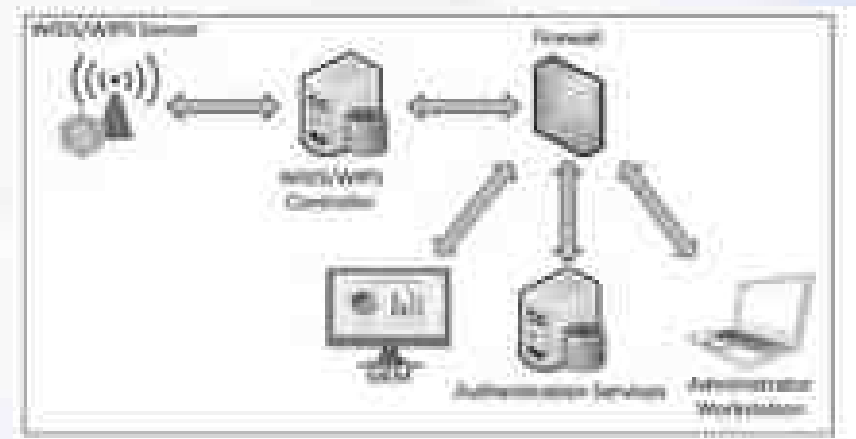
Types of WIPS

- **Overlay WIPS:** A separate wireless sensor network is deployed to monitor and secure the wireless network.
- **Integrated WIPS:** The WIPS functionality is integrated into the wireless access points (APs) themselves.

WIPS Architecture

WIPS architecture includes the following components:

- **Access Points:** Provide wireless connectivity to devices and also monitor for suspicious activity.
- **Sensors:** Detect wireless attacks or suspicious behavior and notify the access points to take appropriate action.
- **Management Console:** Provides the interface for administrators to configure and manage the WIPS, and review alerts and logs.



WIPS Deployment

- WIPS can be deployed in two ways: standalone or integrated.
- Standalone deployment: A separate sensor network is deployed to monitor wireless traffic and detect attacks.
- Integrated deployment: WIPS functionality is integrated into wireless APs themselves, reducing the need for additional hardware.

Advantages of WIPS

- Provides real-time monitoring of wireless traffic.
- Detects and prevents potential threats to the wireless network, including rogue APs and unauthorized access attempts.
- Can be configured to monitor and protect specific types of wireless traffic, such as voice or data.
- Supports compliance with regulatory requirements, such as PCI-DSS.

Disadvantages of WIPS

- **False positives:** Alerts generated by WIPS may not always indicate a genuine threat, which can lead to unnecessary investigations.
- **Limited visibility:** WIPS can only monitor wireless traffic, and may not be able to detect attacks on wired networks or applications.
- **Performance impact:** WIPS can impact wireless performance, especially if the wireless network traffic is high.

Conclusion

- WIPS is a crucial tool for wireless network security, providing real-time monitoring and prevention of potential threats. 
- WIPS architecture includes access points, sensors, and a management console for configuration and management.
- WIPS can be deployed standalone or integrated, with advantages and disadvantages for each deployment method.

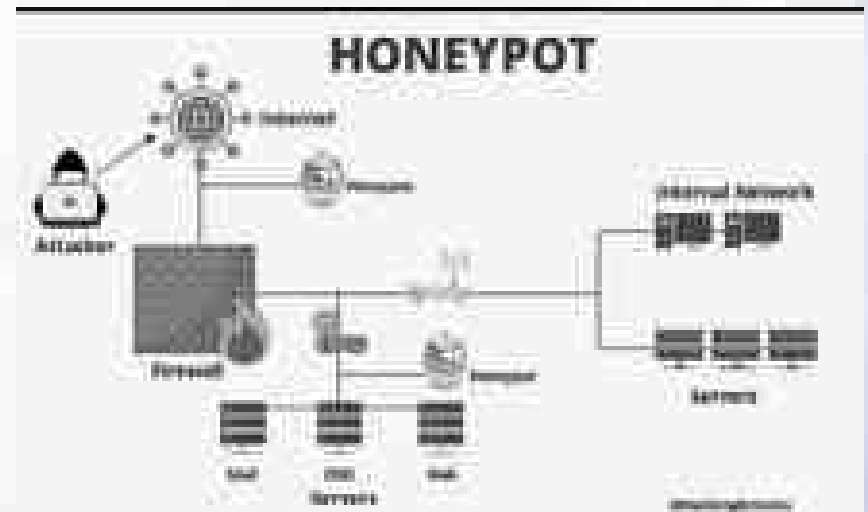
Honeypots

Introduction

- Honeypots are a type of security tool that simulate vulnerable systems or applications to attract attackers and gather information about their techniques and motives.
- Honeypots are a crucial tool for modern-day cybersecurity. 
- Honeypots can provide valuable insights into attacker behavior and help improve overall security posture.

Types of Honeypots

- **Production honeypots:** Real systems or applications that are deployed to gather information about attackers.
- **Research honeypots:** Simulated systems or applications that are deployed in a controlled environment to gather research data about attacker behavior.



Advantages of Honeypots

- Provides early warning of potential attacks, allowing for quick detection and response.
- Can gather valuable intelligence about attacker techniques, tactics, and motives.
- Helps identify vulnerabilities in systems or applications that can be remediated to improve overall security posture.
- Can divert attackers away from real systems and applications, reducing the risk of successful attacks.

Disadvantages of Honeypots

- **False positives:** Honeypots can generate false alarms, which can lead to unnecessary investigations and waste of resources.
- **Security risks:** Honeypots can be compromised by attackers, potentially exposing sensitive information or systems.
- **Maintenance overhead:** Honeypots require regular maintenance and updates, which can be resource-intensive.

Honeypot Deployment Strategies

- **Low interaction honeypots:** Simulate only the most basic functionality of a system or application, providing limited interaction with attackers.
- **Medium interaction honeypots:** Simulate more functionality of a system or application, allowing attackers to interact with them more fully.
- **High interaction honeypots:** Provide a full simulation of a real system or application, allowing attackers to interact with it as if it were real.

HoneyPot Tools

Examples of honeypot tools include:

- **KFSensor:** A Windows-based honeypot that simulates vulnerable services and applications.
- **Honeyd:** A customizable honeypot that can simulate multiple operating systems and services.
- **Cowrie:** A high-interaction honeypot that simulates a full SSH environment.

Conclusion

- Honeypots are a crucial tool for modern-day  cybersecurity, providing valuable insights into attacker behavior and improving overall security posture.
- Honeypots can be deployed in different ways, with advantages and disadvantages for each deployment strategy.
- Honeypot tools, such as KFSensor, Honeyd, and Cowrie, are available as open-source solutions or as part of commercial cybersecurity solutions.

Vulnerability Mangement & Assessment

Vulnerability Mangement & Assessment

- **Vulnerability assessment:**
- is the process of **identifying** and **evaluating** security vulnerabilities in a system or network.
- involves **running scans** and **tests** to discover vulnerabilities
- analyzing the results to determine the severity and potential impact of each vulnerability.

- **Vulnerability management:**
- process of **addressing** and **mitigating** vulnerabilities that have been identified through the vulnerability assessment.
- includes **prioritizing vulnerabilities** based on severity and potential impact, **developing a plan** to address them, and implementing the necessary **fixes or patches**.
- remediated through **patching** and **configuration** of security settings.

Terms

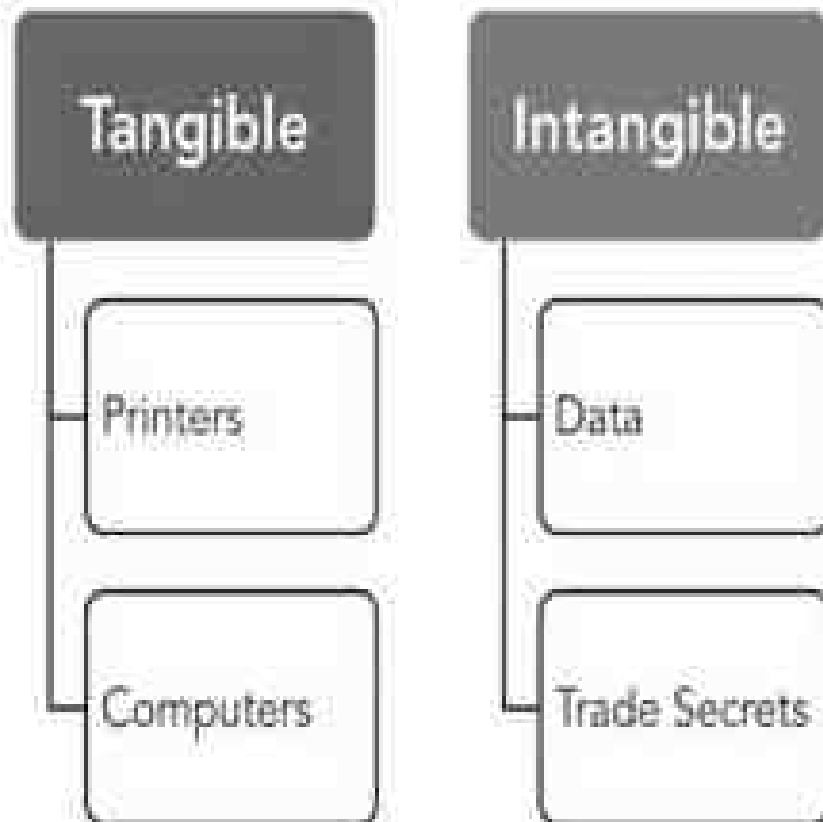
Assets

Risks

Threats

Vulnerabilites

Assets



RISK

- Risk refers to the potential harm or damage that can be caused by a cyber attack or security breach.
- Includes bussiness disruption, financial loss.

Threat

- Anything that can exploit a vulnerability
- obtain , damage or destroy an asset

What is a vulnerability ?

- **vulnerability**

refers to a **weakness** or **flaw** in a system, application, or network

exploited by attackers to gain **unauthorized access**, **steal data**, **disrupt operations**

Vulnerabilities can be caused by **software bugs**, **configuration errors**, **design flaws**, or **unpatched systems** that leave systems exposed to potential attacks.

Examples of common vulnerabilities:

- Weak or easily guessable passwords
- Unpatched software vulnerabilities
- Misconfigured settings
- Malware infections

- A vulnerability assessment uses automated network security scanning tools.

- Common vulnerability scanners ?
 - OpenVAS
 - Nessus
 - Qualys
 - Rapid7
 - Nmap

END

Vulnerability management life cycle

- Threats exist, as well as vulnerabilities.
- You can't control the threats.
- You can reduce the vulnerabilities

Vulnerability management life cycle



Vulnerability management life cycle

Initial Assessment:

- Identify assets, define risk and possible business impact
- Helps answer the question: “Why are we doing this?”
- Understanding the overall impact of a cyber attack will inspire everyone to be more vested in mitigating vulnerabilities

Vulnerability management life cycle



Vulnerability management life cycle

- **Plan:**
 - **Check for compliance requirements**
 - **Determine the best time to perform the scan**
 - **Decide on what tools to use**
 - Port Scan, network scans, or web application scans
 - **Run the automated scan**
 - **Generate report**

Vulnerability management life cycle



Vulnerability management life cycle

- Detailed description, discovery date ,what was affected
- OS, application, network, or mobile device
- Common Vulnerabilities and exposures(CVE) score
- Prioritize according to the risk level
- Determine a time to reassess the vulnerability

Vulnerability management life cycle



Vulnerability management life cycle

- Remediate
- Take steps to correct system integrity
- Research the best way to mitigate the vulnerability
 - Research vulnerabilities
 - Evaluate fixes and remediation method
 - Test the patches and fixes
 - Apply patches/fixes
 - Monitor results

Vulnerability management life cycle



Vulnerability management life cycle

- **Retest and verify:**
- Retest and verify that you successfully corrected the problem
- This involves rescanning the system and comparing the results

Vulnerability management life cycle



Vulnerability management life cycle

- Vulnerability management life cycle
A continuous best practice process to protect your organization and data

Why Is A VM Program Required ?

- What is a patch ?

“A **patch** is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing **security** vulnerabilities and other bugs”

[https://en.wikipedia.org/wiki/Patch_\(computing\)](https://en.wikipedia.org/wiki/Patch_(computing))

Why Is A VM Program Required ?

- What is patch management ?

Patch management is an area of [systems management](#) that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system.

<http://searchenterprisedesktop.techtarget.com/definition/patch-management>

Why Is A VM Program Required ?

- Patch management tasks :

Maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed.

<http://searchenterprisedesktop.techtarget.com/definition/patch-management>

Why Is A VM Program Required ?

- Patch management tasks:
properly, testing systems after installation, and documenting all associated procedures, such as specific configs required.

[http://searchenterprisedesktop.techtarget.com/
definition/patch-management](http://searchenterprisedesktop.techtarget.com/definition/patch-management)

Why Is A VM Program Required ?

Risk of not patching:

- By not applying a patch you might be leaving the door open for a [malware](#) attack

Why Is A VM Program Required ?

- Risk of not patching:
- Defects in clients like web browsers, email programs, image viewers, instant messaging software, and media players may allow malicious websites, etc. to infect or compromise your computer.

Why Is A VM Program Required ?

A VM program addresses timely management of patching to ensure that vulnerabilities are not present for hackers to exploit.

END

What Is An Exploit ?

- What is an exploit ?
 - Program or some code that takes advantage of a security hole (i.e. a vulnerability) in an application or system, so that an attacker can use it for their benefit.

<https://www.welivesecurity.com/2015/02/27/exploits-work/>

What Is An Exploit ?

- Remote exploit:

A remote exploit works over a network and exploits the security vulnerability without any prior access to the vulnerable system.

For example, an attacker compromises a web server on a corporate network, the attacker can then use the compromised web server to attack other systems on the network

[https://en.wikipedia.org/wiki/Exploit_\(computer_security\)](https://en.wikipedia.org/wiki/Exploit_(computer_security))

What Is An Exploit ?

- Local exploit:

A *local exploit* requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator.

[https://en.wikipedia.org/wiki/Exploit_\(computer_security\)](https://en.wikipedia.org/wiki/Exploit_(computer_security))

What Is An Exploit ?

- Exploit database:
 - The Exploit Database is a [CVE compliant](https://www.exploit-db.com/about/) archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.

<https://www.exploit-db.com/about/>

What Is An Exploit ?



<https://www.exploit-db.com/>

What Is An Exploit ?

- Zero-day exploit:

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix

Security Breach Case Study 1: Home Dept 2014

- 56 million payment cards compromised
- Early September 2014

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
 - The attackers were able to gain access to one of Home Depot's vendor environments by using a third-party vendor's login credentials

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
 - Then they exploited a zero-day vulnerability in Windows, which allowed them to rotate from the vendor-specific environment to the Home Depot corporate environment.

Security Breach Case Study 1: Home Depot 2014

- Sequence of events:
 - Once they were in the Home Depot network, they were able install memory scraping malware on over 7,500 self-checkout POS terminals (Smith, 2014).

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
 - This malware was able to grab 56 million credit and debit cards. The malware was also able to capture 53 million email addresses (Winter, 2014).

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
 - The stolen payment cards were used to put up for sale and bought by carders. The stolen email addresses were helpful in putting together large phishing campaigns.

<https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367>

Security Breach Case Study 1: Home Depot 2014

- Home Depot didn't have secure configuration of the software or hardware on the POS terminals.
- There was no proof of regularly scheduled vulnerability scanning of the POS environment.

<https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367>

Security Breach Case Study 1: Home Depot 2014

- They didn't have proper network separation between the Home Depot corporate network and the POS network.

