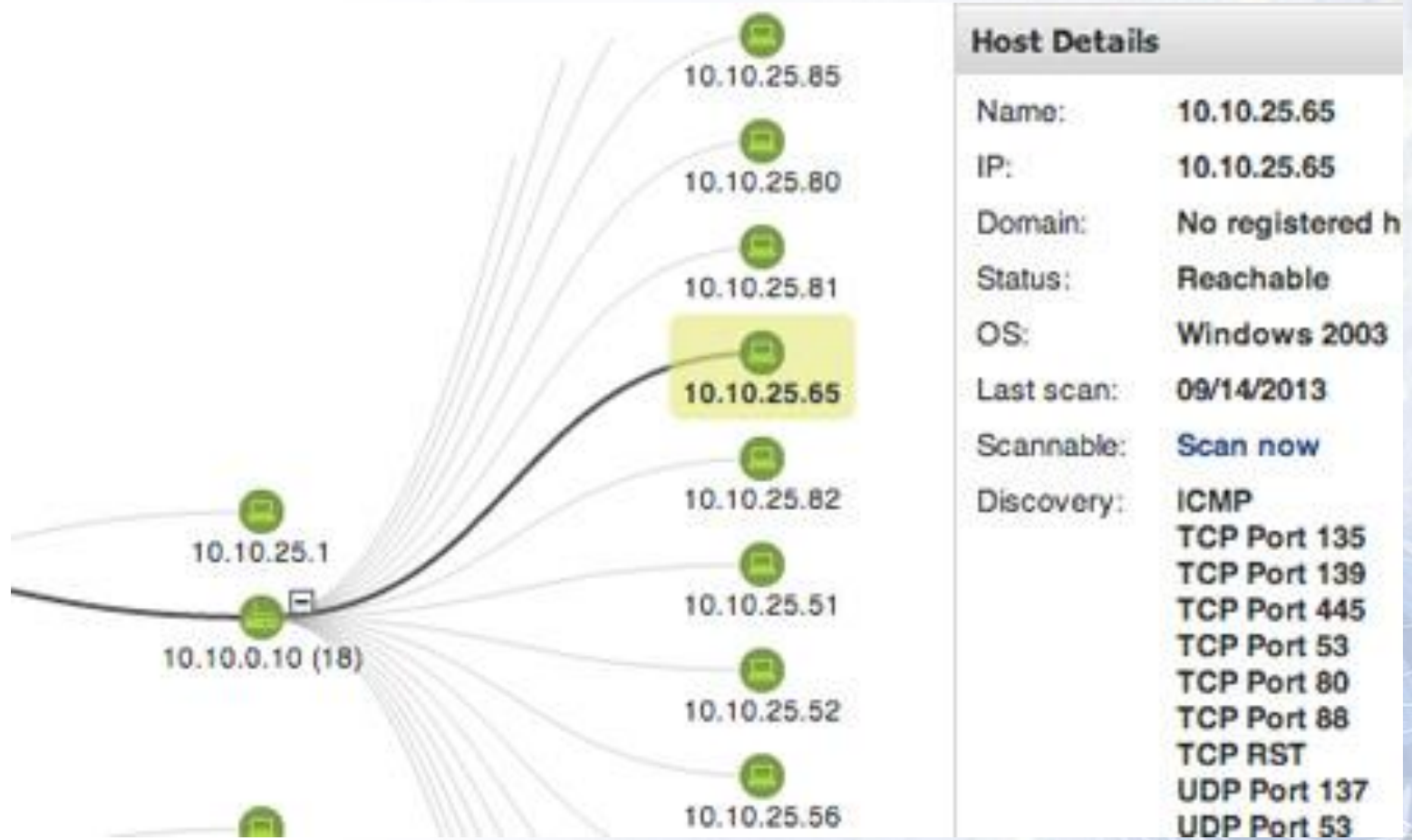
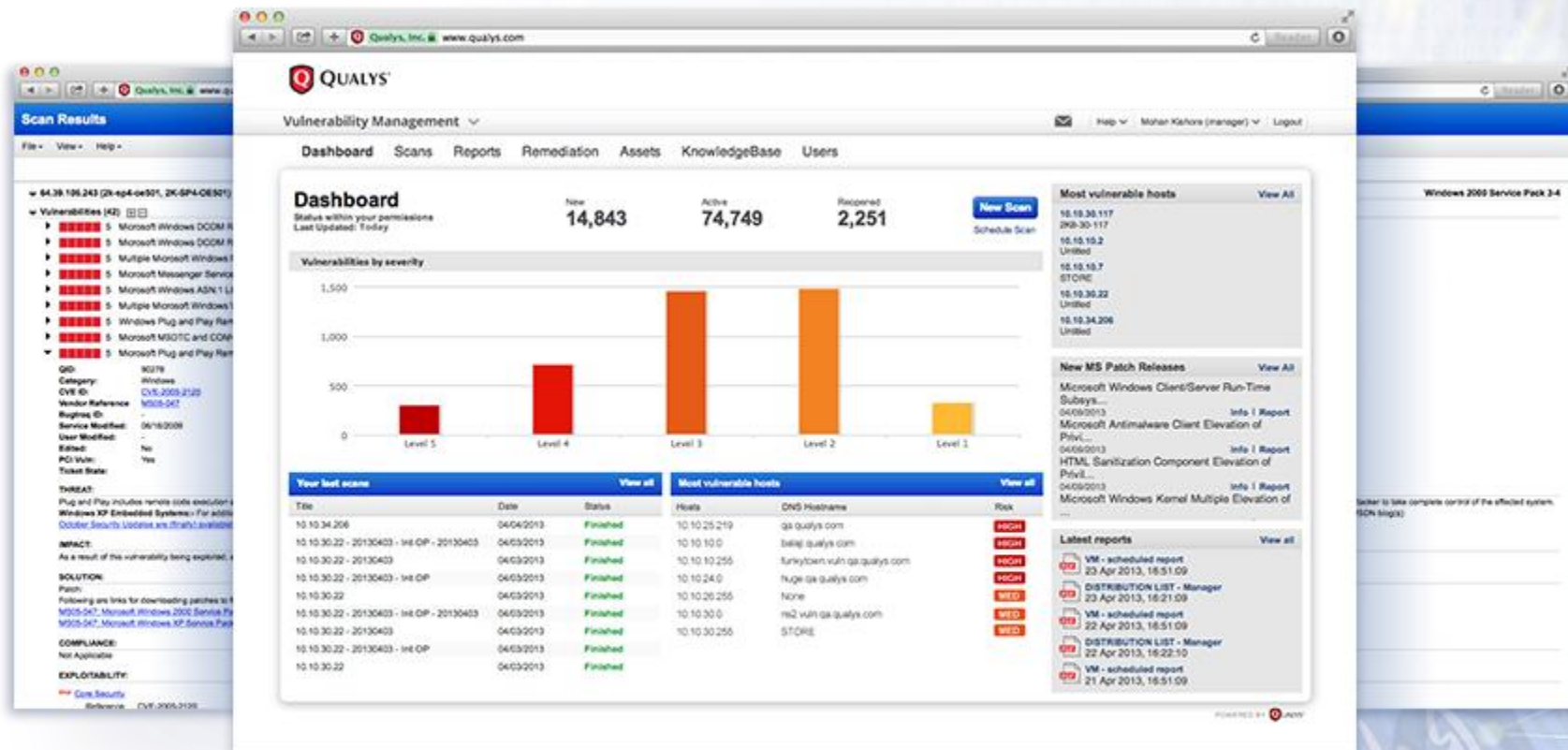


Qualys Features



Qualys Features



Qualys Features

Patch Report

Report Summary

Agency: Qualys Training
 Created by: Philip Niegos
 Created on: 01/10/2014

Total
Patches

149

Hosts Requiring
Patches

14

Vulnerabilities
Addressed

156

[Report Targets...](#)

HOSTS				PATCHES required on '192.168.1.211' (41)			
DNS Name	NetBIOS	OS	Patches	Vendor ID	Sev.	Title	Published
1.2... centos5.lab.local		CentOS 5.10	41	Apache1.3, A...	3	Apache 1.3 and 2.0 Web Server Multiple ...	6 years ago
1.2... cisco.lab.local		Cisco IOS 12.2(13)ZHI, EA...	40	FEDORA-200...	3	APR-util Library Integer Overflow Vulnera...	4 years ago
1.2... centos6.lab.local		CentOS 6.4	16	Apache 2.2.15	4	Apache HTTP Server Prior to 2.2.15 Multi...	3 years ago
1.2... windows8_1.lab.local	WINDOWSS...	Windows 8.1 Enterprise	10	Tomcat5, To...	3	Apache Tomcat Directory Traversal Weak...	3 years ago
1.2... ws2k8r2.lab.local	WS2K8R2	Windows Server 2008 R2 E...	9	Apache Tomc...	3	Apache Tomcat Servlet Host Manager Ser...	5 years ago
1.2... winserver2012.lab.lo...	WINSERVE...	Windows Server 2012 Stand...	7	Apache Tomc...	3	Apache Tomcat 5 and 6 Host Manager W...	5 years ago
1.2... vistax64.lab.local	VISTAX64	Windows Vista 64 bit Editio...	6	Tomcat4, To...	3	Apache Tomcat RequestDispatcher Infor...	5 years ago
1.2... win7x64.lab.local	WIN7X64	Windows 7 Ultimate 64 bit ...	5	Apache Tomc...	3	Apache Tomcat Java AJP Connector Invali...	4 years ago
Page 1 of 1	Filter	X	1 - 14 of 14	Page 1 of 2	Filter	X	

Qualys Features

The screenshot displays the QualysGuard KnowledgeBase interface. At the top, the QualysGuard logo is visible. Below it, a navigation bar includes 'Vulnerability Management' and a dropdown arrow. A secondary navigation bar contains links for 'Dashboard', 'Scans', 'Reports', 'Remediation', 'Assets', 'KnowledgeBase' (which is highlighted), and 'Users'. The KnowledgeBase section has a blue header with tabs for 'KnowledgeBase', 'Predictions', 'Search Lists', and 'iDefense Intelligence'. Below the tabs, there are 'New' and 'Search' buttons. The main content area is a table of vulnerabilities.

QID	Title	Severity	Category	CVE ID	Vendor R
1013	Hack a Tack backdoor detected	5	Backdoors and trojan horses		
1015	"NetBus" Backdoor	5	Backdoors and trojan horses		
1020	Potential Remote Shell Trojan	5	Backdoors and trojan horses		
1021	Installed Back Orifice 2000	5	Backdoors and trojan horses		
1135	Sasser Worm Detected	5	Backdoors and trojan horses		

Qualys Features

The image displays the Qualys SECURE SEAL interface. At the top, the Qualys logo is followed by the text "QUALYS® SECURE SEAL". Below this is a navigation bar with a home icon, the text "Qualys SECURE Seal", and a dropdown menu showing the URL "http://funkytown.vuln.qa.qualys.com". The main content area shows the same URL. On the left, there is a sidebar with links: "Results" (with a magnifying glass icon), "History" (with a clock icon), "Exceptions" (with a document icon), and "Recommend to Others" (with a person icon). Below these links is a "Filter Results" section with three checkboxes: "Perimeter", "Web Application", and "Malware". The main content area displays the "Seal Status: FAIL" in red, "Scan Status: Finished" in blue, and the "URL: http://funkytown.vuln.qa.qualys.com/cassium/xs" followed by the IP address "10.10.26.77". At the bottom, there are four circular icons representing different security checks: "Perimeter" (cloud icon with a red X), "Web App" (document icon with a red X), "Malware" (biohazard icon with a green checkmark), and "Certificate" (lock icon with a red X).