<https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367>

Security Breach Case Study 1: Home Dept 2014

- Overall:

Several controls missing, vendor management of IDs and access management missing, and monitoring of the network was missing

END

Security Breach Case Study 2: Anthem

- Health Insurer Anthem
- Affected 78.8 million individuals

<http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627>

Security Breach Case Study 2: Anthem

- Sequence of events:
 - Data [breach](#) began on Feb. 18, 2014, when a user within one of Anthem's subsidiaries opened a phishing email containing malicious content

<http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627>

Security Breach Case Study 2: Anthem

- Sequence of events:
 - Opening the email launched the download of malicious files to the user's computer and allowed hackers to gain remote access to that computer and dozens of other systems within the Anthem enterprise, including Anthem's data warehouse

<http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627>

Security Breach Case Study 2: Anthem

- Sequence of events:
 - Starting with the initial remote access, the attacker was able to move laterally across Anthem systems and escalate privileges, gaining increasingly greater ability to access information and make changes in the environment

Security Breach Case Study 2: Anthem

- Sequence of events:
 - The attacker utilized at least 50 accounts and compromised at least 90 systems within the Anthem enterprise environment including, eventually, the company's enterprise data warehouse -

Security Breach Case Study 2: Anthem

- Sequence of events:
 - a system that stores a large amount of consumer personally identifiable information
 - Queries to that data warehouse resulted in access to an exfiltration of approximately 78.8 m unique user records

Security Breach Case Study 2: Anthem

- Vulnerabilities:
 - Exploitable vulnerabilities were found in anthem network
 - User security awareness training conducted to prevent phishing and social engineering

<http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627>

Security Breach Case Study 2: Anthem

- Remediation measures:
 - Implemented two-factor [authentication](#) on all remote access tools, deployed a privileged account management solution and added enhanced logging resources to its security event and incident management solutions

Security Breach Case Study 2: Anthem

- Remediation measures:
 - Further, the company conducted a complete reset of passwords for all privileged users, suspended all remote access pending implementation of two-factor authentication and created new Network Admin IDs

END

VM Challenges & Pitfalls

- Challenges:
 - Internal expertise on VM tool
 - Not enough support from IT teams
 - Vulnerability patching causing application failure
 - Management support

VM Challenges & Pitfalls

- Internal expertise on VM tool
 - Not too much expertise required
 - Monitor traffic pattern
 - Train staff if possible
 - Patch small portions of the network first

VM Challenges & Pitfalls

- Not enough support from IT teams:
 - Create reports and share among IT management
 - Highlight and educate risks to IT management and board

VM Challenges & Pitfalls

- Patching causing application failure:
 - In test environment create work around or compensating controls
 - Test the compensating controls
 - Document the compensating controls

VM Challenges & Pitfalls

- Not enough management support:
 - Share reports with management highlighting recent incidents
 - Share industry-specific or geographically relevant breach reports
 - Create awareness

Vulnerability scanners

- Vulnerability scanners are automated tools used to identify, assess, and report security vulnerabilities

Test for vulnerabilities

- Vulnerabilities or weakness exist in many different places:
software, **operating systems**, **networks** and even **people**
- There are many choices today for assessment tools
- Some are free, some online and some are subscription-based

Types of vulnerability scanners

- There are two types of vulnerability scanners
- **Network-based scanners:** These scanners scan an organization's network to identify vulnerabilities in network devices such as routers, switches, and firewalls.
- **Host-based scanners:** These scanners are installed on individual systems or servers to identify vulnerabilities in the underlying operating system, applications, and services.

vulnerability scanners

Provide comprehensive view of their potential attack surface

- identify vulnerabilities
- Prioritize remediation efforts
- Improve security posture
- Save time and resources

Vulnerbailtuy scanners examples

OpenVAS



<https://www.greenbone.net/en/testnow/>

SlideFly is a leading provider of professional presentation services. We specialize in creating high-quality, engaging presentations for businesses, organizations, and individuals. Our team of experts uses the latest design trends and technologies to deliver presentations that are both visually appealing and informative. We offer a wide range of services, including custom slide design, animation, and video integration. Our presentations are designed to capture the attention of your audience and effectively communicate your message. Whether you need a presentation for a business meeting, a conference, or a marketing campaign, SlideFly has the expertise and resources to deliver a presentation that meets your needs and exceeds your expectations. Contact us today to learn more about our services and how we can help you create a presentation that truly stands out.

SlideFly

SlideFly: Your Professional Presentation Partner



SlideFly

Professional Presentation Services

Custom Slide Design | Animation | Video Integration

SlideFly is a leading provider of professional presentation services. We specialize in creating high-quality, engaging presentations for businesses, organizations, and individuals. Our team of experts uses the latest design trends and technologies to deliver presentations that are both visually appealing and informative. We offer a wide range of services, including custom slide design, animation, and video integration. Our presentations are designed to capture the attention of your audience and effectively communicate your message. Whether you need a presentation for a business meeting, a conference, or a marketing campaign, SlideFly has the expertise and resources to deliver a presentation that meets your needs and exceeds your expectations. Contact us today to learn more about our services and how we can help you create a presentation that truly stands out.

Our Services

- Custom Slide Design
- Animation
- Video Integration
- Professional Editing
- Revisions and Updates
- Print and Digital Delivery

Why Choose SlideFly?

- Expert Designers
- High-Quality Results
- Fast Turnaround
- Competitive Pricing
- Excellent Customer Service
- Proven Track Record

Contact Us

Phone: (123) 456-7890

Email: info@slidefly.com

Website: www.slidefly.com

Summary

This document provides a summary of the OpenVAS scan results. The scan was performed on 2020-09-10 at 10:00:00. The scan results are summarized in the table below.

Hosts scanned: 10.10.10.10 - 10.10.10.10

Hosts scanned: 10.10.10.10 - 10.10.10.10

Hosts scanned: 10.10.10.10 - 10.10.10.10

Hosts scanned:

Hosts scanned:

Vulnerability Summary



The scan results show that no vulnerabilities were detected on the scanned hosts. The scan was performed on 2020-09-10 at 10:00:00. The scan results are summarized in the table below.

Host Summary

Host	IP	OS	Architecture	Version	Severity	Count
10.10.10.10	10.10.10.10	Ubuntu 18.04	x86_64	18.04	0	0

Results per Host

Host: 10.10.10.10

Summary: 0 Critical, 0 High, 0 Medium, 0 Low, 0 Informational

Hosts scanned:

Hosts scanned: 10.10.10.10 - 10.10.10.10

Hosts scanned:

Hosts scanned:

Hosts scanned:

Hosts scanned:

<https://hackertarget.com/sample-vulnerability-report/sample-openvas-report.pdf>

~~<https://hackertarget.com/sample-vulnerability-report/metasploitable-2.0-openvas.pdf>~~

CHINA'S RISE: CHANGING THE GLOBAL ORDER



Quesada, David. China's Rise: Changing the Global Order. New York: Oxford University Press, 2017.

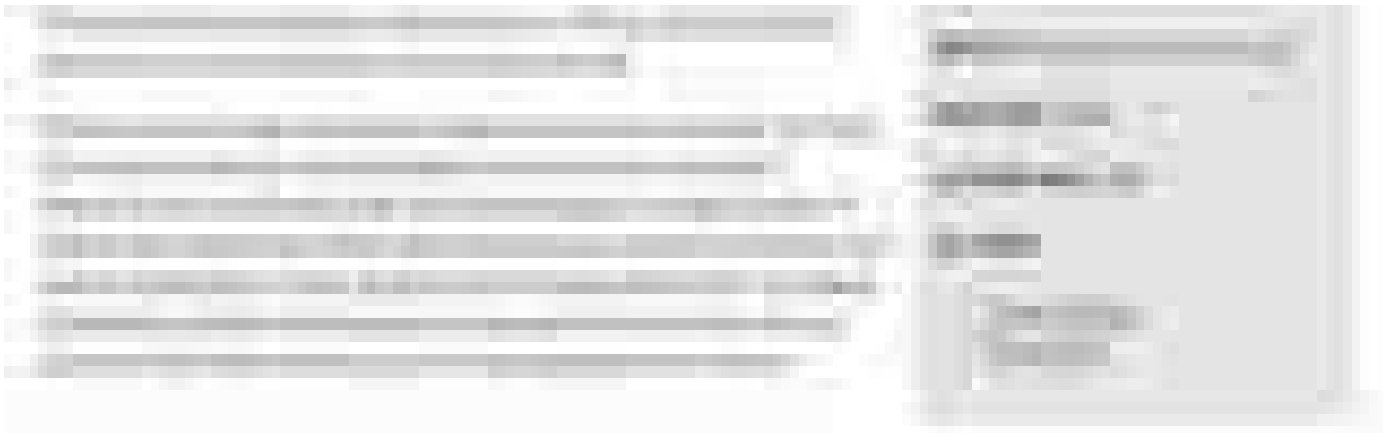
Tripwire



velocity, results, and accountability. Making the
priority list meeting that everyone can follow easily
without any



WELCOME TO VU LEARNING HUB



KALI Linux



TRY NGSPHUG EXCEL FOR 7 DAYS



Quintix Cloud Platform

The world's most advanced distributed and
centralized Clouds IT infrastructure and
compliance platform.

Learn More

Quintix Cloud Platform

Cloud Infrastructure

Cloud Security

Cloud Compliance

Cloud

Cloud

Cloud

Cloud

Cloud

Cloud

Cloud

Cloud



<https://www.sonicwall.com/phishing-iq-test/#>





Question Summary

[illegible]

QUESTION

1. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

Person	Hours
1	12
2	15
3	18
4	20
5	22
6	25
7	28
8	30
9	32
10	35



2. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

3. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

4. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

5. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

6. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

7. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

8. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

9. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

10. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

11. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

12. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

13. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

14. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

15. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

16. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

17. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

18. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

19. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

20. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

21. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

22. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

23. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

24. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

25. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

26. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

27. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

28. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:

29. The following table shows the number of hours spent on a project by a team of 10 people. The data is as follows:



- Vulnerability scanners typically work by scanning systems, applications, and network devices for known vulnerabilities and misconfigurations, using a database of known vulnerabilities and attack vectors.

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Manual & Automated mechanisms for security hardening & validation

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Step 1: Scan an IT asset using Qualys compliance scan, NISSUS compliance scan, or CIS CAT PRO Tool
- Acquire report of failed controls

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Step 2: Apply the failed controls using AD (for Windows) or manually for other systems & devices

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Step 3: Use the automated feature of Qualys compliance scan, Nessus compliance scan or CIS CAT Pro Tool to verify that the applied controls are in place
- Compare the ‘before’ and ‘after’ report

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Step 4: manually verify if any discrepancy is found (control should be in place but not being validated by the tool)

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Step 5: For any system or device for which the Qualys compliance scan, Nessus compliance scan, or CIS CAT Pro Tool scan cannot be performed, conduct the validation of control implementation manually

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Use sampling where necessary during manual validation work to reduce workload
- For example, 15-20 % of assets may be checked at random
- Or 15-20% of controls may be checked on an asset

END

SCAP

(Security Content Automation Protocol)

SCAP

- SCAP was developed by the **National Institute of Standards and Technology (NIST)** in collaboration with various **government agencies** and **industry partners**
- To create a **consistent language** and **format** for discussing security issues

SCAP Components

- Common Weakness Enumeration (CWE)
- Common vulnerabilities and exposures (CVE)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Common vulnerability scoring system (CVSS)

Common Weakness Enumeration (CWE)

- CVE is a community-developed list of **software** and **hardware** weakness types.
- It serves as a **measuring stick** for security tools, and as a baseline for **weakness identification**, **mitigation**, and **prevention** efforts.
- <https://cwe.mitre.org/index.html>



Common vulnerabilities and exposures (CVE)

- CVE Provides detailed information on **known vulnerabilities**
- is used to **identify** and **classify** vulnerabilities that may impact a software and hardware products.

Common Configuration Enumeration (CCE)

- Common Configuration Enumeration (CCE) is a standardized method of **identifying** and **describing** security-relevant **system configuration settings**.
- CCE is maintained by the National Institute of Standards and Technology (**NIST**).
- Security teams evaluate the **security posture** of their systems, **identify misconfigured settings** that may increase their risk.
- https://cce.mitre.org/lists/cce_list.html



Common Platform Enumeration (CPE)

- **CPE** is a standardized method of describing and identifying software systems, applications, and operating systems using a unique identifier format.
- provides a structured and uniform way of describing the attributes of a software product, such as the vendor name, product name, version number, and edition.
- <https://nvd.nist.gov/products/cpe>

Common Platform Enumeration (CPE)

- consists of three components separated by colons:
- The first component identifies the **vendor name**,
- The second component identifies the **product name**, and
- The third component identifies the **version number**.
- For example, the CPE string for Windows 10 would be:
- **cpe:/o:microsoft:windows_10**
- This format is used by various security tools, such as **vulnerability scanners**, to **identify and match** software products with known vulnerabilities or other security issues.
- <https://nvd.nist.gov/products/cpe>



Common vulnerability scoring system (CVSS)

- CVSS is a standardized method of **assessing** and **scoring** the **severity** of cyber security **vulnerabilities**.
- **prioritize** and **manage** vulnerabilities based on their **potential impact**.

Common Vulnerabilities and Scoring System

Exploitability Matrix:

- Access Vector
- Attack Complexity
- Privileges Required
- User Interaction

National Vulnerability Database (NVD)

- NVD is the **largest publicly available** source of **vulnerability intelligence** by National Institute of Standards and Technology (NIST)
- Vulnerabilities in the NVD are called Common Vulnerabilities and Exposures (CVE).
- <https://nvd.nist.gov/>

Common Vulnerabilities and Exposures

- Common Vulnerabilities and Exposures (CVE) is a standardized **list of publicly known cyber security vulnerabilities** and exposures.
- Each CVE entry includes a **unique identifier**, a **description** of the vulnerability, the **affected software or hardware**, and a **score** based on the Common Vulnerability Scoring System (CVSS).
- The score is derived from a set of metrics using the **(CVSS)**
- The CVE feeds into the National Vulnerabilities Database(**NVD**)

<https://cve.mitre.org/>

<https://www.cvedetails.com/vulnerabilities-by-types.php>

<https://www.cvedetails.com/vulnerability-list/opsqli-1/sql-injection.html>



Common Vulnerabilities and Exposures

[illegible]

Common Vulnerabilities and Expore



<https://nvd.nist.gov/search>

Common Vulnerabilities and Exposures



Common Vulnerabilities and Exposures



Common Vulnerabilities and Exposures



Common Vulnerabilities and Expore

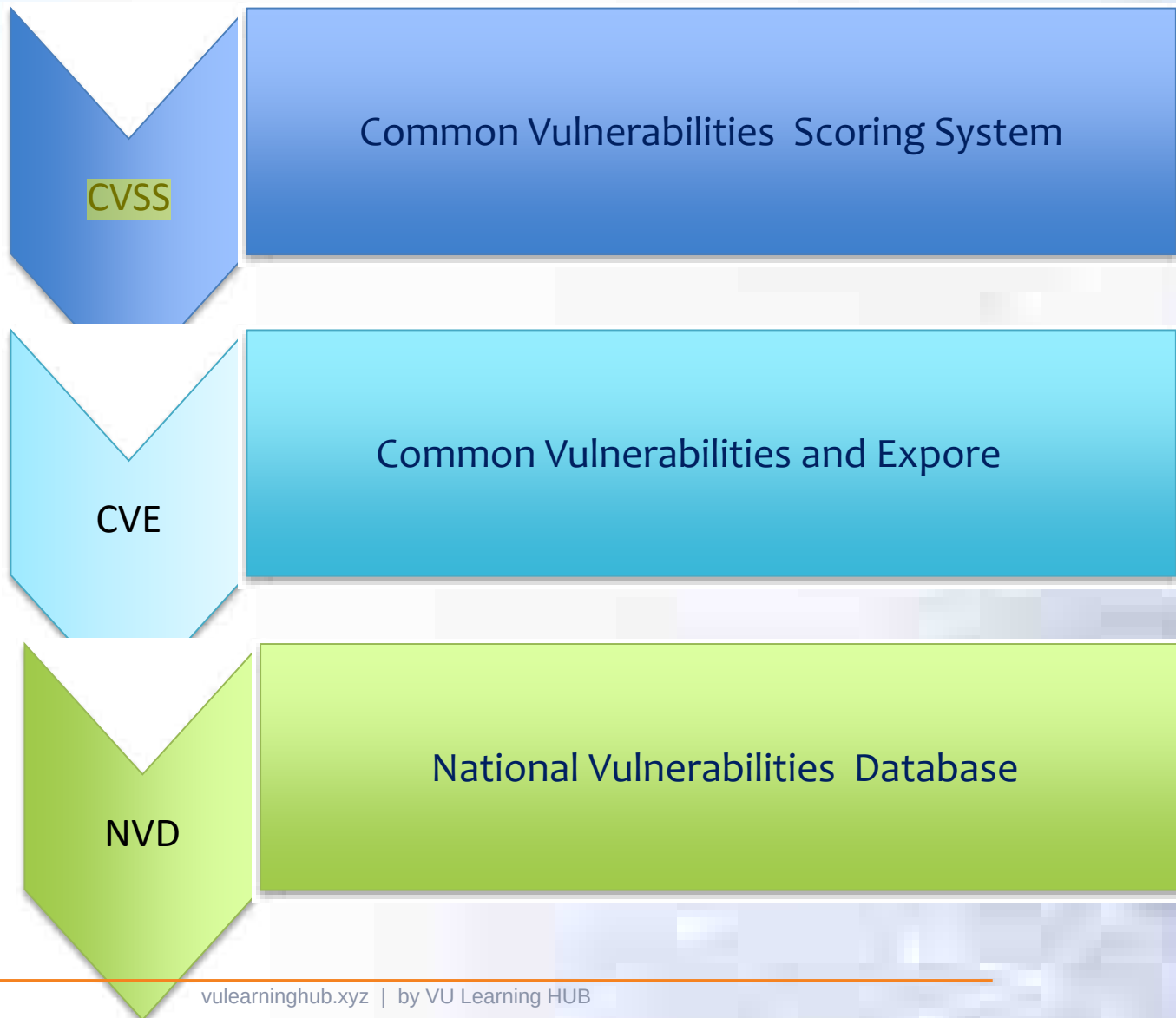


Common Vulnerabilities and Exposures



<https://sec.cloudapps.cisco.com/security/center/publicationListing.x>

Common Vulnerabilities and Exposures



Common Vulnerabilities and Scoring System

- Industry standard that rates the severity of vulnerabilities
- Used in Common Vulnerabilities and Exposures (CVE) listings to aid in prioritizing vulnerabilities
- Based on a set of metrics that determines the overall score

Common Vulnerabilities and Scoring System

TABLE 1. CVSS Scoring System: Vulnerability Severity

Vulnerability Severity	Base Score Range	Severity	Description
Critical	9.0-10.0	C	The vulnerability is exposed and potentially exploitable, with a severe impact. Exploitation could lead to other vulnerabilities and high-level access to the system, resulting in a total system compromise or destruction.
High	7.0-8.9	H	The vulnerability is a high-severity problem that, if exploited, will lead to significant impact on the system. A single exploit could lead to significant consequences, such as data loss, denial of service, or compromise of confidentiality.
Medium	4.0-6.9	M	The vulnerability is a moderate-severity problem that, if exploited, will lead to moderate consequences, such as a denial of service or loss of confidentiality.
Low	2.0-3.9	L	The vulnerability is a low-severity problem that, if exploited, will lead to low consequences, such as a denial of service or loss of confidentiality.
None	0.0-1.9	N	The vulnerability is not a problem, or the impact is so low that it is not considered a vulnerability.

CVSS severity factors

- **Attack vector:** the attacker needs to be **authenticated** or whether the attack can be launched **remotely**.
- **Attack complexity:** the attack requires **special knowledge** or **tools**
- **Privileges required:** an attacker would need **administrative access** or **user-level access**.
- **Impact on confidentiality, integrity, and availability:** **potential impact** of the vulnerability on the **confidentiality, integrity, and availability** of systems and data.
- CVSS uses a scoring system ranging from **0 to 10**, with higher scores indicating more severe vulnerabilities.

CVSS Score Qualitative Rating:

Score	Rating
0.0	None
0.1 – 3.9	Low
4.0 – 6.9	Medium
7.0 – 8.9	High
9.0 – 10.0	Critical

<https://www.first.org/cvss/v3.1/examples>

<https://nvd.nist.gov/vuln-metrics/cvss>

Current 2013 House Composition (by % representation)



Common Vulnerabilities and Scoring System

Impact Metrics:

- What impact will this have if the threat is able to exploit the vulnerability?
- Will it be a violation of confidentiality, integrity, or availability

Common Vulnerabilities and Scoring System

Temporal Metrics:

- The Current state of the exploit

Common Vulnerabilities and Scoring System



<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

Common Vulnerabilities and Scoring System



Common Vulnerabilities and Scoring System



The image shows a web form titled "CVE Scoring Matrix". It contains several sections for inputting vulnerability details. The first section, "Report Title (Required)", has a text input field and a "Report Title" button. The second section, "Description (Required)", has a text input field and a "Description" button. The third section, "CVSS Base Score", has a dropdown menu and a "CVSS Base Score" button. The fourth section, "CVSS Temporal Score", has a dropdown menu and a "CVSS Temporal Score" button. The fifth section, "CVSS Environmental Score", has a dropdown menu and a "CVSS Environmental Score" button. The form is designed to collect data for scoring vulnerabilities according to the CVE system.

Common Vulnerabilities and Scoring System



The screenshot displays the CVE website interface, which is organized into three main columns. The left column lists various vulnerability categories such as 'Common Vulnerabilities and Exposures', 'CVE Details', 'CVE Details', 'CVE Details', 'CVE Details', 'CVE Details', 'CVE Details', 'CVE Details', 'CVE Details', and 'CVE Details'. The middle column provides a list of specific vulnerability entries, each with a CVE ID (e.g., CVE-2017-16995, CVE-2017-16996, CVE-2017-16997, CVE-2017-16998, CVE-2017-16999, CVE-2017-17000, CVE-2017-17001, CVE-2017-17002, CVE-2017-17003, CVE-2017-17004) and a brief description of the vulnerability. The right column contains a list of links or references related to each vulnerability, including 'CVE Details', 'CVE Details', 'CVE Details', 'CVE Details', 'CVE Details', 'CVE Details', 'CVE Details', 'CVE Details', 'CVE Details', and 'CVE Details'.

Category	Vulnerability Details	Links/References
Common Vulnerabilities and Exposures	CVE-2017-16995	CVE Details
CVE Details	CVE-2017-16996	CVE Details
CVE Details	CVE-2017-16997	CVE Details
CVE Details	CVE-2017-16998	CVE Details
CVE Details	CVE-2017-16999	CVE Details
CVE Details	CVE-2017-17000	CVE Details
CVE Details	CVE-2017-17001	CVE Details
CVE Details	CVE-2017-17002	CVE Details
CVE Details	CVE-2017-17003	CVE Details
CVE Details	CVE-2017-17004	CVE Details

1. The first step in the process is to identify the problem. This involves understanding the current situation and the desired outcome. Once the problem is identified, the next step is to develop a plan of action. This plan should outline the steps that need to be taken to solve the problem. Finally, the plan should be implemented and the results monitored.

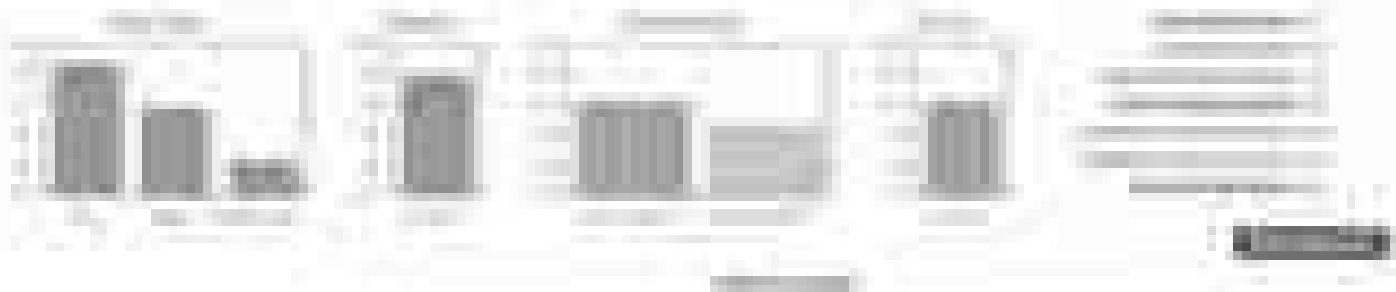
2. The second step in the process is to develop a plan of action. This involves identifying the steps that need to be taken to solve the problem. The plan should be realistic and achievable, and it should be flexible enough to allow for changes as the situation evolves. Once the plan is developed, the next step is to implement it.

3. The third step in the process is to implement the plan. This involves putting the plan into action and monitoring the results. It is important to stay focused on the goal and to be willing to make adjustments as needed. Once the plan is implemented, the next step is to evaluate the results.

4. The fourth step in the process is to evaluate the results. This involves comparing the actual results with the desired outcome. If the results are not as good as desired, it may be necessary to go back to the plan and make adjustments. If the results are good, then the process is complete.

5. The fifth step in the process is to communicate the results. This involves sharing the results with the relevant stakeholders and providing feedback. This step is important because it allows the organization to learn from its experience and to make improvements for the future.

6. The sixth step in the process is to document the results. This involves creating a record of the process and the results. This documentation is important for several reasons. First, it provides a reference for future projects. Second, it allows the organization to track its progress over time. Finally, it provides a basis for accountability.



Project Summary			
Project Name	Project X		
Project Manager	John Doe		
Project Start Date	2023-01-01		
Project End Date	2023-03-31		
Project Budget	\$100,000		
Project Status	Completed		
Project Description	A new software application for managing customer data.		
Project Objectives	To improve customer data management and increase sales.		
Project Deliverables	A new software application, training materials, and documentation.		
Project Risks	Data security, integration with existing systems, and user adoption.		
Project Results	The project was completed on time and within budget. Customer data management has improved and sales have increased.		

What Is CVE & Vulnerability Database ?

Impact

CVSS Severity (version 3.0)

CVSS v3 Base Score: 9.8 Critical

Vector: CVSS:3.0/AV:N/AC:L/

(legend)

Impact Score: 5.9

Exploitability Score: 3.9

CVSS Version 3 Metrics

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): High

Integrity (I): High

Availability (A): High

What Is CVE & Vulnerability Database ?

CVE Details (version 2.0)

CVE ID Base Score: 7.5 (High)

Vector: `OS:Linux; Linux kernel 2.6.18-128.el5`

Impact Subscore: 6.4

Exploitability Subscore: 10.0

CVE Version 2 Details

Access Vector: Network (remote)

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows (authenticated) disclosure of information, Allows (authenticated) denial of service, Allows (authenticated) DoS (Denial of Service)

NESUSS

- Nessus dates back to 1998
- Nessus moved to closed source commercial product in 2005
- The most trusted and gold standard vulnerability assessment solution
- Most widely deployed security standard



- Nessus Essential is limited to scanning only 16 IP addresses 

[Home](#)
[About](#)
[Contact](#)
[Privacy Policy](#)
[Terms of Service](#)

THE HELLAS FAMILY

Introducing the new Hellas family of products, designed to help you manage your business more effectively.

Hellas

Introducing the new Hellas family of products, designed to help you manage your business more effectively.

Introducing the new Hellas family of products, designed to help you manage your business more effectively.

- Introducing the new Hellas family of products, designed to help you manage your business more effectively.
- Introducing the new Hellas family of products, designed to help you manage your business more effectively.
- Introducing the new Hellas family of products, designed to help you manage your business more effectively.

Hellas

Introducing the new Hellas family of products, designed to help you manage your business more effectively.

Introducing the new Hellas family of products, designed to help you manage your business more effectively.

- Introducing the new Hellas family of products, designed to help you manage your business more effectively.
- Introducing the new Hellas family of products, designed to help you manage your business more effectively.
- Introducing the new Hellas family of products, designed to help you manage your business more effectively.

Hellas

Introducing the new Hellas family of products, designed to help you manage your business more effectively.

Introducing the new Hellas family of products, designed to help you manage your business more effectively.

- Introducing the new Hellas family of products, designed to help you manage your business more effectively.
- Introducing the new Hellas family of products, designed to help you manage your business more effectively.
- Introducing the new Hellas family of products, designed to help you manage your business more effectively.

1

Outdated Protocols

SSL is no longer a secure protocol

2

Insecure Cipher Suites

Only support strong encryption

3

Certificate Issues

Watch for expired, self-signed, or missing certificates



1. **Identify the problem.** The first step in the problem-solving process is to identify the problem. This involves understanding the situation, gathering information, and defining the problem clearly.

2. **Analyze the problem.** Once the problem is identified, the next step is to analyze it. This involves breaking the problem down into smaller, more manageable parts and identifying the causes of the problem.

3. **Generate solutions.** The third step is to generate potential solutions. This involves brainstorming ideas and considering different approaches to solving the problem.

4. **Evaluate solutions.** The fourth step is to evaluate the potential solutions. This involves comparing the solutions against the problem and considering the pros and cons of each.

5. **Implement the solution.** The final step is to implement the chosen solution. This involves putting the solution into action and monitoring its progress.

[illegible]

<https://www.tenable.com/products/nessus/nessus-essentials?action=register>





<https://www.tenable.com/downloads/nessus?loginAttempted=true>



<https://docs.tenable.com/nessus/Content/GettingStarted.htm>

Cloud based service



CHOOSE YOUR HYBRID EXPOSURE TEAM WITH MESSEUS

At Messeus, we have a team of experts who can help you choose the right hybrid exposure team for your business. Our team of experts can help you choose the right hybrid exposure team for your business.





NESUSS



<https://www.tenable.com/products/nessus/nessus-essentials>





Oracle University

My Oracle Support

Thank You for Registering for Nassu Essentials

Thank you for registering for Nassu Essentials. You will receive a confirmation email from Oracle University.

Thank you for registering for Nassu Essentials. You will receive a confirmation email from Oracle University.

Welcome To Network Essentials

Welcome to Network Essentials and congratulations on taking the first step towards your network. We offer the latest software for vulnerability scanning, policy, helping you identify more vulnerabilities and design your network accordingly.

If you're looking for more advanced capabilities such as live traffic and configuration analysis, we need to be using the next generation of the Network Essentials. To learn more, visit the [Network Essentials Learning](#).

Activating Your Network Essentials License

Get your license code by [following these steps](#).

[Click here to activate your license](#)



This is a one-time code. If you cannot get your license, please contact support for further assistance.

After your activation is complete, you will be prompted to create your account. Your account will be used to manage your subscription, view the license status.

Do you have any questions?