QUALYS® SECURE SEAL

Qualys SECURE Seal <http://funkytown.vuln.qa.qualys.com>

<http://funkytown.vuln.qa.qualys.com>

Results

History

Exceptions

Recommend to Others

Filter Results

- ☐ Perimeter
- ☐ Web Application
- ☐ Malware

Seal Status: **FAIL**

Scan Status: **Finished**

URL: <http://funkytown.vuln.qa.qualys.com/cassium/xs>
10.10.26.77

Perimeter Web App Malware Certificate

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 ▾

DASHBOARDEVENTSINCIDENTSASSETSCONFIGURAT

FIM

Welcome to Qualys® File Integrity Monitoring

Built on our revolutionary Cloud Agent technology, Qualys FIM logs and centrally tracks file change events and alerts. You're all set and ready to get started!

Get started with these quick steps

1

Install Cloud Agents (using CA) >
Go to Cloud Agent (CA) to install and activate agents on the systems you want to monitor. When you're done, return to FIM and continue to the next step.

2

Configure monitoring profiles >
Associate a set of rules with the assets you want to monitor (assign directly or use asset tags). Import a profile from our Library or create a new profile.

3

View your events >
Check out the events detected on your assets and search for specific event details.



All agent installations are managed in Qualys Cloud Agent. We'll help you create activation keys, download and install agents and activate your agents for FIM.

Take me to Qualys Cloud Agent

FILE INTEGRITY MONITORING

QUALYS FEATURES

Search ×

Category: ☐ NOT

Patch Solution: ☒ Patch Available
☐ Trend Micro Virtual Patch Available
☐ No Patch Solution

CVE ID: ☐ NOT

CPE:

Exploitability:

Associated Malware:

Vendor Reference: ☐ NOT

CVSS Base Score:

Search

SEARCH KNOWLEDGEBASE

QUALYS FEATURES

Vulnerability Management				
Dashboard Scans Reports Remediation Assets KnowledgeBase Users				
KnowledgeBase				
QID	Title		Category	CVE ID
87347	Cisco Data Center Network Manager Path Traversal Vulnerability		Web server	CVE-2018-0464
316166	Cisco Email Security Appliance and Content Security Management Appliance HTTP Response Splitting Vulnerability (cisco-sa-20171115-esa)		Cisco	CVE-2017-12309
38728	Cisco TelePresence VCS Denial of Service Vulnerability(cisco-sa-20180815-uomimps-dos)		General remote services	CVE-2018-0409
316315	Cisco Unity Connection Apache Struts Remote Code Execution Vulnerability(cisco-sa-20180823-apache-struts)		Cisco	CVE-2018-11776
316314	Cisco Unified Communications Manager IM And Presence Service Apache Struts Remote Code Execution Vulnerability(cisco-sa-20180823-apache-struts)		Cisco	CVE-2018-11776
316313	Cisco Unified Communications Manager Apache Struts Remote Code Execution Vulnerability(cisco-sa-20180823-apache-struts)		Cisco	CVE-2018-11776
87350	Cisco Data Center Network Manager Cross-Site Scripting Vulnerability(cisco-sa-20180905-dcnm-xss)		Web server	CVE-2018-0450

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

You have 14 applications available in your subscription

PCI Compliance

Achieve compliance with the PCI Data Security Standard (DSS).

[Visit now](#)

AssetView

Discover assets and use dynamic tags to keep your assets automatically organized.

[Visit now](#)

Cloud Agent

Stay updated with network security by deploying agents on your hosts.

[Visit now](#)

Vulnerability Management

Map and scan your network, prioritize your critical vulnerabilities and fix them.

[Visit now](#)

Continuous Monitoring

Set up monitoring and alerting of new security risks

[Visit now](#)

Administration

Control user access permissions and activity in your subscription.

[Visit now](#)

Threat Protection

Add threat intelligence feed to your existing AssetView

[Visit now](#)

Policy Compliance

Define, Audit and Document IT Security Compliance

[Visit now](#)

Security Assessment Questionnaire

Automate risk and compliance through questionnaire campaigns.

[Visit now](#)

Web Application Scanning

Identify and manage web application security risks.

[Visit now](#)

Web Application Firewall

Detect attacks and protect your web applications.

[Visit now](#)

Malware Detection

Identify and manage web site malware risks.

[Visit now](#)

File Integrity Monitoring

Monitor changes on file systems

[Visit now](#)

Certificate View

Analyse and manage SSL/TLS certificates and vulnerabilities

[Visit now](#)

QUALYS

14 APPLICATIONS

QUALYS DEMO - PART 2

 Qualys. Express

Vulnerability Management

Dashboard Scans Reports Remediation Assets KnowledgeBase Users

Scans Scans Maps Schedules Appliances Option Profiles Authentication Search Lists Setup

Actions (0) New Search Filters

☐	Title	Targets	User	Reference
☐	 internal tst	192.168.0.103	Nahil Mahmood	scan/1536503914.55170
☐	 Certview FreeScheduledScan2018-07-04T14:03:12.881Z	192.168.0.103	Nahil Mahmood	scan/1534321994.94111
☐	 Certview FreeScheduledScan2018-07-04T14:03:12.881Z	192.168.0.103	Nahil Mahmood	scan/1533717201.49301
☐	 Certview FreeScheduledScan2018-07-04T14:03:12.881Z	192.168.0.103	Nahil Mahmood	scan/1533112468.01806
☐	 Certview FreeScheduledScan2018-07-04T14:03:12.881Z	192.168.0.103	Nahil Mahmood	scan/1532507598.57569
☐	 Certview FreeScheduledScan2018-07-04T14:03:12.881Z	192.168.0.103	Nahil Mahmood	scan/1531902800.14745
☐	 Certview FreeScheduledScan2018-07-04T14:03:12.881Z	192.168.0.103	Nahil Mahmood	scan/1531297997.70529
☐	 Certview FreeScan 2018-07-04T14:11:11.988Z	192.168.0.103	Nahil Mahmood	scan/1530713485.27682
☐	 Certview FreeScan 2018-07-04T14:03:15.421Z	192.168.0.103	Nahil Mahmood	scan/1530713013.27660
☐	 WAF and Website	192.168.0.103	Nahil Mahmood	scan/1530003752.74867

VULNERABILITY MANAGEMENT DASHBOARD

QUALYS DEMO - PART 2

Launch Vulnerability Scan

General Information

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from the

Title:

Option Profile: * [Select](#)

Processing Priority:

Scanner Appliance: [View](#)

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

☒ Assets ☐ Tags

Asset Groups [Select](#)

IPs/Ranges [Select](#)
Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges [Select](#)
Example: 192.168.0.87-192.168.0.92, 192.168.0.200

☐ Scan agent hosts in my target

Notification

☒ Send notification when this scan is finished

LAUNCH VULNERABILITY SCAN

QUALYS DEMO - PART 2

Scan Status (scan/1537463084.29199)

General Information >

Scanners >

Option Profile >

Targets >

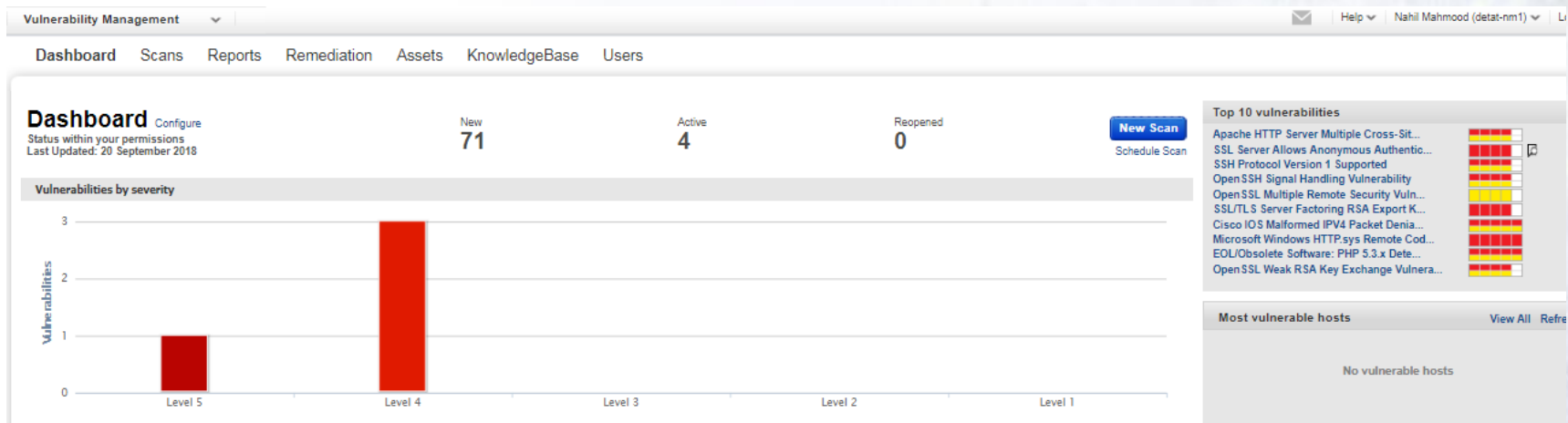
Scan Overview

Scan Information

Scan Title:	NEW SCAN
Launch Date:	09/20/2018 at 22:04:44 (GMT+0500)
Status:	Queued
Total IPs Scanned:	0
Scanner Appliance:	...

SCAN INITIATED

QUALYS DEMO - PART 2



VULNERABILITY MANAGEMENT DASHBOARD

QUALYS DEMO - PART 2

[Dashboard](#) [Scans](#) [Reports](#) [Remediation](#) [Assets](#) [KnowledgeBase](#) [Users](#)

 **Scans**

[Scans](#) [Maps](#) [Schedules](#) [Appliances](#) [Option Profiles](#) [Authentication](#) [Search Lists](#) [Setup](#)

 **Get Started Tutorials: Scans**

☐ Do not show tutorials

This is where you can manage your vulnerability scans and your scan configurations.

**Manage Vulnerability Scans**
Launch new vulnerability scans, monitor the status of running scans and view the details of vulnerabilities discovered after scans complete.
Watch demo  (8min 0sec)

**Configure Scan Schedules**
Configure scans to run automatically, or on a recurring basis and monitor results of your scans.
Watch demo  (4min 0sec)

**Manage Discovery Scans**
Use free discovery scans (maps) to discover live devices on your network. Discovered devices can be selected for vulnerability scanning based on the info gathered (OS, ports, etc.) in a map.
Watch demo  (6min 6sec)

**Configure Scanner Appliances**
Scanner Appliances (physical or virtual) are required to scan devices on internal networks. Managers can download appliances and configure them for scanning.

**Configure Scan Settings**
Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. A default profile is provided for common environments.
Watch demo  (9min 28sec)

**Set Up Host Authentication**
Use the authentication feature (Windows, Linux, Oracle, etc) to discover and validate vulnerabilities by performing an in-depth assessment of your hosts.
Watch demo  (9min 28sec)

**Configure Search Lists**
Apply custom lists of vulnerabilities to scan profiles in order to limit scanning to certain vulnerabilities only.

SCAN TUTORIALS

7

QUALYS DEMO - PART 2

Launch Vulnerability Scan

General Information

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner.

Title:

Option Profile: * [Select](#)

Processing Priority:

Scanner Appliance: [View](#)

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

☒ Assets ☐ Tags

Asset Groups [Select](#)

IPs/Ranges [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

☐ Scan agent hosts in my target

Notification

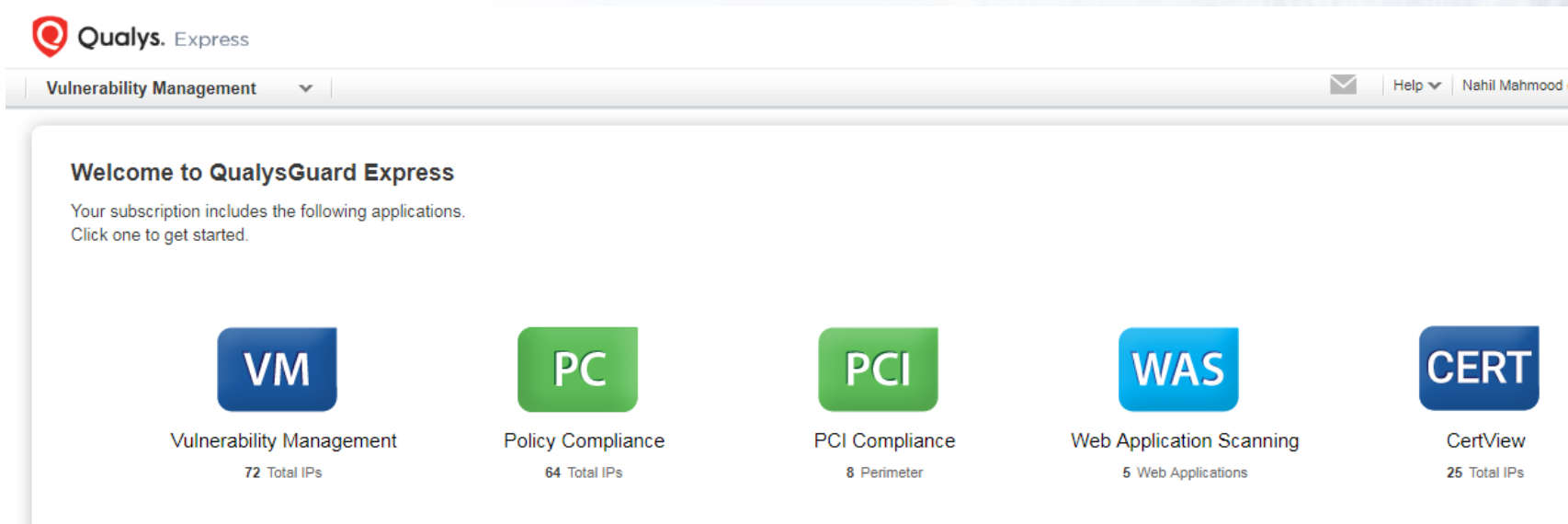
☐ Send notification when this scan is finished

WANNACRY & SHADOW BROKERS SCAN

QUALYS DEMO – SECURITY HARDENING

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

QUALYS DEMO – SECURITY HARDENING



The image shows the QualysGuard Express home screen. At the top, there is a header with the Qualys logo and the text "Qualys. Express". Below the header, there is a navigation bar with "Vulnerability Management" selected. To the right of the navigation bar, there is a mail icon, a "Help" link, and the user name "Nahil Mahmood". The main content area is titled "Welcome to QualysGuard Express" and includes a message: "Your subscription includes the following applications. Click one to get started." Below this message, there are five application tiles, each with a colored square icon containing a white acronym, the application name, and a count of resources.

Application	Count
Vulnerability Management (VM)	72 Total IPs
Policy Compliance (PC)	64 Total IPs
PCI Compliance (PCI)	8 Perimeter
Web Application Scanning (WAS)	5 Web Applications
CertView (CERT)	25 Total IPs

QUALYS GUARD – HOME SCREEN

QUALYS DEMO – SECURITY HARDENING



Policy Compliance ▾

[Dashboard](#) [Policies](#) [Scans](#) [Reports](#) [Exceptions](#) [Assets](#) [Users](#)

Welcome to Qualys® Policy Compliance

Thank you for signing up for our cloud based security service for policy compliance. You'll find helpful information below to get started with your scans.

Steps for a successful scan

[Skip to Dashboard >](#)



1 Add IP addresses to scan >

Add the IPs/ranges that you want to scan for compliance.



2 Configure scan settings >

Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. [View compliance profiles](#) provided by Qualys or [create a new profile](#).



3 Configure authentication >

Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.

POLICY COMPLIANCE – HOME SCREEN

QUALYS DEMO – SECURITY HARDENING

Welcome to Qualys® Policy Compliance

Thank you for signing up for our cloud based security service for policy compliance. You'll find helpful information below to get started with your scans.

Steps for a successful scan

[Skip to Dashboard >](#)



3 Configure authentication >

Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.



4 Start your scan >

You're now ready to start scanning! Launch a new compliance scan or schedule your scan to run automatically or on a recurring basis.

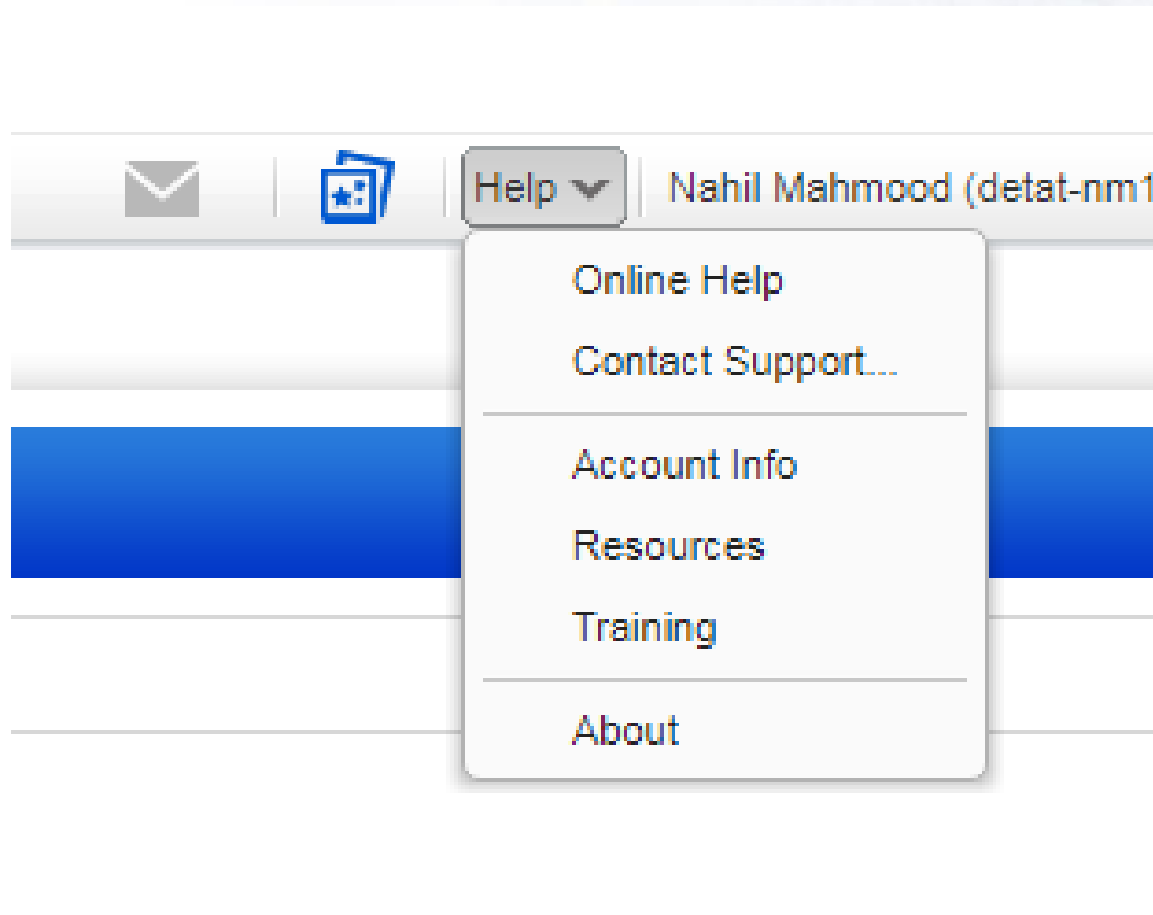


5 Build a policy >

Quickly create a new policy based on a scanned host. The service builds the policy for you using the host as a Golden Image. Or import a policy from the Library. Once you have a policy, go to the [Policy Summary](#) to check your compliance status and run reports.

POLICY COMPLIANCE – 5 STEPS

QUALYS DEMO – SECURITY HARDENING



HELP OPTIONS

QUALYS DEMO – SECURITY HARDENING

Contents Search Back Print

VM - Vulnerability Management
PC - Policy Compliance
Start Here
Policies
Scans
Reports
PC - SCAP Compliance
SCA - Security Configuration Assessment
Assets
Users
Resources

Scanning - The Basics (for PC Scans)

Good to Know

Recommendation for your first scan
What you can scan
How often you should scan
Scan complete email notification

What to Scan

How do I identify hosts to scan?
Can I exclude hosts from the scan?
Can I scan my IPv6 addresses?
Will the scan impact my hosts?
What are asset groups?
What are asset tags?

How to Scan

Which option profile should I use?
How can I customize my scan?
Why should I use authentication?

Which Scanner to Use

Are you scanning internally or externally
Options when scanning asset groups
Do I need to whitelist Qualys scanners?
Scanning through a firewall
Don't see the scanner appliance option
How do I get a scanner appliance?

Recommendation for your first scan

We recommend you start small, maybe one or two IPs. Review the results, fix the compliance issues found, and re-scan the IPs to verify. Once you're comfortable, you can scan larger sets of IPs. By the way, down you'll feel more comfortable scanning larger sets of IPs.

What you can scan

The simple answer to what to scan is this: pretty much anything that's connected to your organization's network. Here's a list: all routers and switches, servers (operating systems), workstations, databases, desktop computers, printers, and wireless access devices.

How often you should scan

ONLINE HELP – POLICY COMPLIANCE

QUALYS DEMO – SECURITY HARDENING

Resources

Look to these resources to help you with our cloud security and compliance solutions.

Get Started

[Quick Tour](#)
[Evaluator's Guide](#)
[Community Edition](#)
[Securing Amazon Web Services with Qualys](#)

Watch Videos

[VM | PC | WAS | WAF | AWS EC2 | Express Lite | More Videos](#)

Get started with your applications

[CloudView](#)
[Container Security](#)
[Indication of Compromise](#)
[Web Application Scanning](#)
- [Crawling REST services using WAS](#)
- [Jenkins Plugin for WAS: user guide | download](#)
- [Qualys Browser Recorder: user guide | download](#)
[Web Application Firewall](#)
[Policy Compliance](#)
[SCAP Compliance](#)
[Security Configuration Assessment](#)
[PCI Compliance](#)
[File Integrity Monitoring](#)

Scan Authentication

Get system and account requirements for supported technologies below.