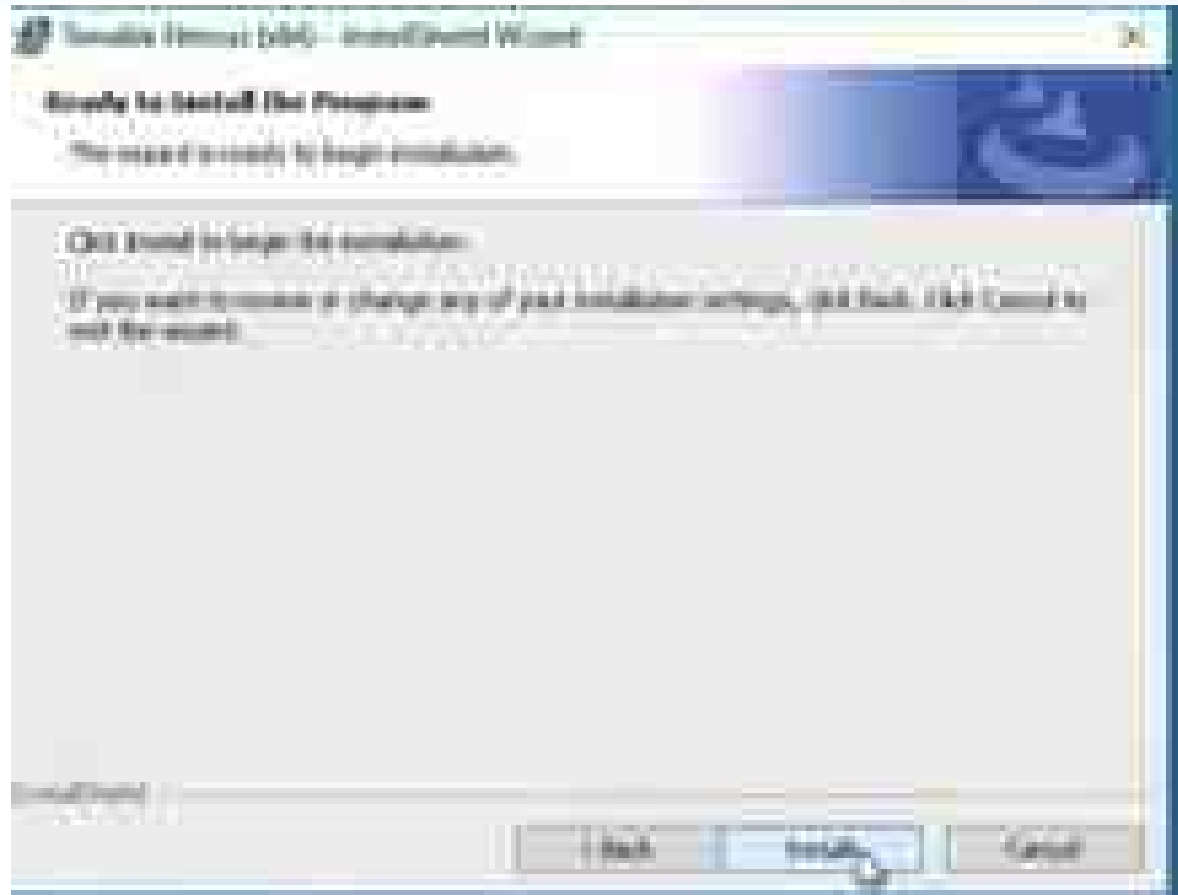
If you have any questions, visit the [Network Essentials page](#) for the latest information.

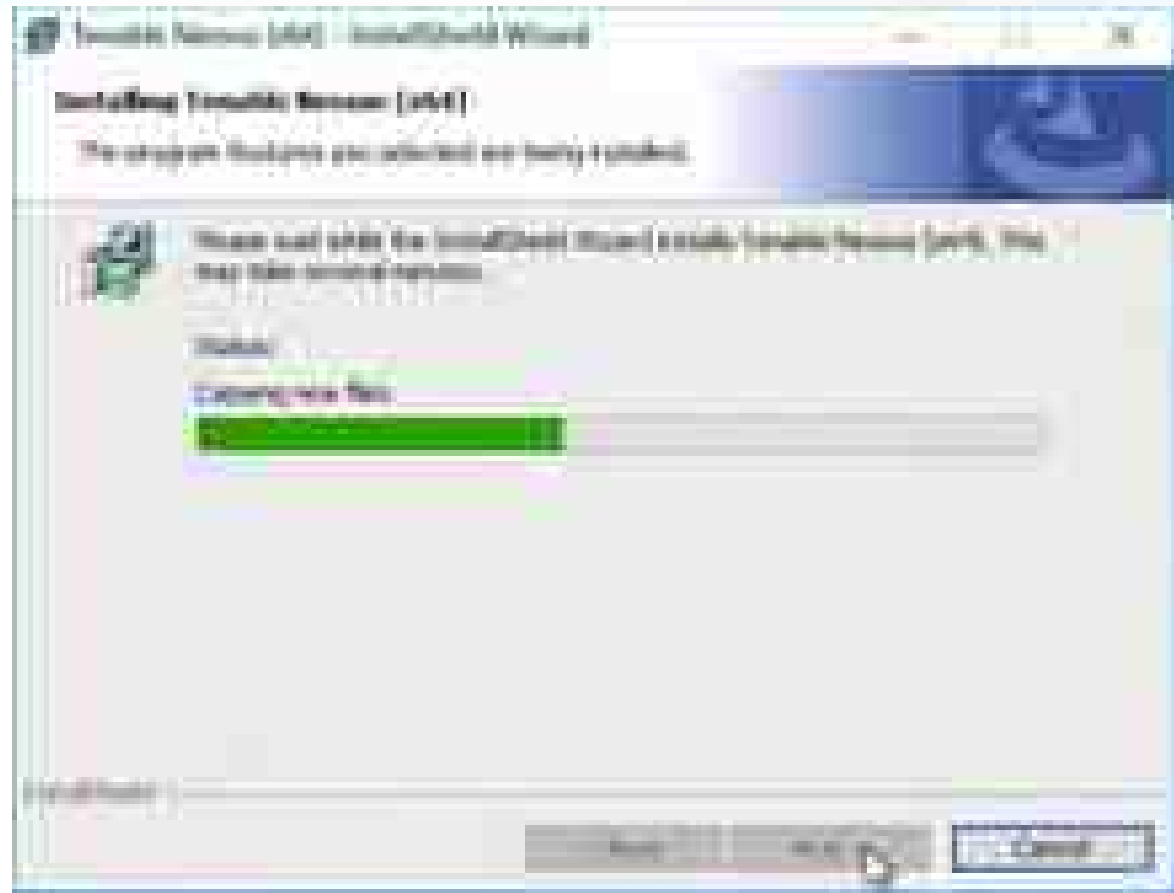








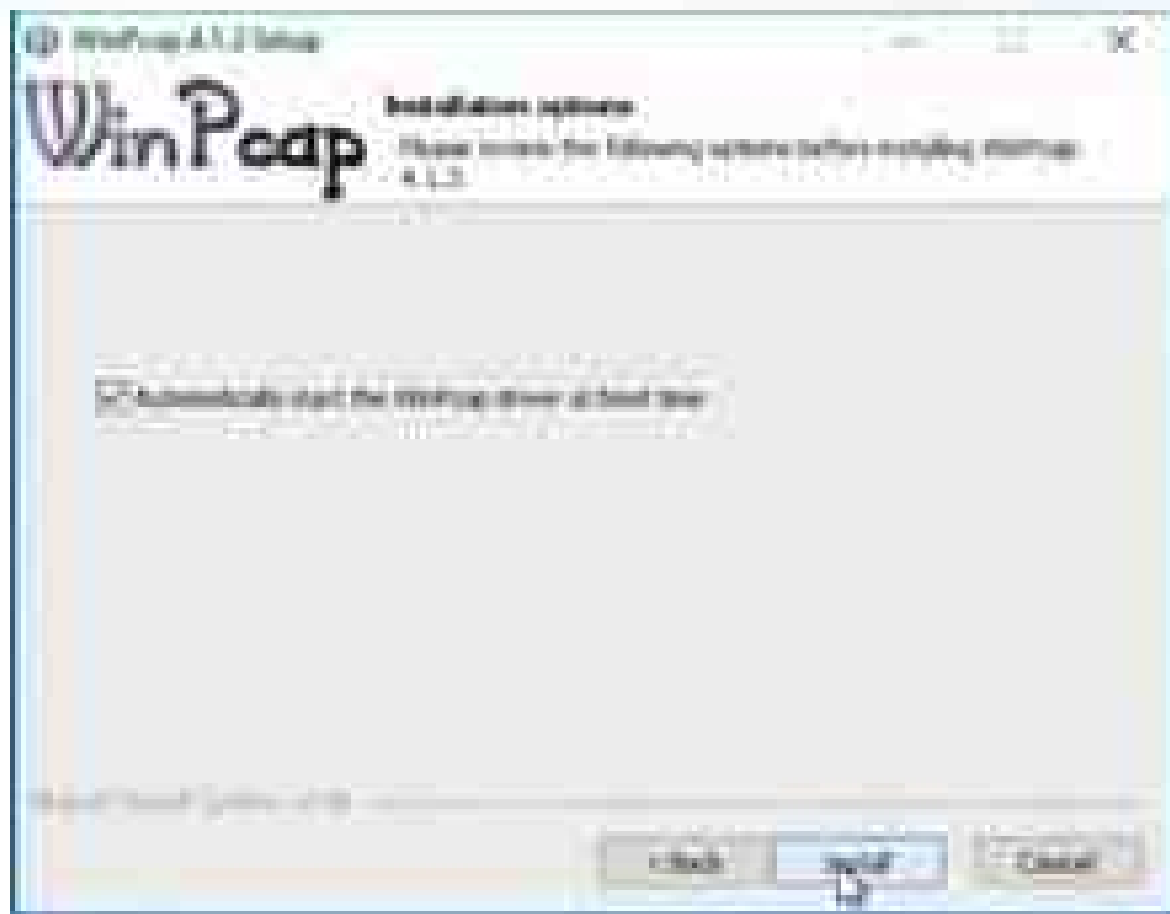




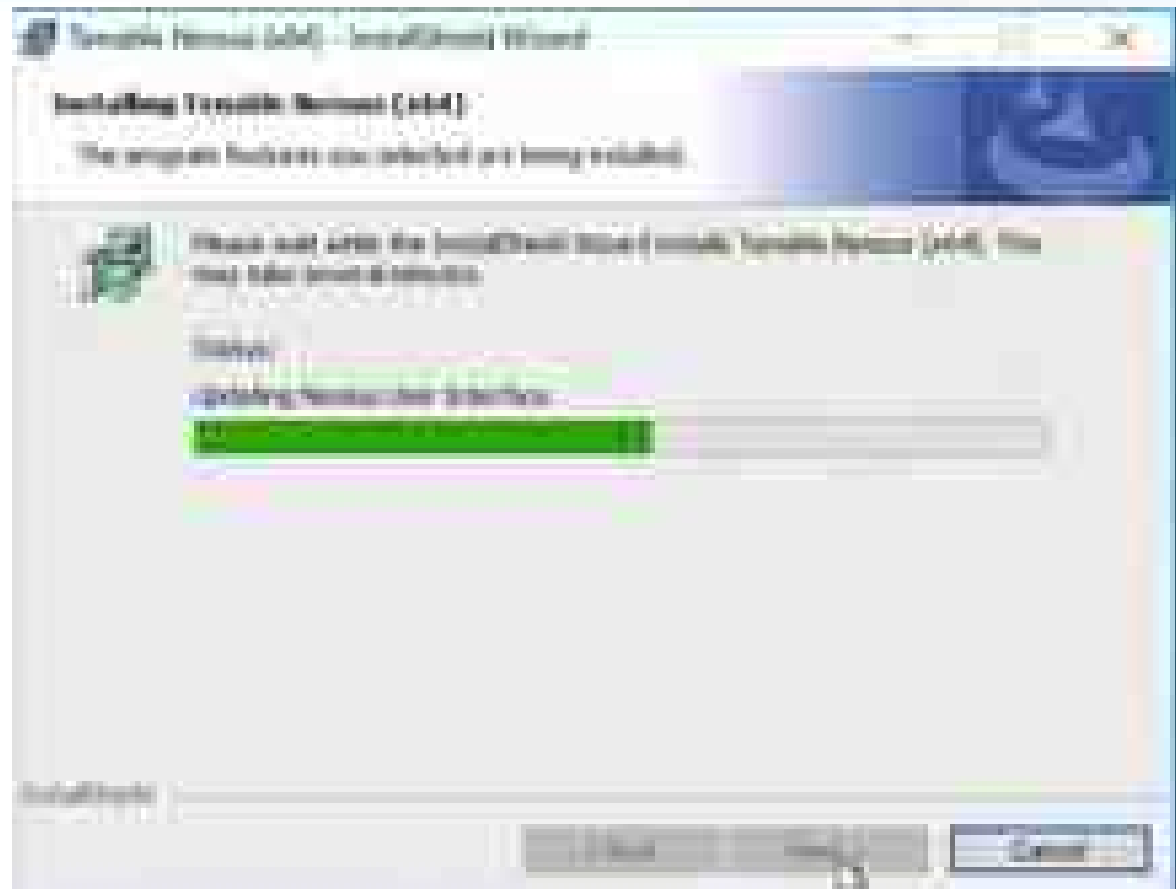


- Nessus installer realize that i don't have windows packet capture library
- Nessus can't work on winods without **WinPcap**



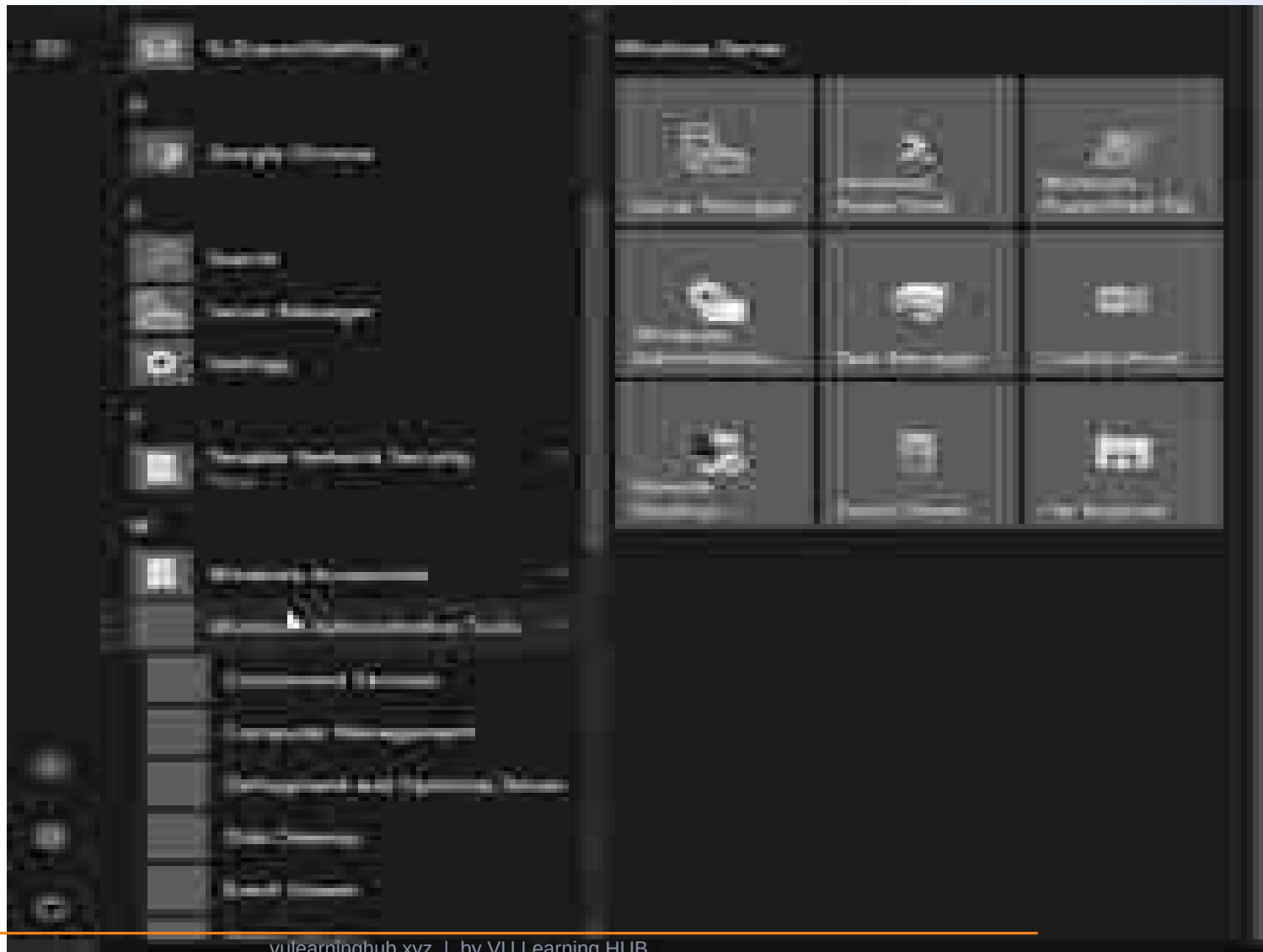




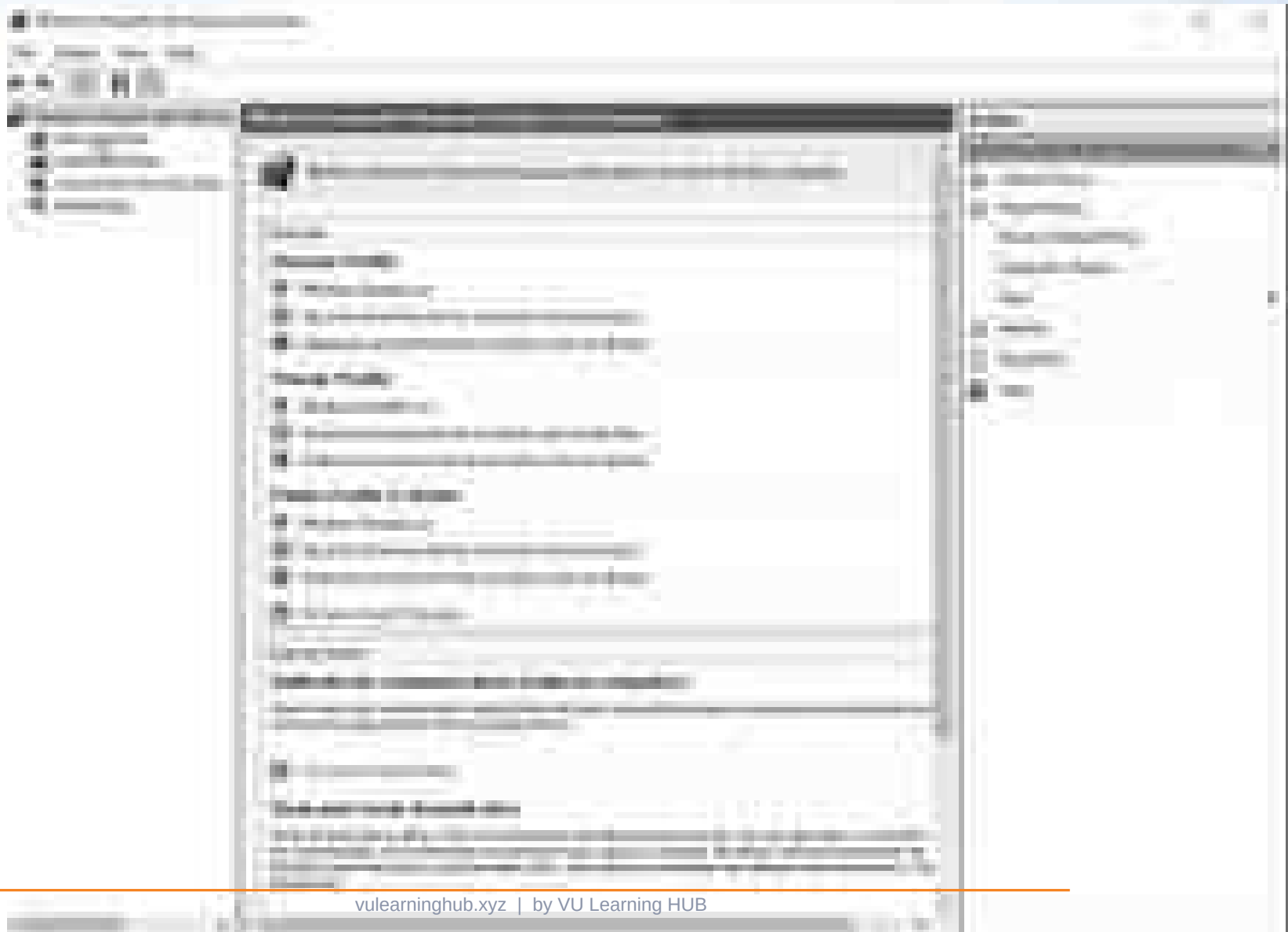




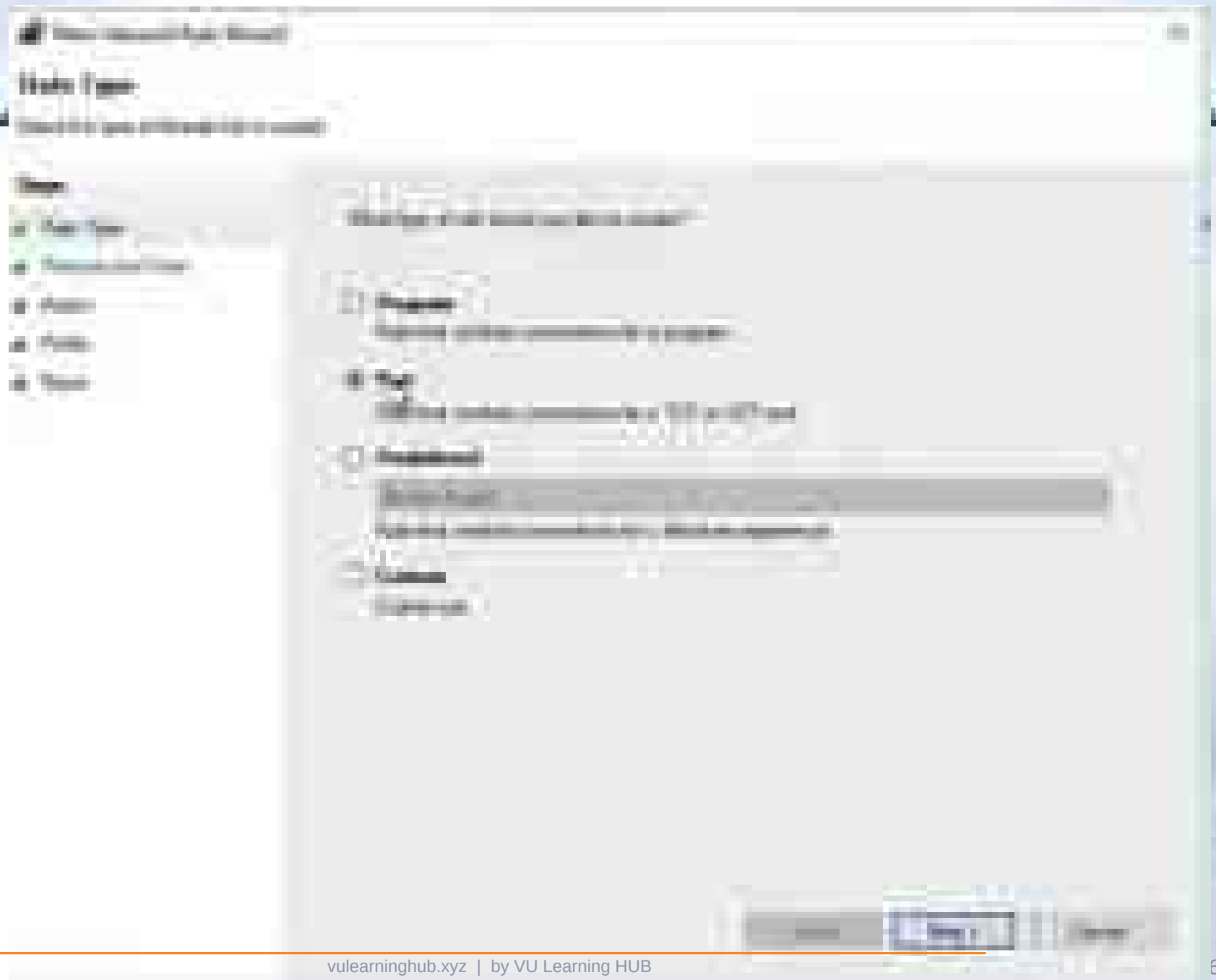
Nessus Manger use TCP port 8834

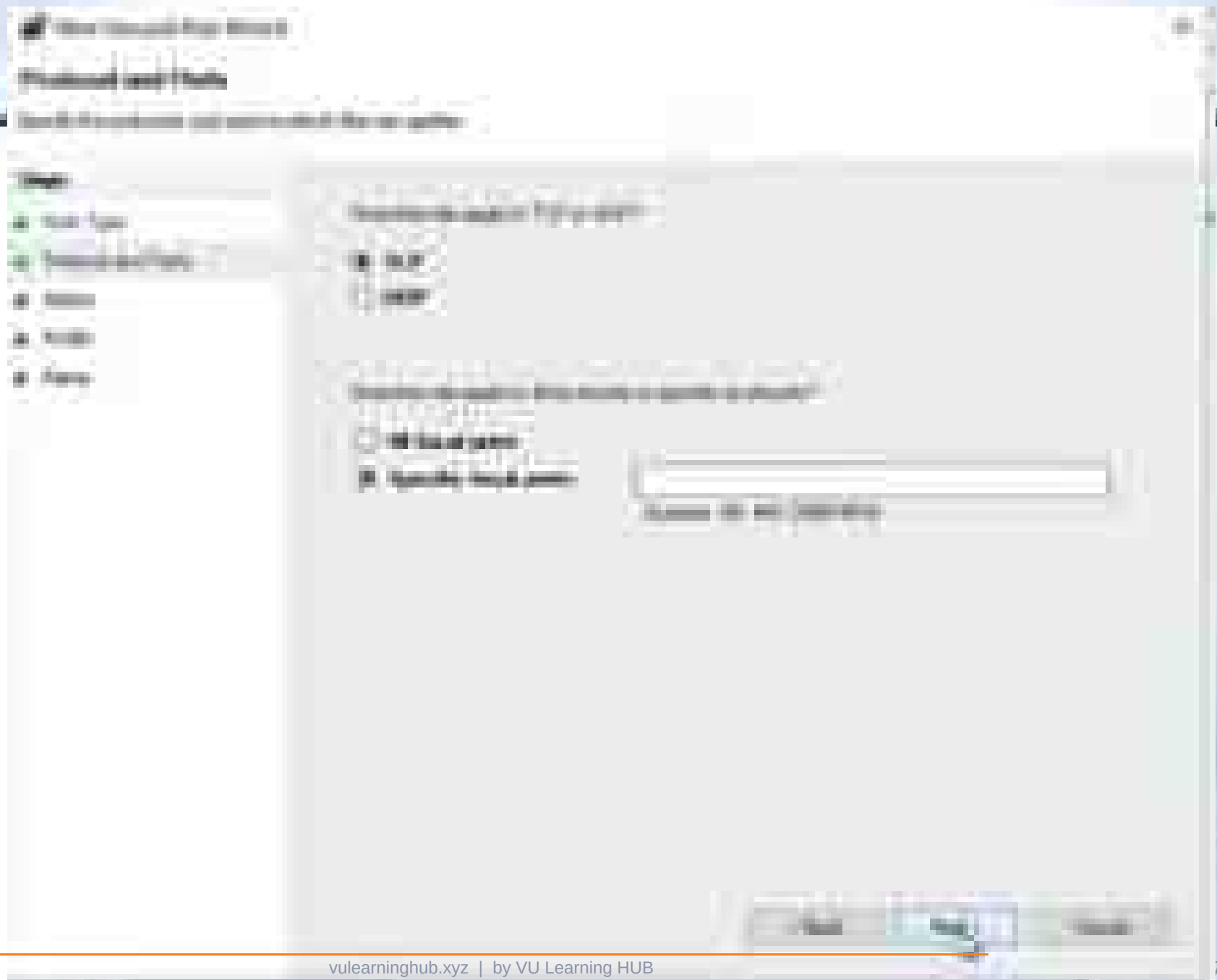






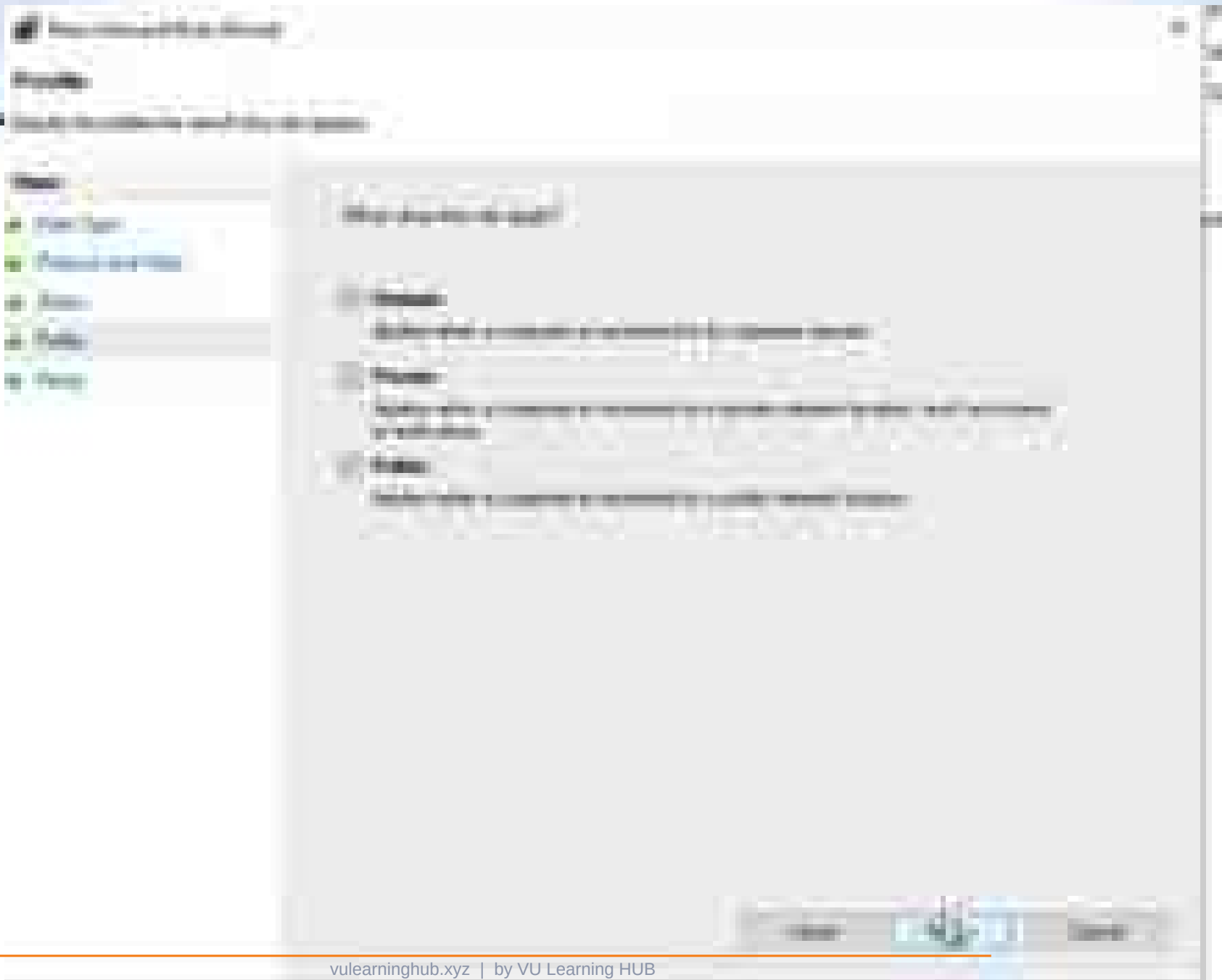


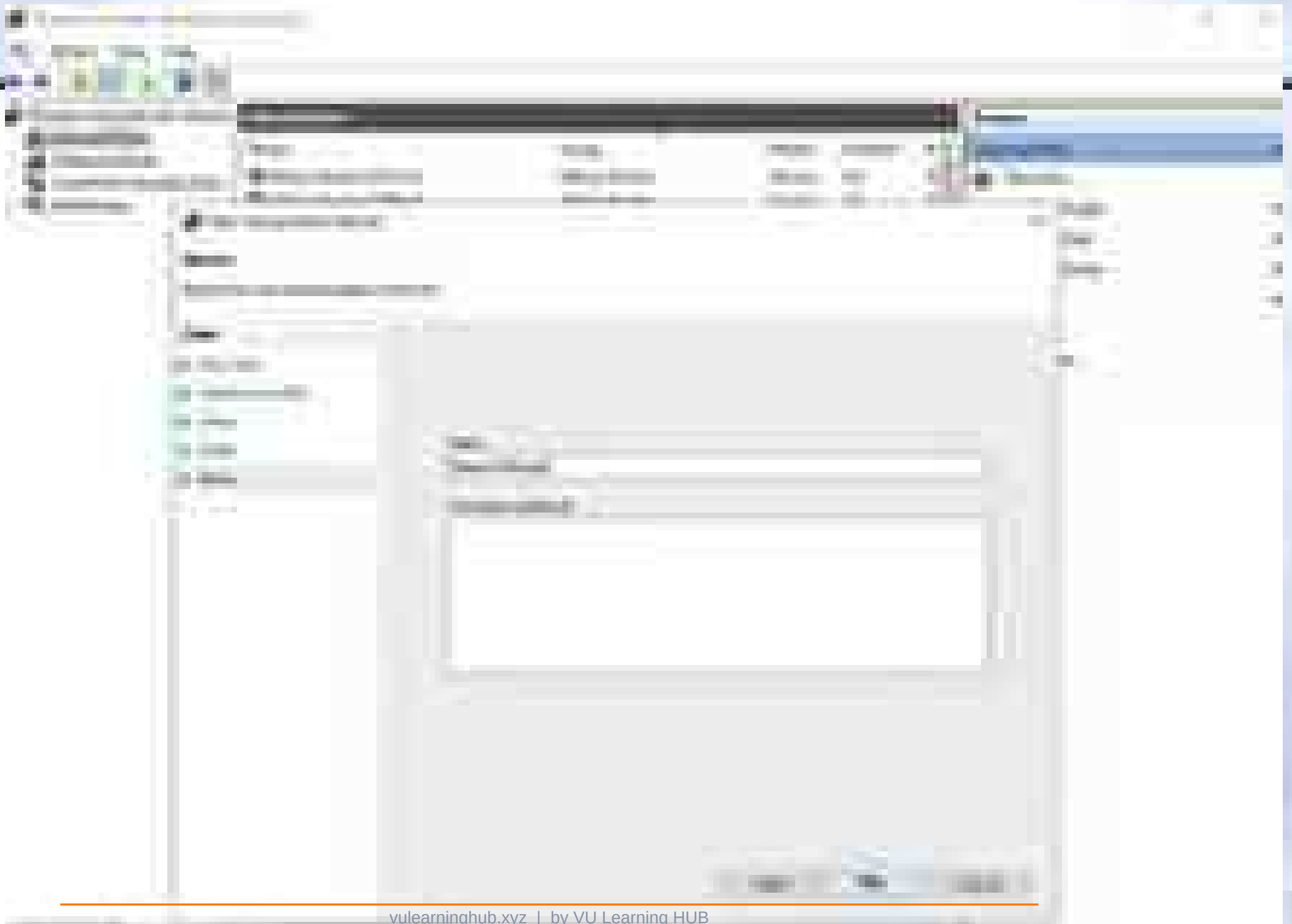












Year	Country	Population (millions)	Urban population (millions)	Urban population (%)	Population density (per sq km)	Urban population density (per sq km)	Population growth rate (%)	Urban population growth rate (%)	Population growth rate (%)	Urban population growth rate (%)	Population growth rate (%)	Urban population growth rate (%)
1950	Algeria	2.5	0.5	20	100	100	1.5	1.5	1.5	1.5	1.5	1.5
1955	Algeria	2.6	0.6	23	110	110	1.6	1.6	1.6	1.6	1.6	1.6
1960	Algeria	2.7	0.7	26	120	120	1.7	1.7	1.7	1.7	1.7	1.7
1965	Algeria	2.8	0.8	29	130	130	1.8	1.8	1.8	1.8	1.8	1.8
1970	Algeria	2.9	0.9	31	140	140	1.9	1.9	1.9	1.9	1.9	1.9
1975	Algeria	3.0	1.0	33	150	150	2.0	2.0	2.0	2.0	2.0	2.0
1980	Algeria	3.1	1.1	35	160	160	2.1	2.1	2.1	2.1	2.1	2.1
1985	Algeria	3.2	1.2	38	170	170	2.2	2.2	2.2	2.2	2.2	2.2
1990	Algeria	3.3	1.3	40	180	180	2.3	2.3	2.3	2.3	2.3	2.3
1995	Algeria	3.4	1.4	41	190	190	2.4	2.4	2.4	2.4	2.4	2.4
2000	Algeria	3.5	1.5	43	200	200	2.5	2.5	2.5	2.5	2.5	2.5
2005	Algeria	3.6	1.6	44	210	210	2.6	2.6	2.6	2.6	2.6	2.6
2010	Algeria	3.7	1.7	46	220	220	2.7	2.7	2.7	2.7	2.7	2.7
2015	Algeria	3.8	1.8	47	230	230	2.8	2.8	2.8	2.8	2.8	2.8
2020	Algeria	3.9	1.9	49	240	240	2.9	2.9	2.9	2.9	2.9	2.9
2025	Algeria	4.0	2.0	50	250	250	3.0	3.0	3.0	3.0	3.0	3.0
2030	Algeria	4.1	2.1	51	260	260	3.1	3.1	3.1	3.1	3.1	3.1
2035	Algeria	4.2	2.2	52	270	270	3.2	3.2	3.2	3.2	3.2	3.2
2040	Algeria	4.3	2.3	53	280	280	3.3	3.3	3.3	3.3	3.3	3.3
2045	Algeria	4.4	2.4	54	290	290	3.4	3.4	3.4	3.4	3.4	3.4
2050	Algeria	4.5	2.5	56	300	300	3.5	3.5	3.5	3.5	3.5	3.5
2055	Algeria	4.6	2.6	57	310	310	3.6	3.6	3.6	3.6	3.6	3.6
2060	Algeria	4.7	2.7	58	320	320	3.7	3.7	3.7	3.7	3.7	3.7
2065	Algeria	4.8	2.8	59	330	330	3.8	3.8	3.8	3.8	3.8	3.8
2070	Algeria	4.9	2.9	60	340	340	3.9	3.9	3.9	3.9	3.9	3.9
2075	Algeria	5.0	3.0	60	350	350	4.0	4.0	4.0	4.0	4.0	4.0
2080	Algeria	5.1	3.1	61	360	360	4.1	4.1	4.1	4.1	4.1	4.1
2085	Algeria	5.2	3.2	62	370	370	4.2	4.2	4.2	4.2	4.2	4.2
2090	Algeria	5.3	3.3	62	380	380	4.3	4.3	4.3	4.3	4.3	4.3
2095	Algeria	5.4	3.4	63	390	390	4.4	4.4	4.4	4.4	4.4	4.4
2100	Algeria	5.5	3.5	64	400	400	4.5	4.5	4.5	4.5	4.5	4.5

Accessing Nessus

1. First, ensure that the Nessus vulnerability scanner is installed on your system.
2. Once Nessus is installed, open a web browser (Chrome, Firefox, etc.) on the system you installed Nessus on.
3. In the web browser, navigate to the following URL: <https://localhost:8834/> OR <https://127.0.0.1:8834/>
4. If Nessus is running on the same system that you are accessing the web interface from, the Nessus login page should appear in your web browser.
5. Enter your Nessus username and password and click "Login" to access the Nessus web interface.

STEP 1 OF 3



Create an account

To use this scanner, an account must be created.
This account can execute commands on remote targets and should be treated as a root user.

Username *

Password *

Continue

STEP 3 OF 4



Register your scanner

Enter an activation code below to run your scanner locally or choose one of the dropdown options to run it in managed mode.

Scanner Type

Home, Professional or Manager

Activation Code *

[Settings](#)

[Back](#)

[Continue](#)