[Monitor scan authentication & status](#)

Cloud Agents

[Cloud Agent Getting Started Guide](#)
[Windows Installation Guide](#)
[Linux Installation Guide](#)
[Unix Installation Guide](#)
[Mac Installation Guide](#)

Using a scanner appliance?

[Scanner Appliance User Guide](#)
[Scanner Appliance Quick Start \(prior version\)](#)
[Virtual Scanner Appliance User Guide](#)
[Offline Scanner Appliance User Guide](#)
[Consultant Scanner Personal Edition User Guide](#)
[Cloud Platforms: AWS | Azure | GCE | OpenStack](#)
[Qualys Scanner - Static Route Configuration](#)
[Qualys Scanner - VLAN Scanning Guide](#)
[Scanner Appliance FAQs](#)

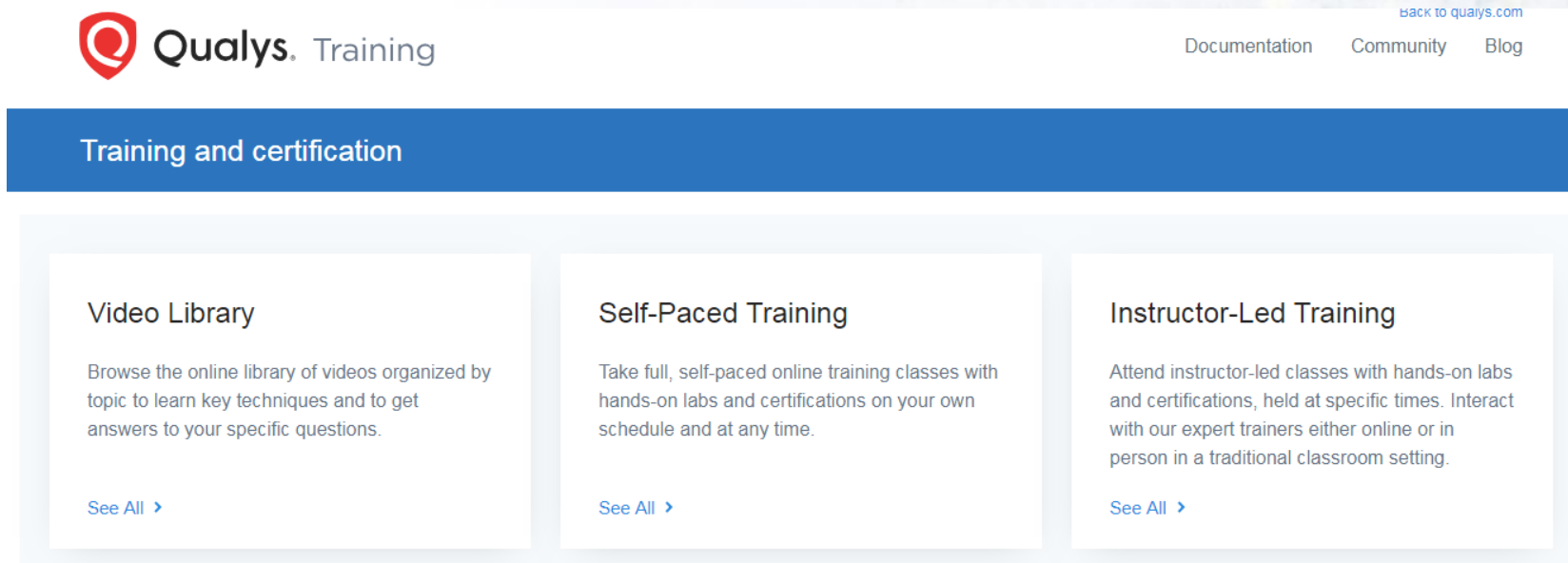
API Documentation

[Qualys API Quick Reference for all APIs](#)
[Qualys API \(VM, SCA, PC\)](#)

[Cloud Agent \(CA\) API](#)
[Web Application Scanning \(WAS\) API](#)
[Web Application Firewall \(WAF\) API](#)
[Malware Detection \(MD\) API](#)

RESOURCES

QUALYS DEMO – SECURITY HARDENING

A screenshot of the Qualys Training website. The header features the Qualys logo and 'Training' text on the left, and links for 'Documentation', 'Community', and 'Blog' on the right. A blue banner below the header reads 'Training and certification'. The main content area has three white boxes: 'Video Library' with a description and a 'See All' link, 'Self-Paced Training' with a description and a 'See All' link, and 'Instructor-Led Training' with a description and a 'See All' link. A 'Back to qualys.com' link is in the top right corner.

 **Qualys.** Training

[Back to qualys.com](#)

[Documentation](#) [Community](#) [Blog](#)

Training and certification

Video Library

Browse the online library of videos organized by topic to learn key techniques and to get answers to your specific questions.

[See All >](#)

Self-Paced Training

Take full, self-paced online training classes with hands-on labs and certifications on your own schedule and at any time.

[See All >](#)

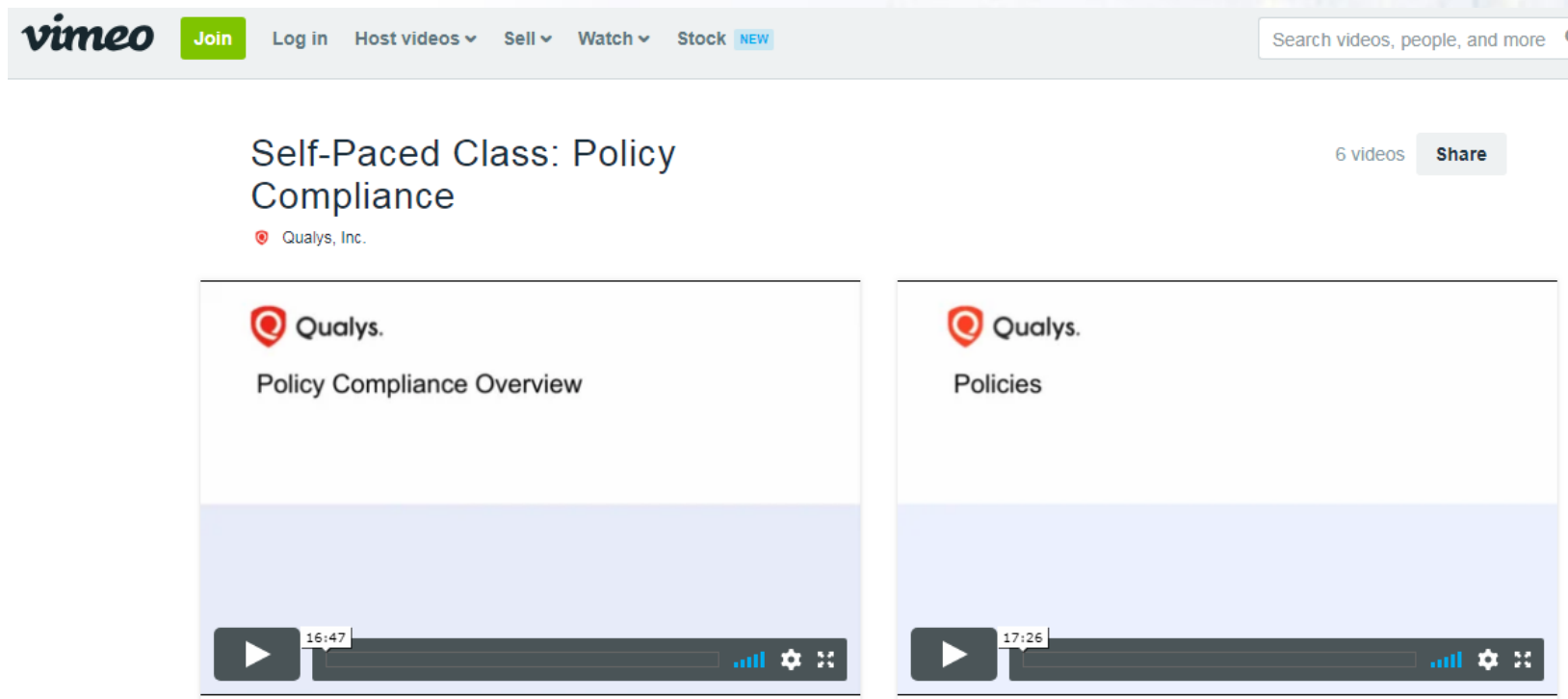
Instructor-Led Training

Attend instructor-led classes with hands-on labs and certifications, held at specific times. Interact with our expert trainers either online or in person in a traditional classroom setting.

[See All >](#)

QUALYS WEBSITE - TRAINING

QUALYS DEMO – SECURITY HARDENING



The screenshot shows the Vimeo interface for a self-paced class titled "Self-Paced Class: Policy Compliance" by Qualys, Inc. The page features a header with the Vimeo logo, navigation links (Join, Log in, Host videos, Sell, Watch, Stock), and a search bar. The main content area displays the class title and a "Share" button. Below this, two video thumbnails are shown: "Policy Compliance Overview" (16:47) and "Policies" (17:26). Both thumbnails include the Qualys logo and a play button icon.

vimeo Join Log in Host videos Sell Watch Stock NEW

Search videos, people, and more

Self-Paced Class: Policy Compliance 6 videos Share

Qualys, Inc.

Qualys.
Policy Compliance Overview 16:47

Qualys.
Policies 17:26

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



Policy Compliance ▾

[Dashboard](#) [Policies](#) [Scans](#) [Reports](#) [Exceptions](#) [Assets](#) [Users](#)

Welcome to Qualys® Policy Compliance

Thank you for signing up for our cloud based security service for policy compliance. You'll find helpful information below to get started with your scans.

Steps for a successful scan

[Skip to Dashboard >](#)



1 Add IP addresses to scan >

Add the IPs/ranges that you want to scan for compliance.



2 Configure scan settings >

Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. [View compliance profiles](#) provided by Qualys or [create a new profile](#).



3 Configure authentication >

Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.

1. ADD IP ADDRESSES TO SCAN

QUALYS DEMO – SECURITY HARDENING

New HostsLaunch Help✕

General Information: >

Host IPs >

Host Attributes >

Host IPs

Enter IPs and ranges in the field below. See the [Help](#) for proper formatting.

IPs: *

192.168.0.6

☐ Add to CertView Module

☐ Add to VM Module

(ex: 192.168.0.200,192.168.0.87-192.168.0.92)

Validate IPs through [Whois](#)

Cancel

Add

1. ADD IP ADDRESSES TO SCAN

QUALYS DEMO – SECURITY HARDENING



Policy Compliance ▾

[Dashboard](#) [Policies](#) [Scans](#) [Reports](#) [Exceptions](#) [Assets](#) [Users](#)

Welcome to Qualys® Policy Compliance

Thank you for signing up for our cloud based security service for policy compliance. You'll find helpful information below to get started with your scans.

Steps for a successful scan

[Skip to Dashboard >](#)



1 Add IP addresses to scan >

Add the IPs/ranges that you want to scan for compliance.



2 Configure scan settings >

Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. [View compliance profiles](#) provided by Qualys or create a new profile.



3 Configure authentication >

Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.