Step 1 of 3

Nessus®

Register your scanner

Enter an activation code below to run your scanner locally or choose one of the deployment options to run it in managed mode.

Scanner Type

Home, Professional or Manager

Activation Code *

Settings

Back

Continue

STEP 2 OF 4



Setup Complete

Please wait while we download and initialize the latest plugins.



Nessus Features

- Lets take a look at Nessus features

Nessus Features

- Nessus (Reports):
 - Customize reports to sort by vulnerability or host
 - Create an executive summary or compare scan results
 - Targeted email notifications of scan results

Nessus Features

- Nessus (Scan Types):
 - Asset discovery
 - Un-credentialed vulnerability discovery
 - Credentialed scanning for system hardening & missing patches

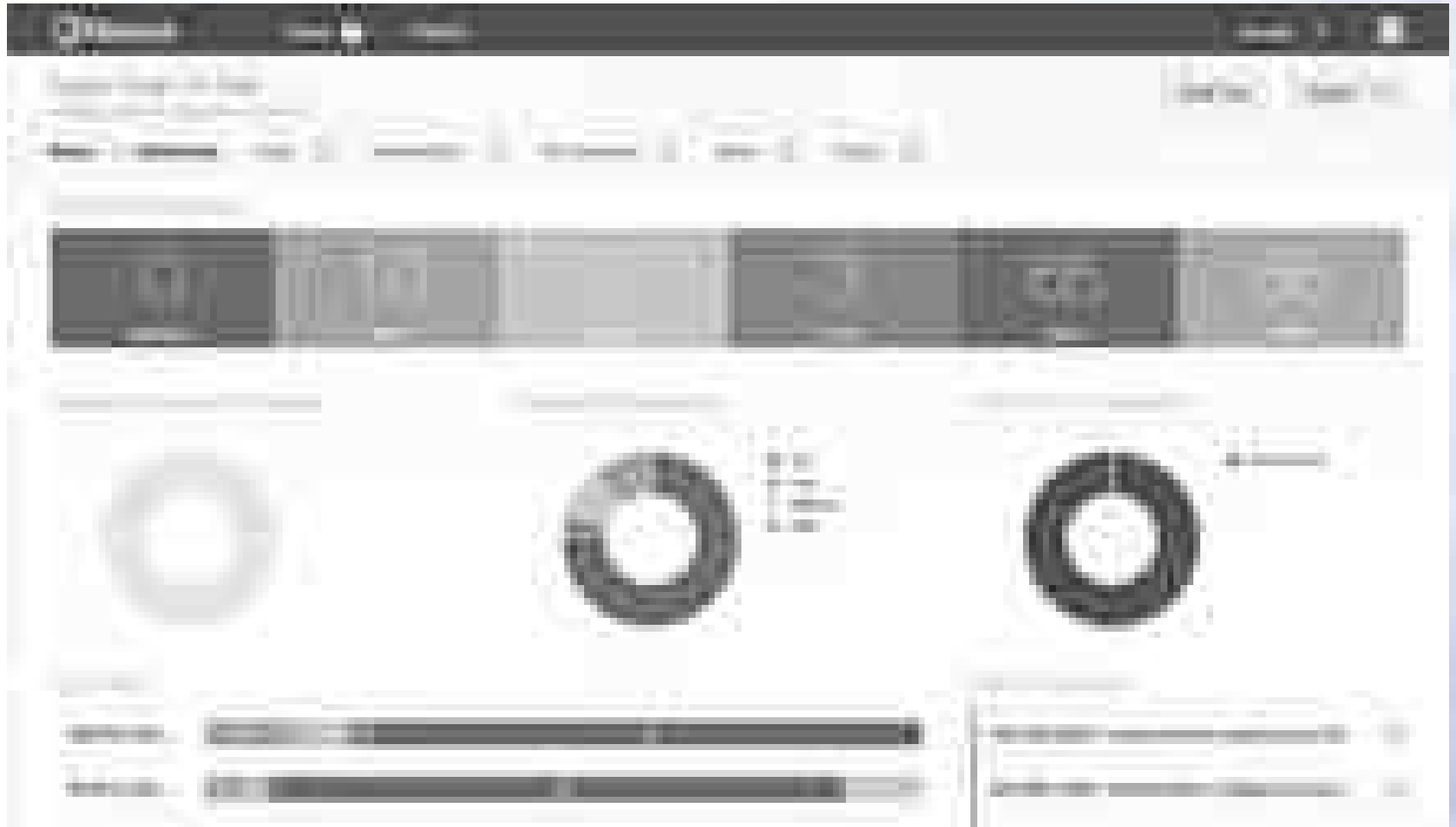
Nessus Features

- Nessus (Compliance & Config Scans):
 - Compliance auditing: FFIEC, FISMA, CyberScope, GLBA, HIPAA/
HITECH, NERC, PCI, SCAP, SOX
 - Configuration auditing: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC,
ISO, NIST, NSA

Nessus Features

- Nessus (Risk scores):
 - Vulnerability ranking based on CVE, five severity levels (Critical, High, Medium, Low, Info), customizable severity levels for recasting of risk

Nessus Features



Nessus Features



Nessus Features



Nessus Features

- Nessus is a cost-effective scanner that gets most of the job done for vulnerability scanning
- It has CIS and DISA compliance templates

Qualys Features

- Lets take a look at Qualys features

Qualys Features

- Qualys:
 - Cloud-based service
 - On-premise device
 - Complete suite
 - Scalable and immediate deployment

Qualys Features

- Qualys:
 - Asset discovery; find and organize hosts
 - Prioritize & manage remediation tickets
 - Continuous monitoring service
 - Policy compliance scanning
 - Qualys Secure Seal for websites

Qualys Features



Qualys Features



Qualys Features

[illegible]

Qualys Features



Qualys Features



Secure Seal

- A Secure Seal for websites refers to a visual indicator, such as a badge or logo, displayed on a website to indicate that the site has been verified and is secure.
- The purpose of the secure seal is to assure visitors that the website is legitimate, trustworthy, and has taken measures to protect the privacy and security of their personal and financial information.

QUALYS FEATURES



FILE INTEGRITY MONITORING

QUALYS FEATURES



SEARCH KNOWLEDGEBASE

QUALYS FEATURES

Item	Unit	Quantity	Unit Price	Total Price
1.000	kg	1.000	1.000	1.000
2.000	kg	2.000	2.000	2.000
3.000	kg	3.000	3.000	3.000
4.000	kg	4.000	4.000	4.000
5.000	kg	5.000	5.000	5.000
6.000	kg	6.000	6.000	6.000
7.000	kg	7.000	7.000	7.000
8.000	kg	8.000	8.000	8.000
9.000	kg	9.000	9.000	9.000
10.000	kg	10.000	10.000	10.000

CISCO VULNERABILITIES – PATCH AVAILABLE

Qualys Features

- Qualys:
 - Website scanning
 - Annual subscription service model
 - Qualys is a convenient and scalable VM tool that comes with several modules
 - Several advantages due to cloud-based service

QUALYS DEMO - PART 2

- Lets have a look at the Qualys features

QUALYS DEMO - PART 2



QUALYS 14 APPLICATIONS

QUALYS DEMO - PART 2



VULNERABILITY MANAGEMENT DASHBOARD

QUALYS DEMO - PART 2

Launch Vulnerability Scan

General Information

Specify the system used to scan vulnerability issues & provide the scan parameters settings, and assign a security service to the scan.