2. CONFIGURE SCAN SETTINGS

QUALYS DEMO – SECURITY HARDENING

Compliance Profile Information

General Information >

Scan Settings >

Additional Settings >

Scan restriction by Policy

Status: Disabled

Auto Update Expected Value

Status:: Disabled

Control Types

File Integrity Monitoring Controls: Disabled

Custom WMI Query Checks: Disabled

Dissolvable Agent

Dissolvable Agent (for this profile): Disabled

Password Auditing Controls: Disabled

Windows Share Enumeration: Disabled

Windows Directory Search: Disabled

Lite OS Discovery: Disabled

Ports

Scanned Ports: Targeted Scan

Hosts to Scan in Parallel

Use Appliance Parallel ML Scaling: Off

External Scanners: 15

Scanner Appliances: 30

Processes to Run in Parallel

Total: 10

HTTP: 10

2. CONFIGURE SCAN SETTINGS

QUALYS DEMO – SECURITY HARDENING

The screenshot displays the Qualys Express web interface. At the top, the 'Policy Compliance' dropdown is visible. Below it, a navigation bar includes links for Dashboard, Policies, Scans (which is highlighted), Reports, Exceptions, Assets, and Users. The 'Scans' section is active, showing a sub-navigation bar with tabs for Scans, PC Scans, Schedules, Appliances, Option Profiles, Authentication, and Setup. A 'New' dropdown menu is open, showing 'Compliance Profile...' and 'Download...'. The main table lists several compliance profiles, with 'CIS SCAN TEST PROFILE' highlighted in yellow.

Actions (1) ▼	Type	Name
☐	Compliance	...
☒	Compliance	CIS SCAN TEST PROFILE
☐	Compliance	Initial PC Options
☐	Compliance	windows-7 scan

NEW COMPLIANCE PROFILE

QUALYS DEMO – SECURITY HARDENING

New Compliance Profile

Compliance Profile Title >

Scan >

Additional >

Compliance Profile Title

Title: * CIS SCAN TEST PROFILE

Owner Nahil Mahmood (Manager: detat-nm1) ▼

☐ Make this a globally available option profile

‘CIS SCAN TEST PROFILE’ CREATED

QUALYS DEMO – SECURITY HARDENING

Welcome to Qualys® Policy Compliance

Thank you for signing up for our cloud based security service for policy compliance. You'll find helpful information below to get started with your scans.

Steps for a successful scan

[Skip to Dashboard >](#)



3 Configure authentication >

Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.



4 Start your scan >

You're now ready to start scanning! Launch a new compliance scan or schedule your scan to run automatically or on a recurring basis.



5 Build a policy >

Quickly create a new policy based on a scanned host. The service builds the policy for you using the host as a Golden Image. Or import a policy from the Library. Once you have a policy, go to the [Policy Summary](#) to check your compliance status and run reports.

3. CONFIGURE AUTHENTICATION

QUALYS DEMO – SECURITY HARDENING

The screenshot displays the Qualys Express web interface. The top navigation bar includes the Qualys Express logo and a 'Policy Compliance' tab. A dropdown menu is open under 'Policy Compliance', listing various record types: Windows Record..., Unix Record..., Oracle Record..., Oracle Listener Record..., SNMP Record..., MS SQL Record..., Cisco Record..., IBM DB2 Record..., VMware ESXi Record..., MySQL Record..., MariaDB Record..., Sybase Record..., Checkpoint Firewall..., PostgreSQL Record..., Palo Alto Networks Firewall Record..., MongoDB Record..., Application Records..., and Authentication Vaults. The 'Download...' option is at the bottom of the dropdown. The main dashboard area shows a 'Scans' sidebar with a search bar and an 'Overview' section. The 'Overview' section displays a 'Credentials Breach' status with a '0' and a 'New' button. The right side of the dashboard features tabs for 'Appliances', 'Option Profiles', 'Authentication', and 'Setup'. Below these tabs, there are four status boxes: 'Passing 0', 'Failing 0', 'Problematic 0', and 'In Vault 0'.

Qualys Express

Policy Compliance

Dashboard

Scans

Search...

Overview

Credentials Breach

0

Actions (0) New

Windows Record...

Unix Record...

Oracle Record...

Oracle Listener Record...

SNMP Record...

MS SQL Record...

Cisco Record...

IBM DB2 Record...

VMware ESXi Record...

MySQL Record...

MariaDB Record...

Sybase Record...

Checkpoint Firewall...

PostgreSQL Record...

Palo Alto Networks Firewall Record...

MongoDB Record...

Application Records...

Authentication Vaults

Download...

Appliances

Option Profiles

Authentication

Setup

Passing 0

Failing 0

Problematic 0

In Vault 0

QUALYS DEMO – SECURITY HARDENING

New Windows Record

Record Title >

Login Credentials >

IPs >

Comments >

Login Credentials

Windows Authentication

☐ Local

☒ Domain

Domain type:

NetBIOS, User-Selected IPs ▼

Domain name: *

syntax: DOMAIN1

Login

For compliance scans, trusted scanning is required. Trusted scanning allows the service to conduct assessment.

Use the basic login credential or choose to use authentication vault for authenticated scanning.

☒ Basic authentication

☐ Authentication Vault

User Name: *

Password:

QUALYS DEMO – SECURITY HARDENING

Welcome to Qualys® Policy Compliance

Thank you for signing up for our cloud based security service for policy compliance. You'll find helpful information below to get started with your scans.

Steps for a successful scan

[Skip to Dashboard >](#)



3 Configure authentication >

Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.



4 Start your scan >

You're now ready to start scanning! Launch a new compliance scan or schedule your scan to run automatically or on a recurring basis.



5 Build a policy >

Quickly create a new policy based on a scanned host. The service builds the policy for you using the host as a Golden Image. Or import a policy from the Library. Once you have a policy, go to the [Policy Summary](#) to check your compliance status and run reports.

3. CONFIGURE AUTHENTICATION

QUALYS DEMO – SECURITY HARDENING

Create a New Policy



Policy from Library: Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels	Technologies	Policies (6)
All	☐ Oracle 11g	 HITRUST Cyber Security Framework (CSF) for Linux, Version 8.1 Version 3.0 07/24/2018 View Description View Policy 
New	☐ Oracle 12c	
Updated	☐ Oracle Enterprise Linux 6.x	
CIS	☐ Oracle Enterprise Linux 7.x	
Qualys	☐ Oracle WebLogic Server 11g	 DISA Security Technical Implementation Guide (STIG) for Red Hat Enterprise Linux 7, V1R4 Version 4.0 08/02/2018 View Description View Policy 
Mandate	☐ Oracle WebLogic Server 12c	
DISA STIG	☐ PaloAlto Networks PAN-OS	
Vendor	☐ Pivotal tc Server 3.x	
	☐ PostgreSQL 9.x	
	☐ Red Hat Enterprise Linux 5.x	 CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1] Version 1.0 06/20/2018 View Description View Policy 
	☐ Red Hat Enterprise Linux 6.x	
	☒ Red Hat Enterprise Linux 7.x	
	☐ SAP Adaptive Server Enterprise 16	 CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2]

Back

Choose Source

Next

COMPLIANCE LIBRARY: CIS RED HAT ENT. LINUX 7

QUALYS DEMO – SECURITY HARDENING

Policy Editor

This policy is locked so it can be used for certification.
Click 'Save As...' to create an editable version of this policy for purposes other than certification.

Overview

CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1] v.1.0

Policy Information

Sections

6

Technologies

1

Controls

295

Status:

 Active | Deactivate

Locking:

 Block other users ☐ OFF

Last Evaluated:

09/20/2018 at 20:25:44 (GMT+0500)

Created By:

Nahil Mahmood (detat-nm1)

Assigned Technologies (1)

Red Hat Enterprise Linux 7.x

assigned to 295 controls

POLICY EDITOR

QUALYS DEMO – SECURITY HARDENING

Launch Compliance Scan

General Information

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from

Title:

SCAN 1

Compliance Profile:

CIS SCAN TEST PROFILE

[View](#)

Scanner Appliance:

External

[View](#)

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

☒ Assets

☐ Tags

Asset Groups

Select items...



[Select](#)

IPs/Ranges

192.168.0.1

[Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges

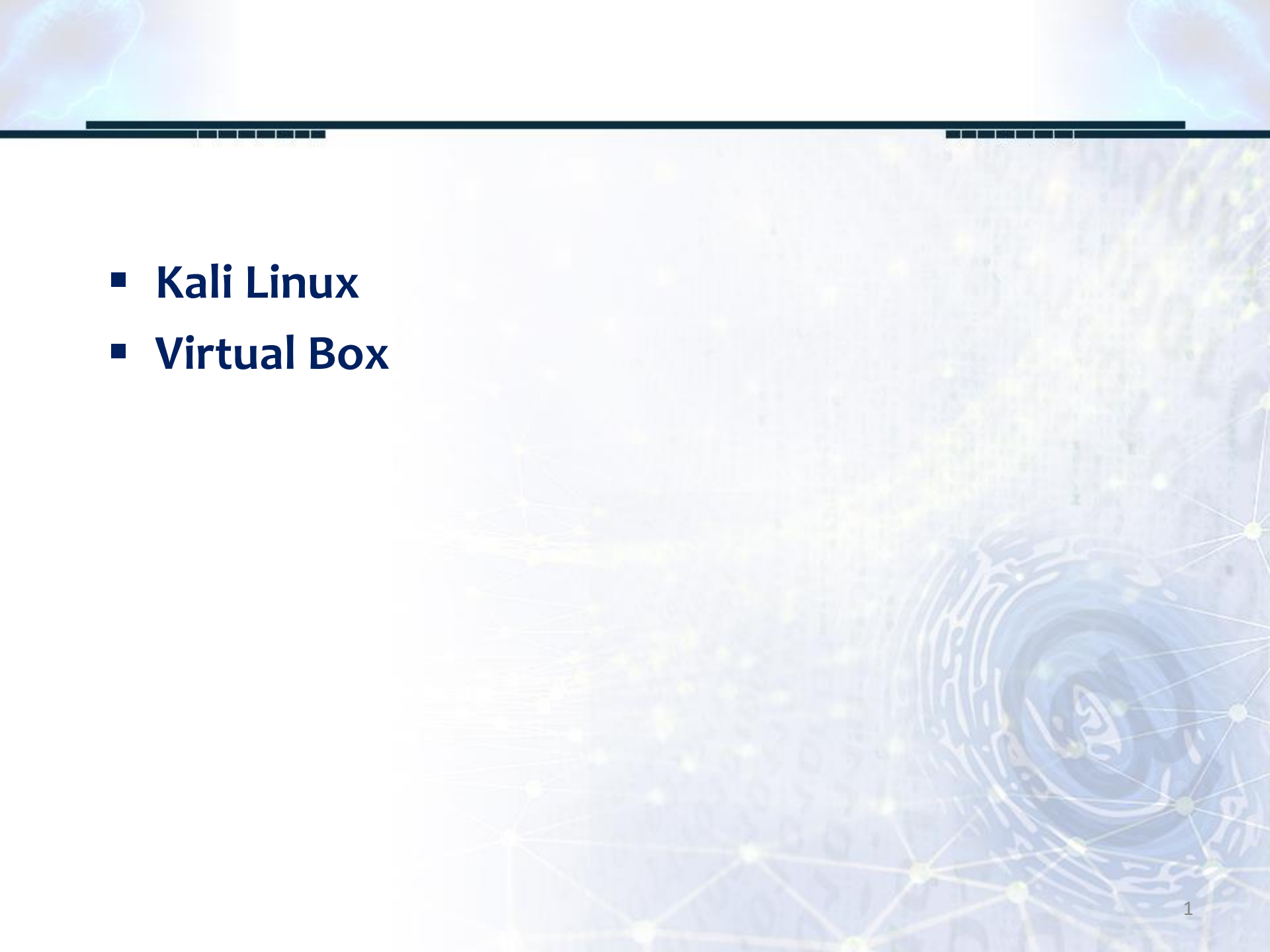
[Select](#)

LAUNCH COMPLIANCE SCAN

QUALYS DEMO – SECURITY HARDENING II

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

END

- 
- Kali Linux
 - Virtual Box

- **Virtual Box**
- <https://www.virtualbox.org/wiki/Downloads>
- **Kali Linux**
- <https://www.kali.org/>
- <https://www.osboxes.org/kali-linux/#kali-linux-2022-3-vbox>



The most advanced Penetration Testing Distribution

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

[DOWNLOAD](#) [DOCUMENTATION](#) 



VirtualBox

Download VirtualBox

search...
Login Preferen

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

If you're looking for the latest VirtualBox 6.1 packages, see [VirtualBox 6.1 builds](#). Version 6.1 will remain supported until December 2023.

VirtualBox 7.0.6 platform packages

- [Windows hosts](#)
- [macOS / Intel hosts](#)
- [Developer preview for macOS / Arm64 \(M1/M2\) hosts](#)
- [Linux distributions](#)
- [Solaris hosts](#)
- [Solaris 11 IPS hosts](#)

The binaries are released under the terms of the GPL version 3.

See the [changelog](#) for what has changed.

You might want to compare the checksums to verify the integrity of downloaded packages. *The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!*

- [SHA256 checksums, MD5 checksums](#)

Note: After upgrading VirtualBox it is recommended to upgrade the guest additions as well.

VirtualBox 7.0.6 Oracle VM VirtualBox Extension Pack

- [All supported platforms](#)

Support VirtualBox RDP, disk encryption, NVMe and PXE boot for Intel cards. See [this chapter from the User Manual](#) for an introduction to this Extension Pack. The Extension Pack binaries are released under the [VirtualBox Personal Use and Evaluation License \(PUEL\)](#). Please install the same version extension pack as your installed version of VirtualBox.

VirtualBox 7.0.6 Software Developer Kit (SDK)

- [All platforms](#)

User Manual

[About](#)

[Screenshots](#)

[Downloads](#)

[Documentation](#)

[End-user docs](#)

[Technical docs](#)

[Contribute](#)

[Community](#)



Search...



[VM IMAGES](#) ▾

[SUPPORT](#) ▾

[BLOG](#)



Oracle VM VirtualBox Manager

File Machine Help



CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off



Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. For a list of currently available tools check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be extended with new tools in future releases.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.



Details

Tool to observe virtual machine (VM) details. Reflects groups of properties for the currently chosen VM and allows basic operations on certain properties (like the machine storage devices).



Snapshots

Tool to control virtual machine (VM) snapshots. Reflects snapshots created for the currently selected VM and allows snapshot operations like create, remove, restore (make current) and observe their properties. Allows to edit snapshot attributes like name and description.





CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off



Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine at the right side of the main tool bar located at the top of the window.

You can click on the question mark icon to get more information and latest news.

← Create Virtual Machine

Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Type: Microsoft Windows

Version: Windows 7 (64-bit)



Expert Mode

Next

Cancel

for the currently chosen VM and allows basic operations on certain properties (like

for the currently selected VM and allows snapshot operations like create, remove, restore, rollback, snapshot, name and description.

New Settings Discard Start

CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. At the right side of the main tool bar located at the top of the window.

You can click on the left arrow to go back to the previous screen or on the right arrow to go forward to the next screen.

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **1024 MB**.



Next

Cancel





CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off



Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine at the right side of the main tool bar located at the top of the window.

You can click on the left arrow to create a new virtual machine.

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

- ☐ Do not add a virtual hard disk
- ☐ Create a virtual hard disk now
- ☒ Use an existing virtual hard disk file

IE8_-_Win7-disk1.vmdk (Normal, 127.00 GB)

Create

Cancel

64 CyberOps Workstation 64
 Powered Off

7 Windows 7
 Powered Off

64 Server 2016
 2016 Powered Off

64 WinDev1903Eval
 10 Powered Off

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. At the right side of the main tool bar located at the top of the main window, you can find a question mark icon for more information and latest news.



← Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

☐ Do not add a virtual hard disk
☐ Create a virtual hard disk now
☒ Use an existing virtual hard disk file

IE8_-_Win7-disk1.vmdk (Normal, 127.00 GB)

Create Cancel

for the currently chosen VM and allows basic operations on certain properties (like

for the currently selected VM and allows snapshot operations like create, remove, at attributes like name and description.

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen

Please choose a virtual hard disk file

« Downloads » Kali » 64bit Search 64bit

Organize New folder

Name	Date modified	Type
Kali Linux 2019.1 (64bit)	5/5/2019 5:37 PM	Virtual

File name: All virtual hard disk files (*.vmd)

Open Cancel



certain properties (like

ns like create, remove,

CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

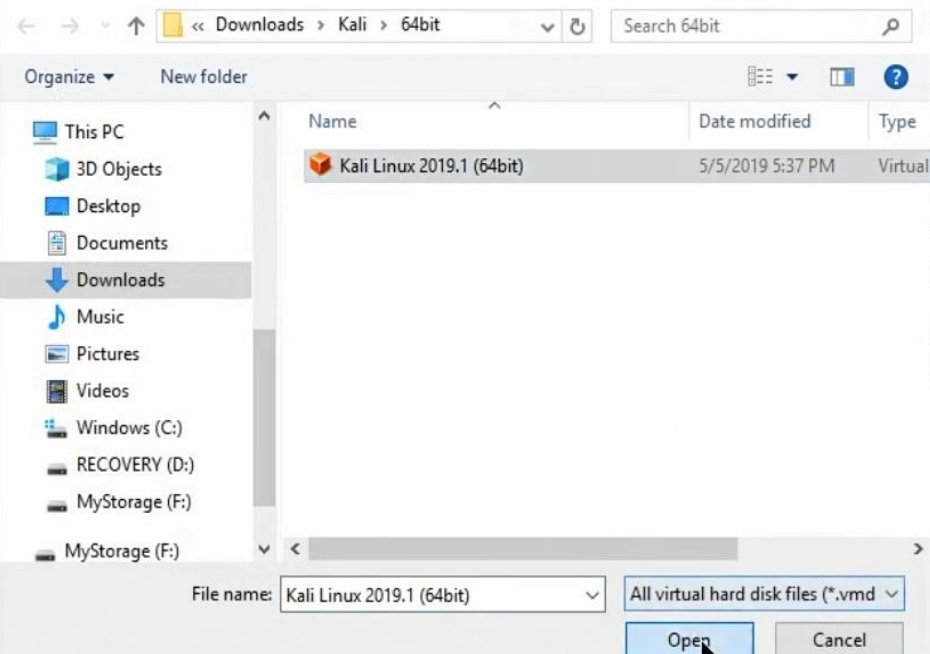
WinDev1903Eval
Powered Off

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine.

Please choose a virtual hard disk file



certain properties (like

ns like create, remove,



CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. You can find the right side of the main tool bar located at the top of the window.

Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

- ☐ Do not add a virtual hard disk
- ☐ Create a virtual hard disk now
- ☒ Use an existing virtual hard disk file

Kali Linux 2019.1 (64bit).vdi (Normal, 500.00 GB)

Create

Cancel



for the currently chosen VM and allows basic operations on certain properties (like

for the currently selected VM and allows snapshot operations like create, remove, restore and attributes like name and description.

Oracle VM VirtualBox Manager

File Machine Help



CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off

Kali Linux - Jasper
Powered Off

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. For a list of currently available tools check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be extended with new tools in future releases.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.



Details

Tool to observe virtual machine (VM) details. Reflects groups of properties for the currently chosen VM and allows basic operations on certain properties (like the machine storage devices).



Snapshots

Tool to control virtual machine (VM) snapshots. Reflects snapshots created for the currently selected VM and allows snapshot operations like create, remove, restore (make current) and observe their properties. Allows to edit snapshot attributes like name and description.





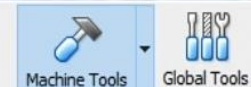
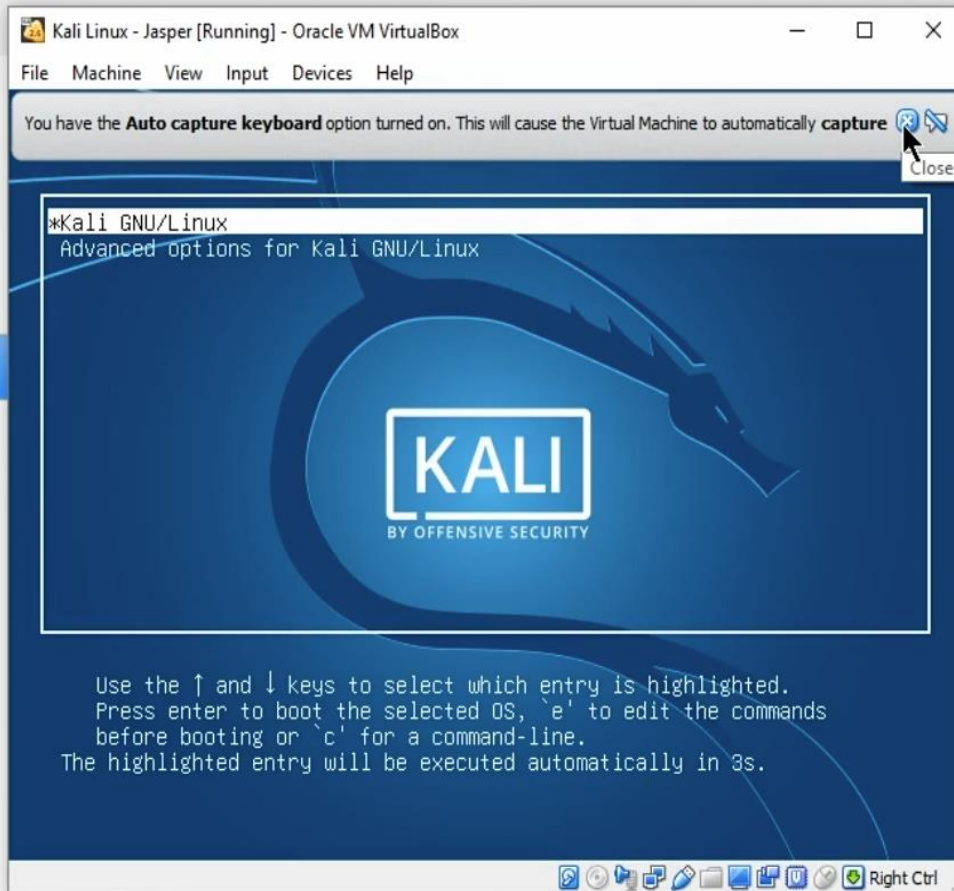
CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off

Kali Linux - Jasper
Running



the currently chosen
bar located at the

WS.

d allows basic operations on certain properties (like

and allows snapshot operations like create, remove,
description.