Scan Type:

Scan Profile: 

Scanning Policy: 

Source Network:   

Choose Target (Hosts) from:

☐ New ☐ Existing

Host Name:   

IP Range: 

Source IP Range: 

☐ Scan system configuration

Notification

☐ Send notification via email

LAUNCH VULNERABILITY SCAN

QUALYS DEMO - PART 2



VULNERABILITY MANAGEMENT DASHBOARD

QUALYS DEMO - PART 2

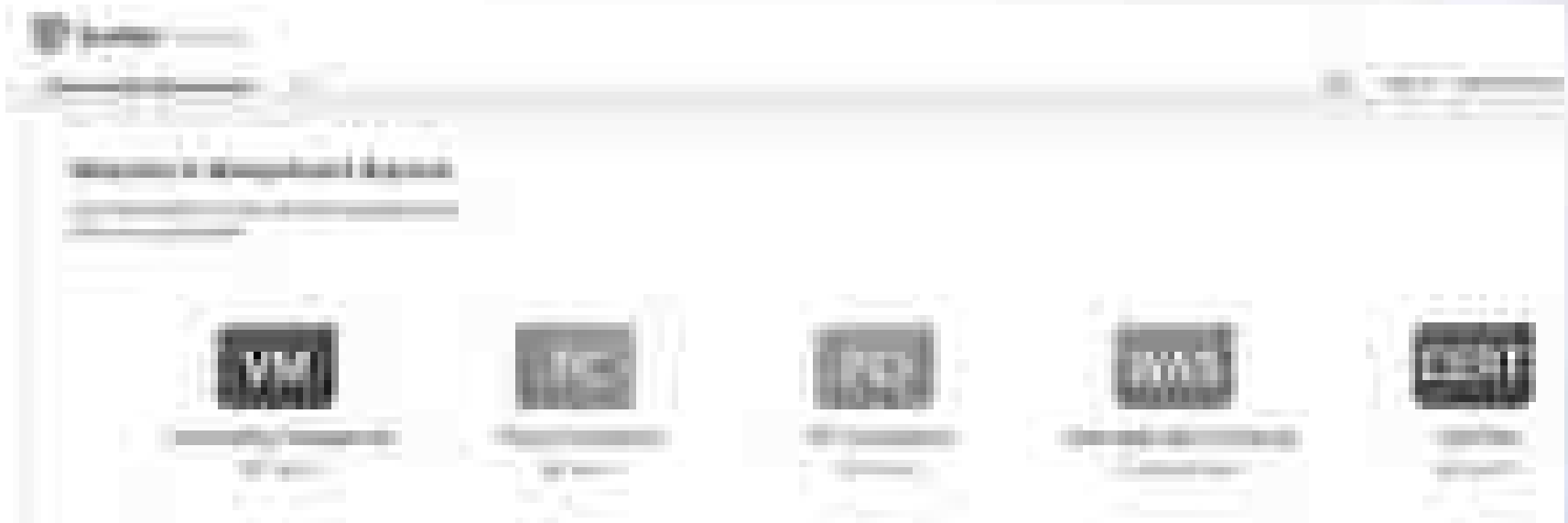


SCAN TUTORIALS

QUALYS DEMO – SECURITY HARDENING

- Lets have a look at how Qualys can aid in the security hardening process

QUALYS DEMO – SECURITY HARDENING



QUALYS GUARD – HOME SCREEN

QUALYS DEMO – SECURITY HARDENING



POLICY COMPLIANCE – HOME SCREEN

QUALYS DEMO – SECURITY HARDENING



POLICY COMPLIANCE – 5 STEPS

QUALYS DEMO – SECURITY HARDENING



HELP OPTIONS

QUALYS DEMO – SECURITY HARDENING



ONLINE HELP – POLICY COMPLIANCE

QUALYS DEMO – SECURITY HARDENING



RESOURCES

QUALYS DEMO – SECURITY HARDENING



QUALYS WEBSITE - TRAINING

QUALYS DEMO – SECURITY HARDENING



TRAINING VIDEOS - VIMEO

QUALYS DEMO – SECURITY HARDENING

- Qualys is an excellent tool with detailed online help, training, and resources to aid the new user

END

QUALYS DEMO – SECURITY HARDENING II

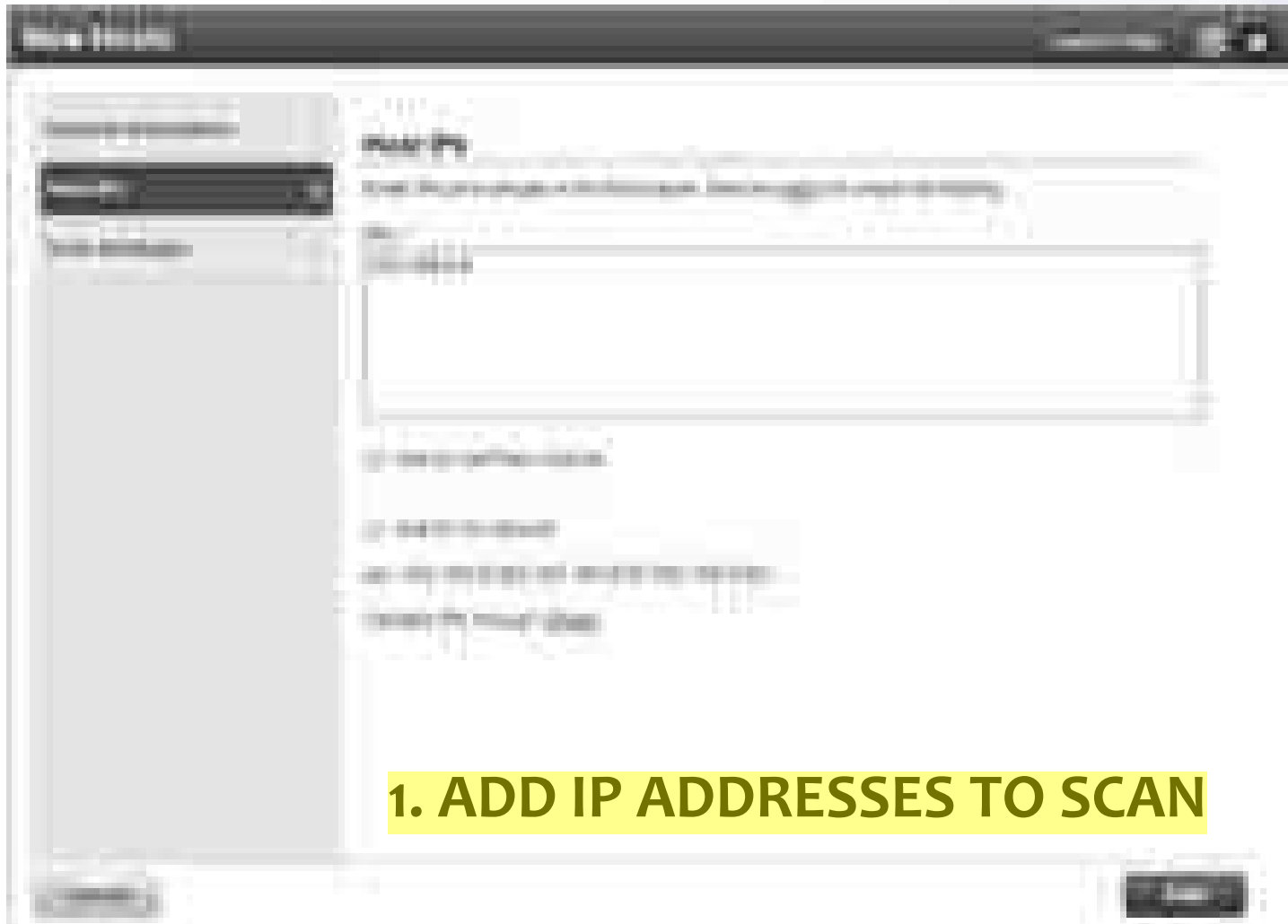
- Lets have a detailed look at Qualys interface for Policy Compliance

QUALYS DEMO – SECURITY HARDENING II



1. ADD IP ADDRESSES TO SCAN

QUALYS DEMO – SECURITY HARDENING



1. ADD IP ADDRESSES TO SCAN

QUALYS DEMO – SECURITY HARDENING



2. CONFIGURE SCAN SETTINGS

QUALYS DEMO – SECURITY HARDENING

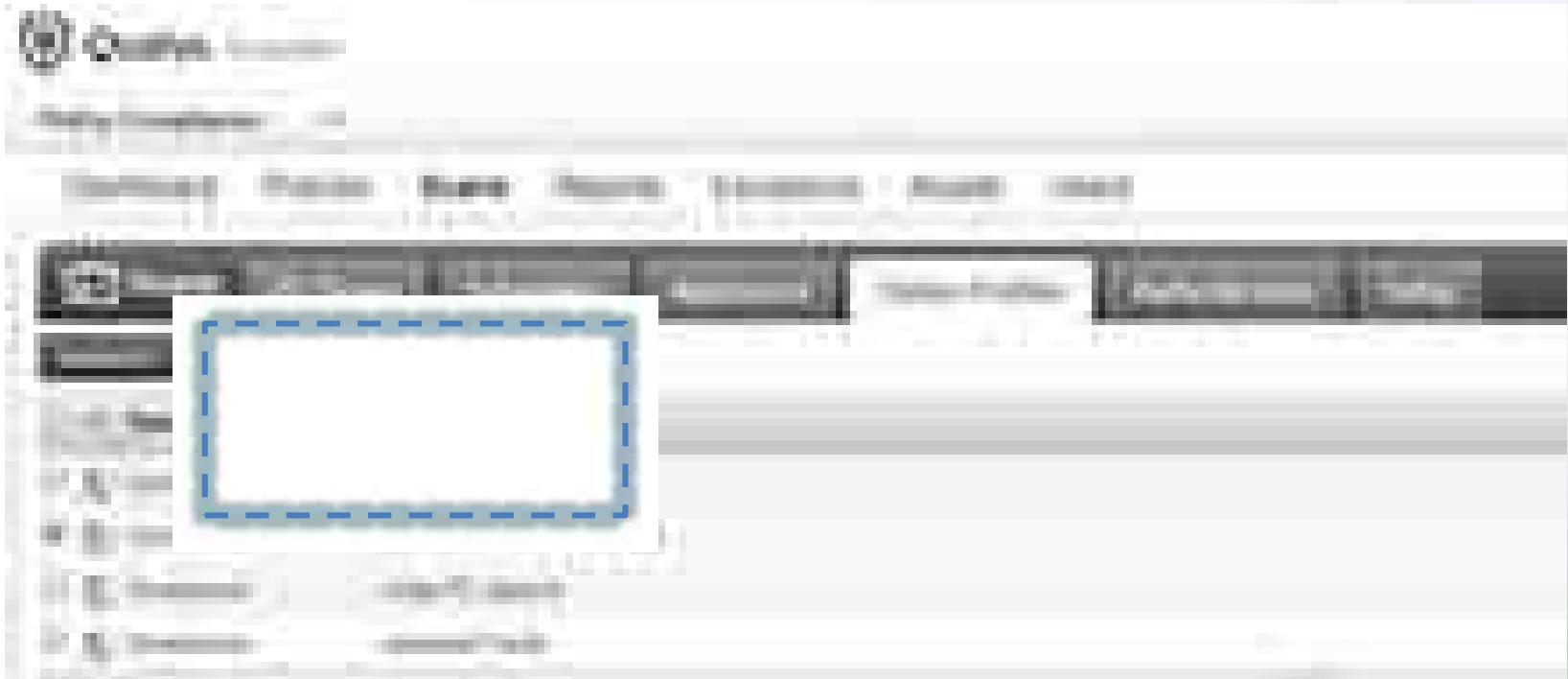


The screenshot displays the 'Compliance Profile Information' page in the Qualys interface. The left sidebar shows a navigation menu with 'Scan Settings' highlighted. The main content area lists various security settings and their current status.

Setting	Status
Allow installation of Policy	On
Block	On
Block (Update Prevention)	On
Block	On
Control Items	On
File Integrity Monitoring (FIM)	On
Control Item (Log Check)	On
Generate Agent	On
Generate Agent (for installation)	On
Password Building Controls	On
Windows Store (Installation)	On
Windows Firewall Settings	On
Win OS (Security)	On
None	On
Scanned Profile	Target Scan
Scans by Scan ID (Target)	On
Use Advanced Password M. Building	On
External Security	On
External Security	On
Processing (to be in Profile)	On
Total	On
Off (to)	On

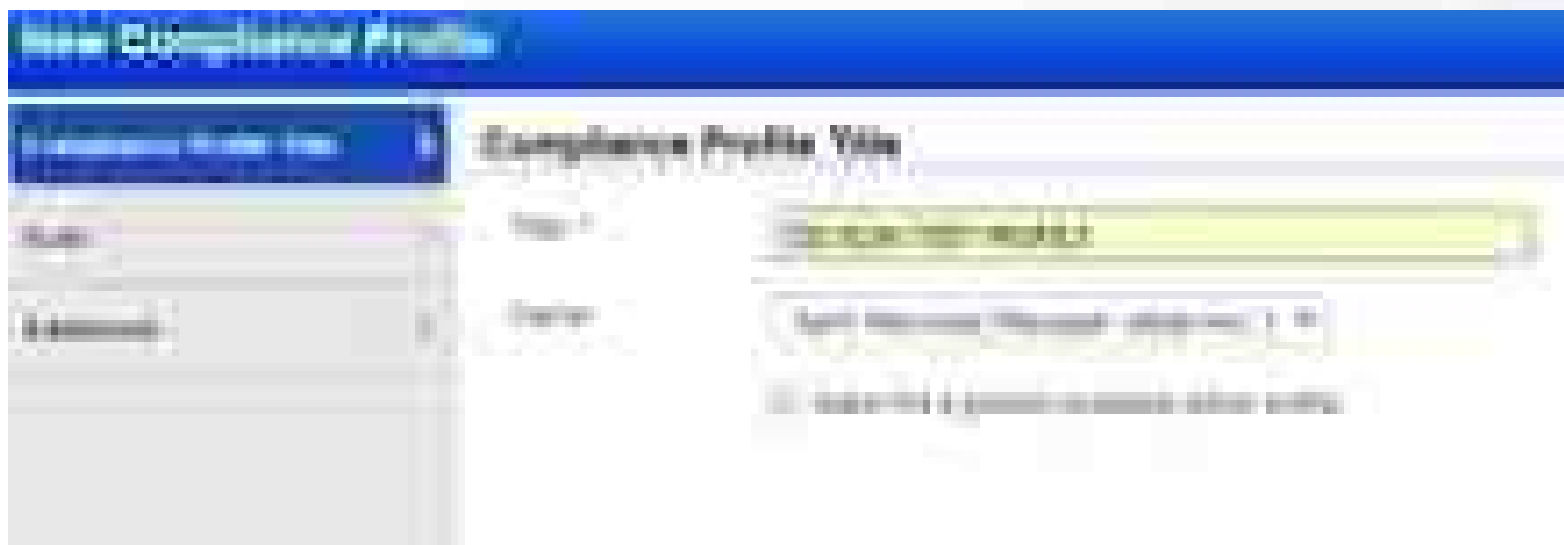
2. CONFIGURE SCAN SETTINGS

QUALYS DEMO – SECURITY HARDENING



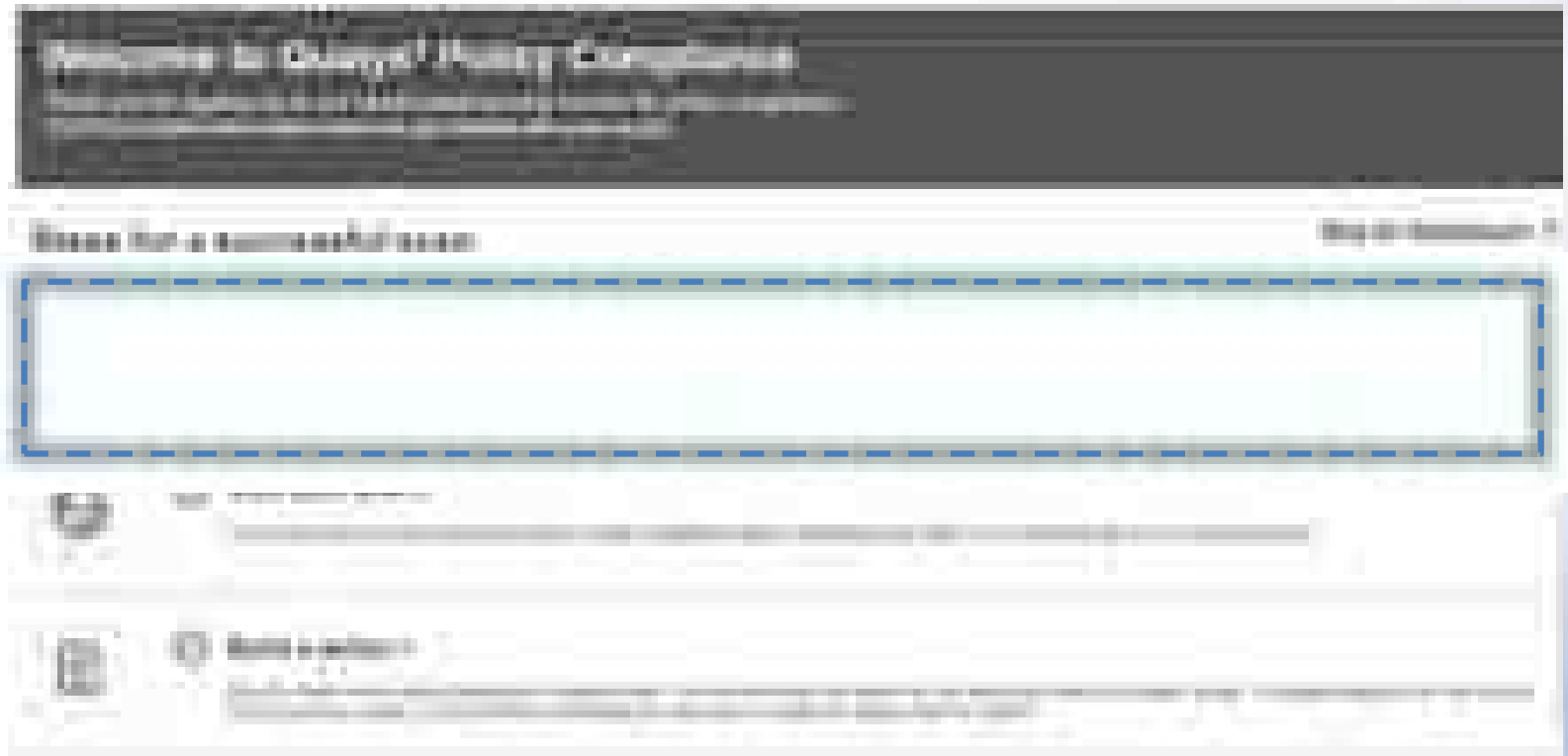
NEW COMPLIANCE PROFILE

QUALYS DEMO – SECURITY HARDENING



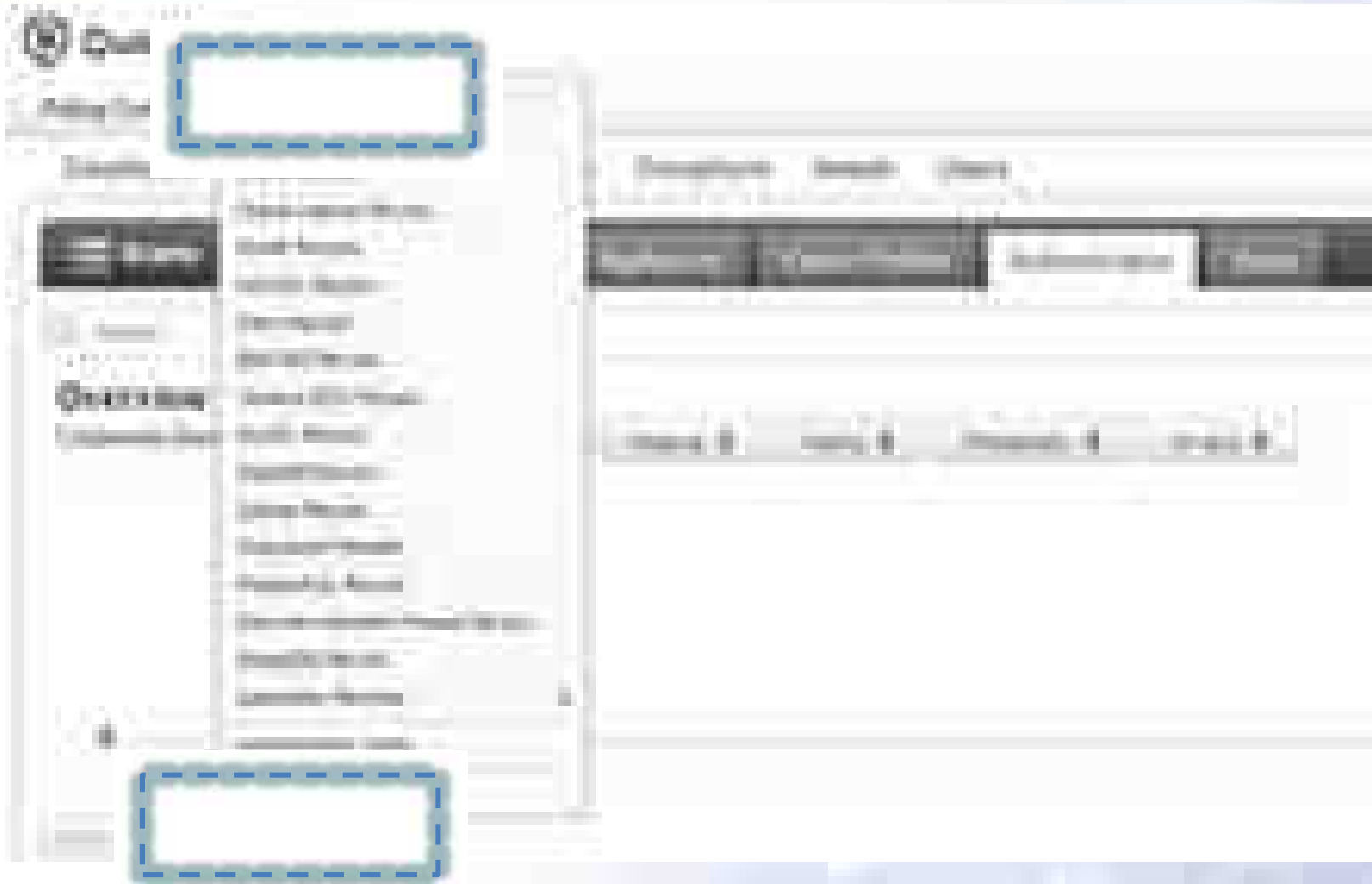
‘CIS SCAN TEST PROFILE’ CREATED

QUALYS DEMO – SECURITY HARDENING

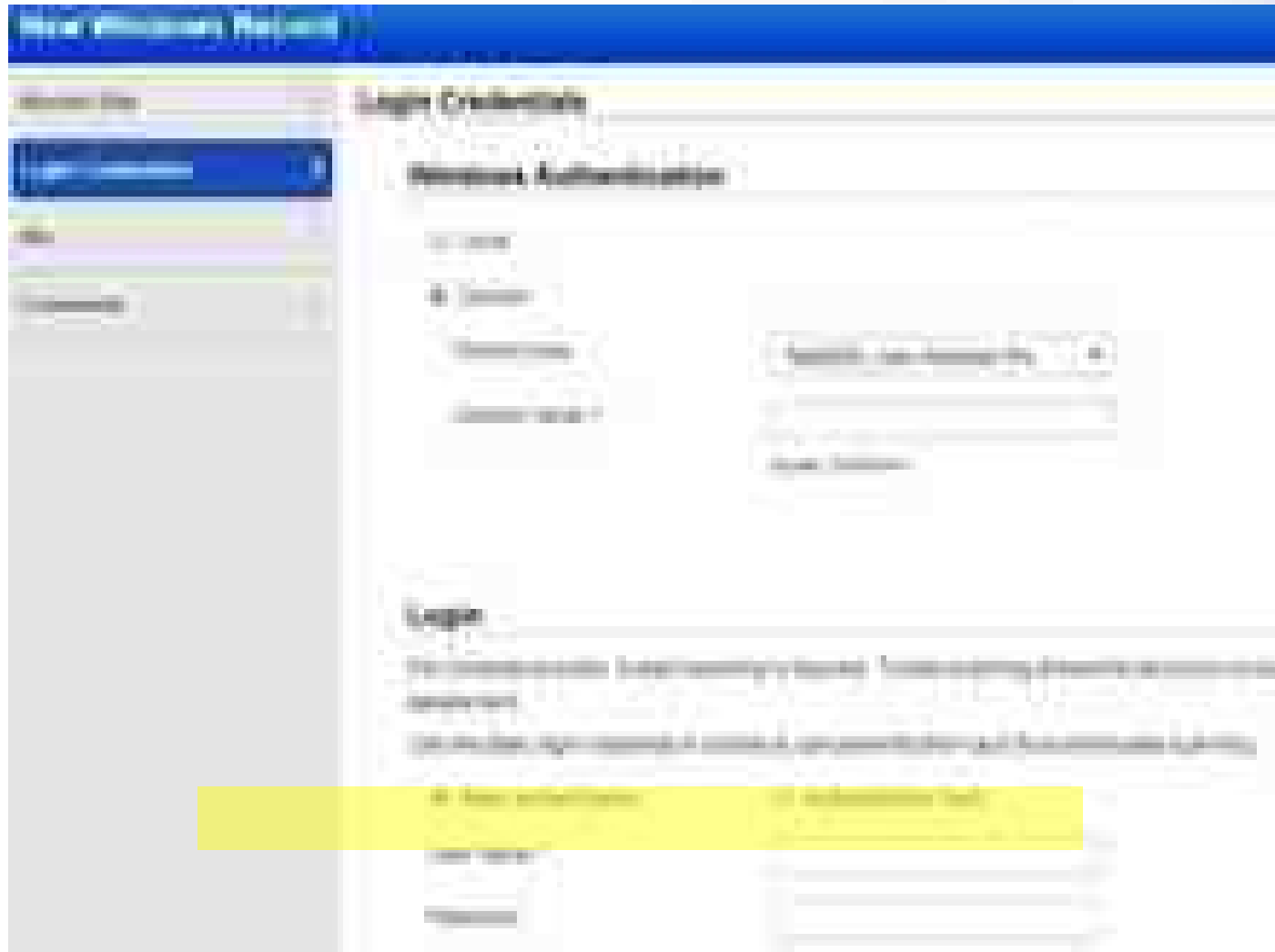


3. CONFIGURE AUTHENTICATION

QUALYS DEMO – SECURITY HARDENING



QUALYS DEMO – SECURITY HARDENING

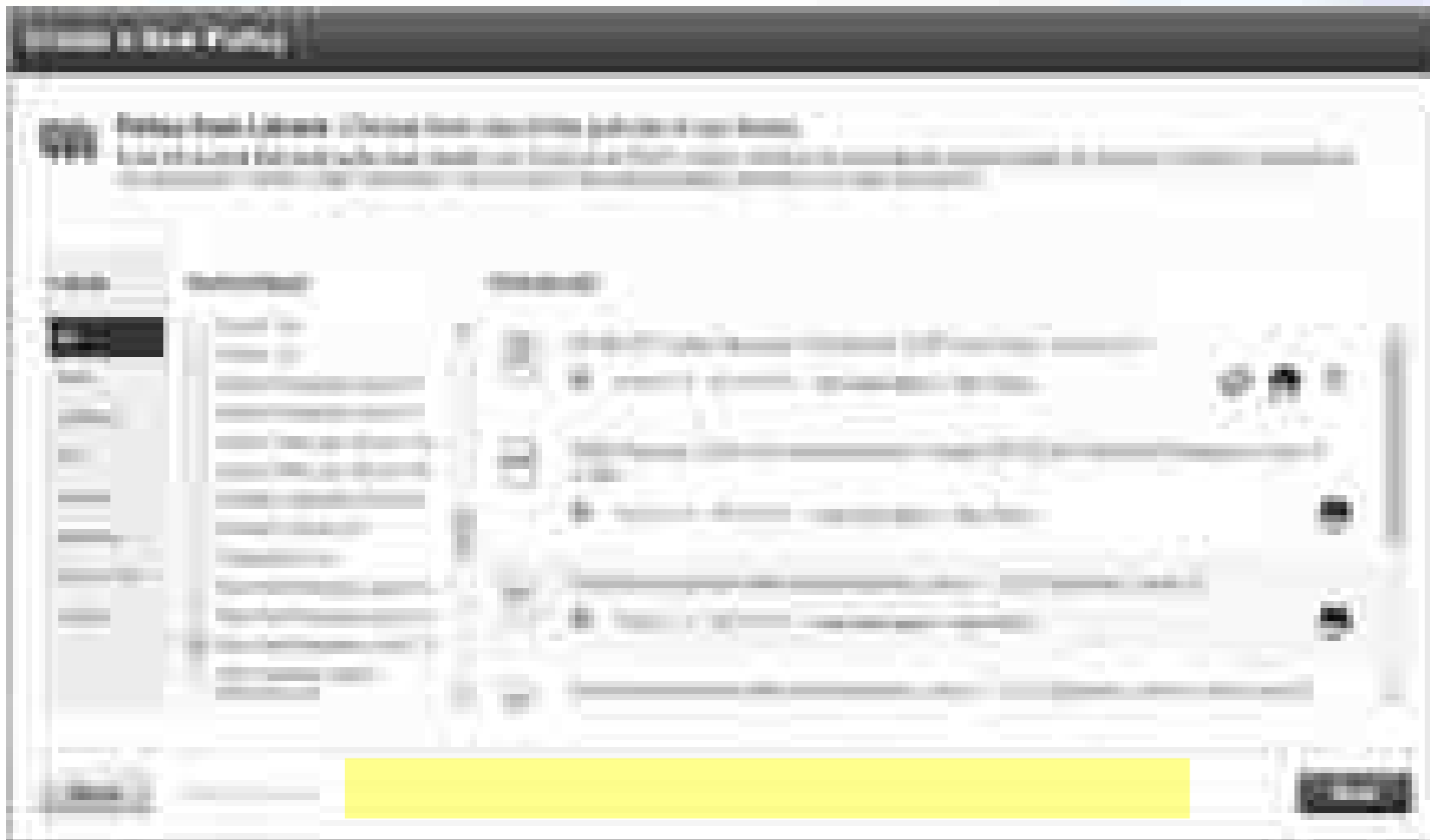


QUALYS DEMO – SECURITY HARDENING



3. CONFIGURE AUTHENTICATION

QUALYS DEMO – SECURITY HARDENING



COMPLIANCE LIBRARY: CIS RED HAT ENT. LINUX 7

QUALYS DEMO – SECURITY HARDENING



POLICY EDITOR

QUALYS DEMO – SECURITY HARDENING

Launch Compliance Scan

General Information
This section is used to provide information about the scan to be performed. It includes the scan name, the target host, and the scan type.

Scan Name

Start Date

End Date

Target Host

Scan Type

Choose Target Hosts
This section is used to choose the target hosts for the scan. It includes a list of hosts and a search bar.

Hosts

Search

Hosts

Search

Hosts

Search

LAUNCH COMPLIANCE SCAN

QUALYS DEMO – SECURITY HARDENING II

- The scan features may also be adjusted from the main Qualys dashboard

END