Kali Linux - Jasper [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

- Full-screen Mode Host+F
- Seamless Mode Host+L
- Scaled Mode Host+C
- Adjust Window Size Host+A
- Auto-resize Guest Display
- Take Screenshot... Host+E
- Video Capture
- Menu Bar ▶
- Status Bar ▶
- Scale Factor ▶
- Virtual Screen 1 ▶

kali

us 31 Mar, 02:37

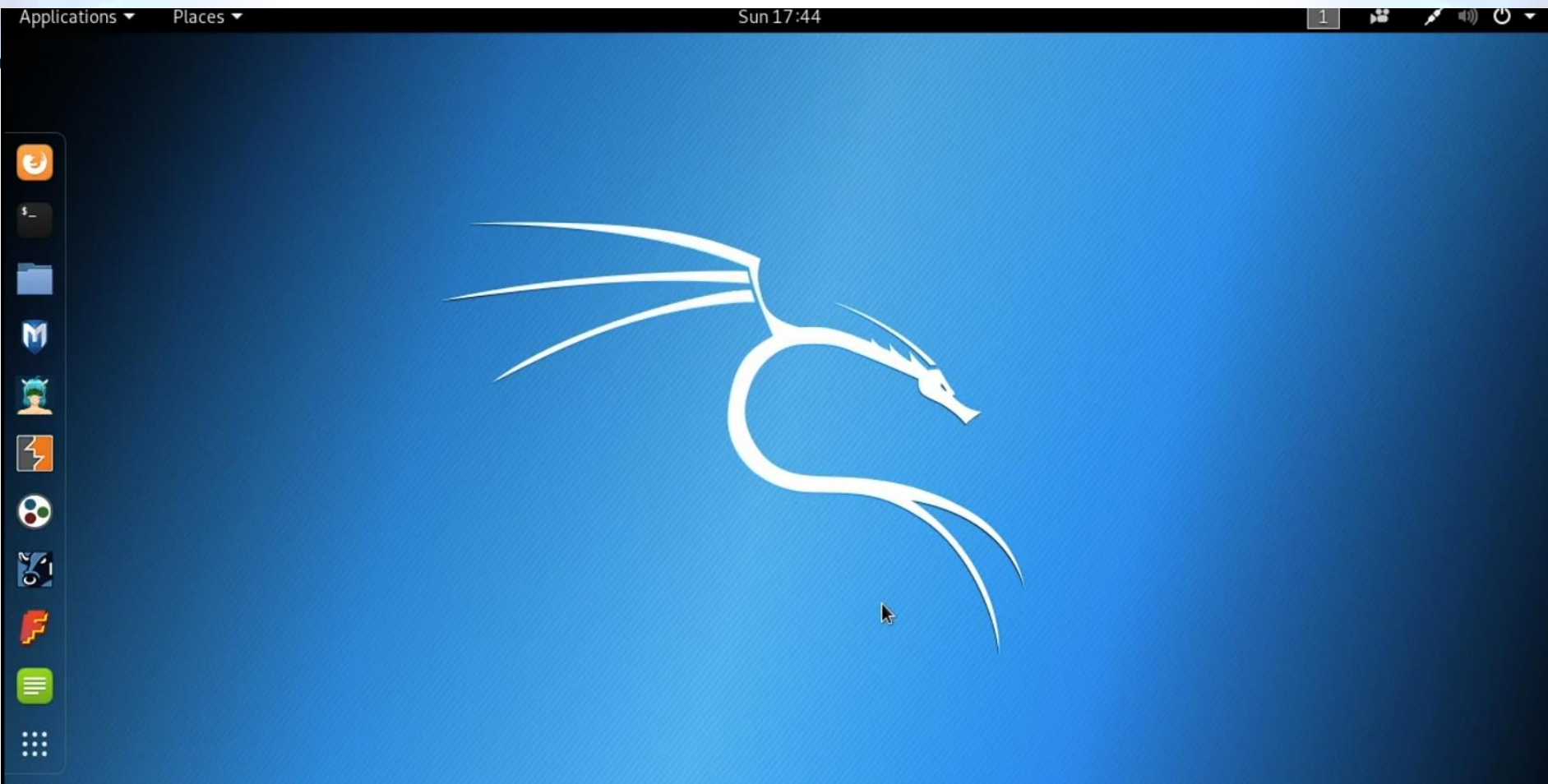


Enter your password

Cancel

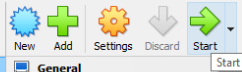
Log In

KALI





kali Linux
2.6
Powered Off



General

Name: kali Linux
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)

System

Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2022.4-virtualbox-amd64.vdi (Normal, 80.09 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders

None

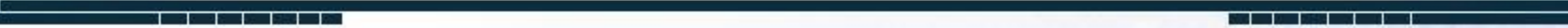
Description

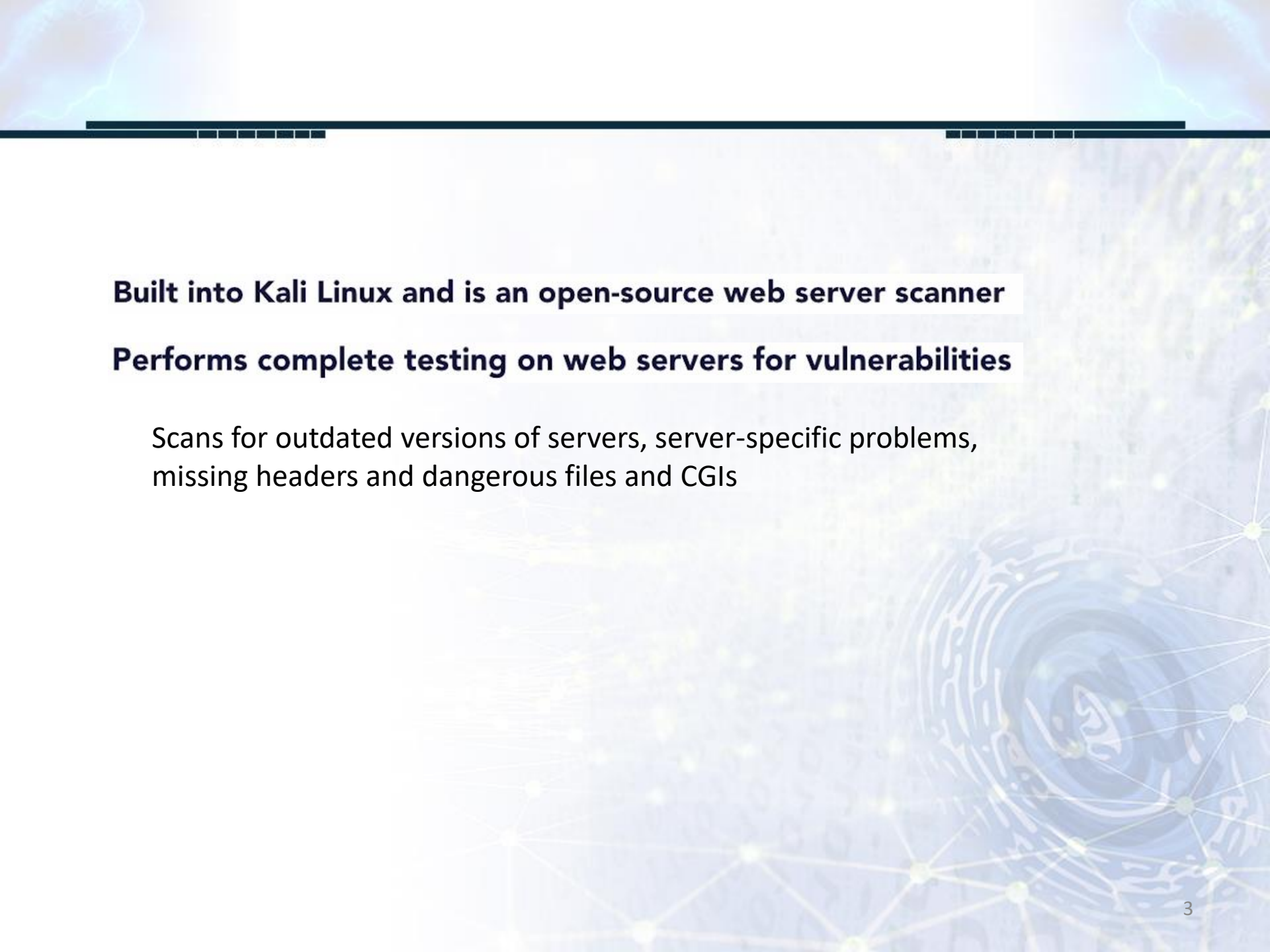
None

Preview



- **Nikto**

- 
- Web server scanning is a black box test that identifies security vulnerabilities.



Built into Kali Linux and is an open-source web server scanner

Performs complete testing on web servers for vulnerabilities

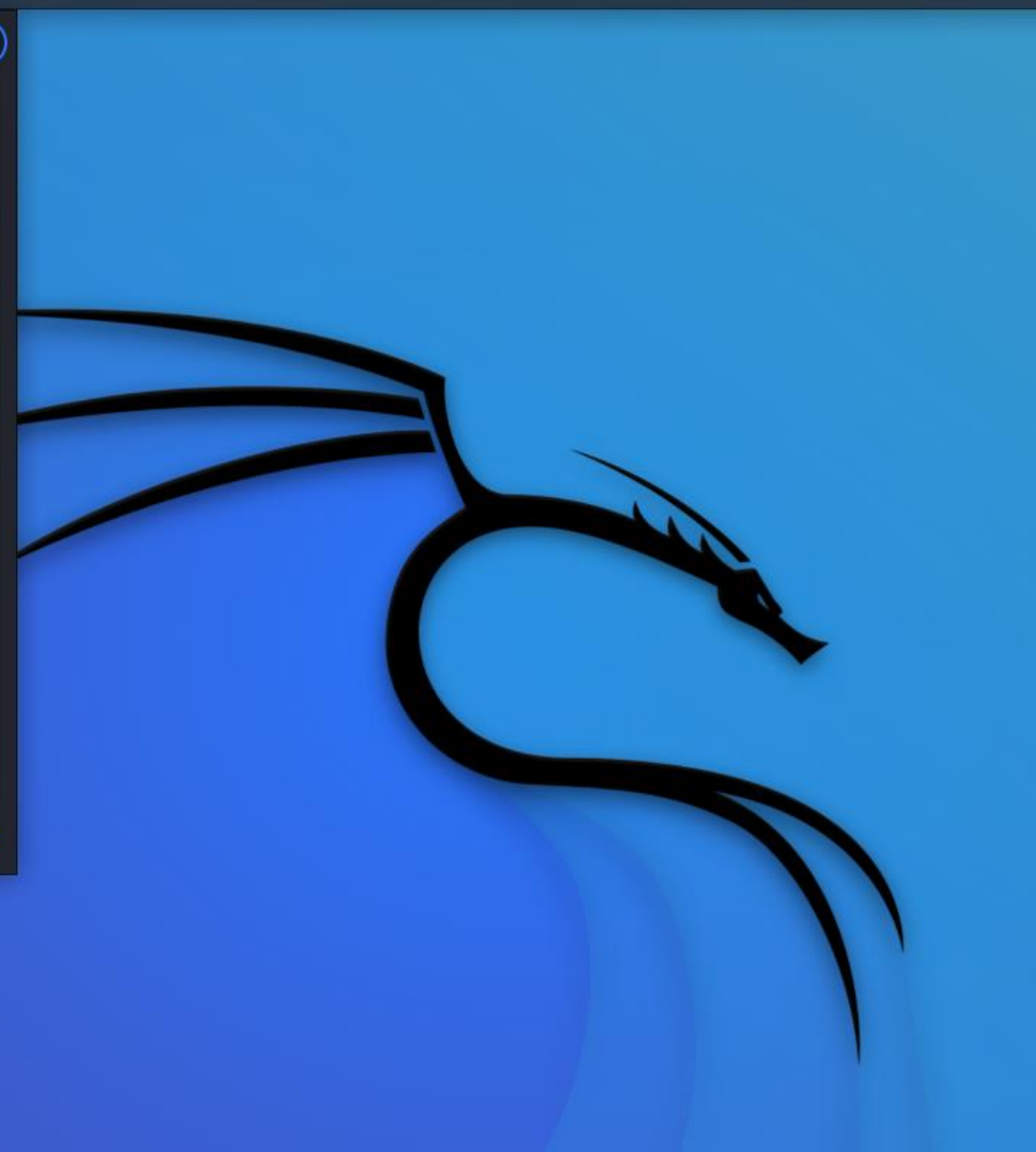
Scans for outdated versions of servers, server-specific problems, missing headers and dangerous files and CGIs

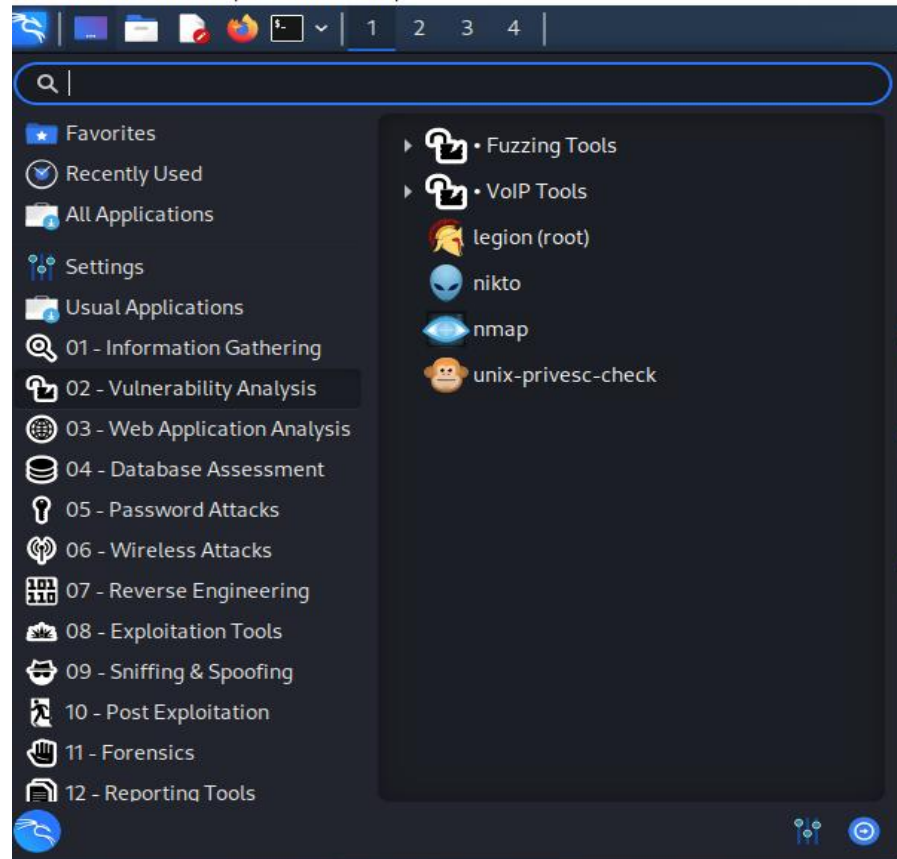


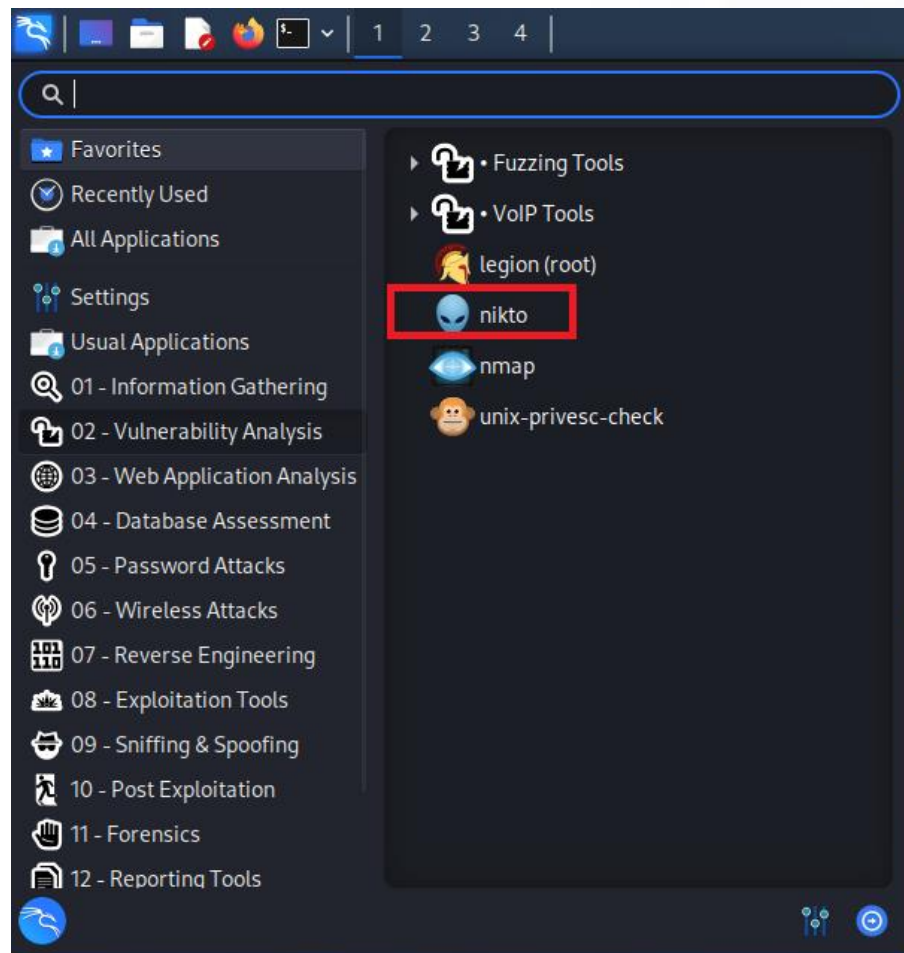
Search |

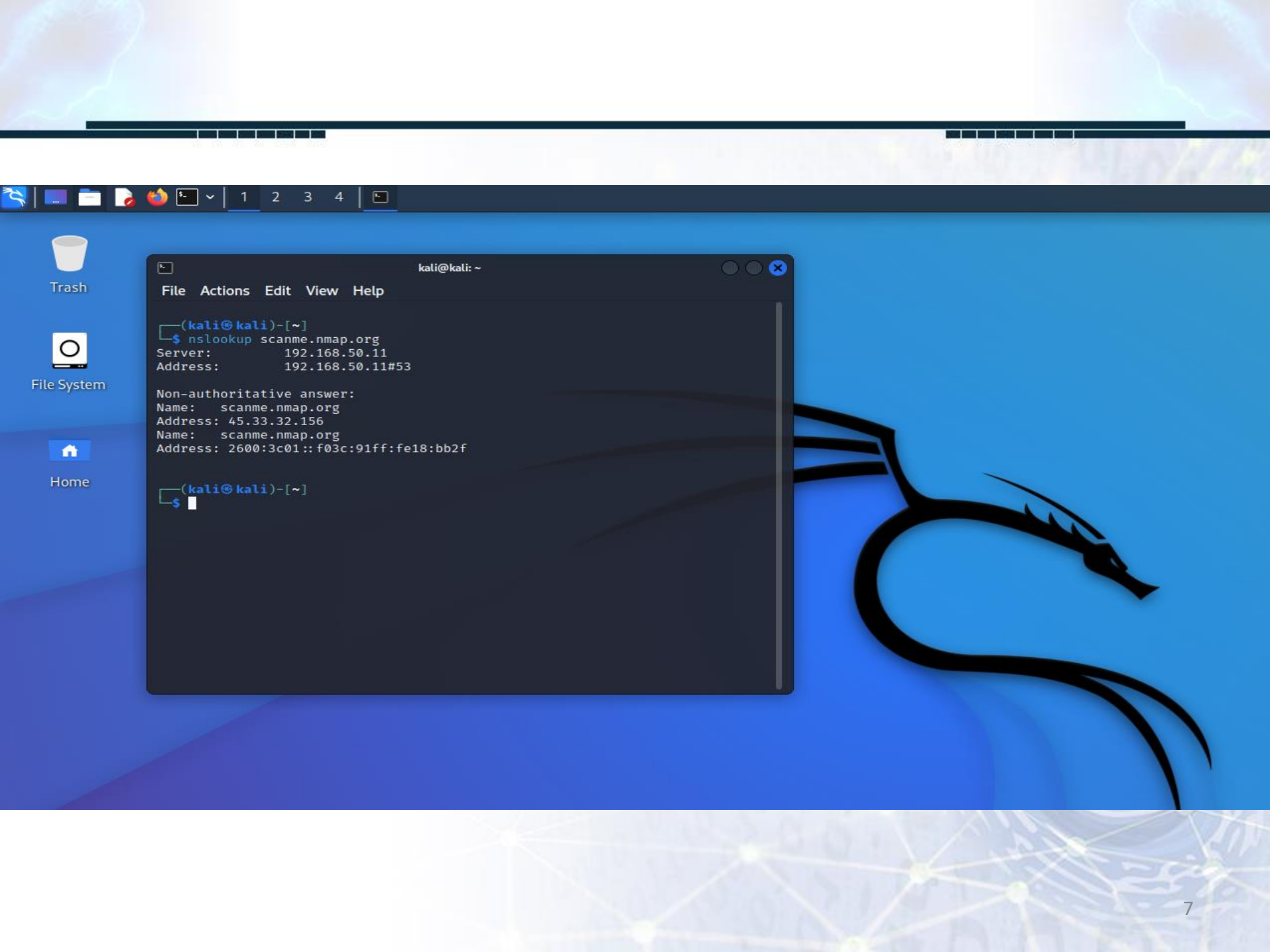
- ★ Favorites
- 🔍 Recently Used
- 📁 All Applications
- ⚙️ Settings
- 📁 Usual Applications
- 🔍 01 - Information Gathering
- 🔗 02 - Vulnerability Analysis
- 🌐 03 - Web Application Analysis
- 🗄️ 04 - Database Assessment
- 🔑 05 - Password Attacks
- 📶 06 - Wireless Attacks
- 🔧 07 - Reverse Engineering
- 🔪 08 - Exploitation Tools
- 📡 09 - Sniffing & Spoofing
- 🚶 10 - Post Exploitation
- 👤 11 - Forensics
- 📄 12 - Reporting Tools

- 💻 Terminal Emulator
- 🔴 Root Terminal Emulator
- 📁 File Manager
- 📄 Text Editor
- 🌐 Web Browser
- 🌐 Kali Linux
- 📄 Kali Docs
- 🔴 Kali Bugs
- 👤 Offensive Security Training
- 🕷️ Exploit Database
- 🏠 VulnHub









Trash

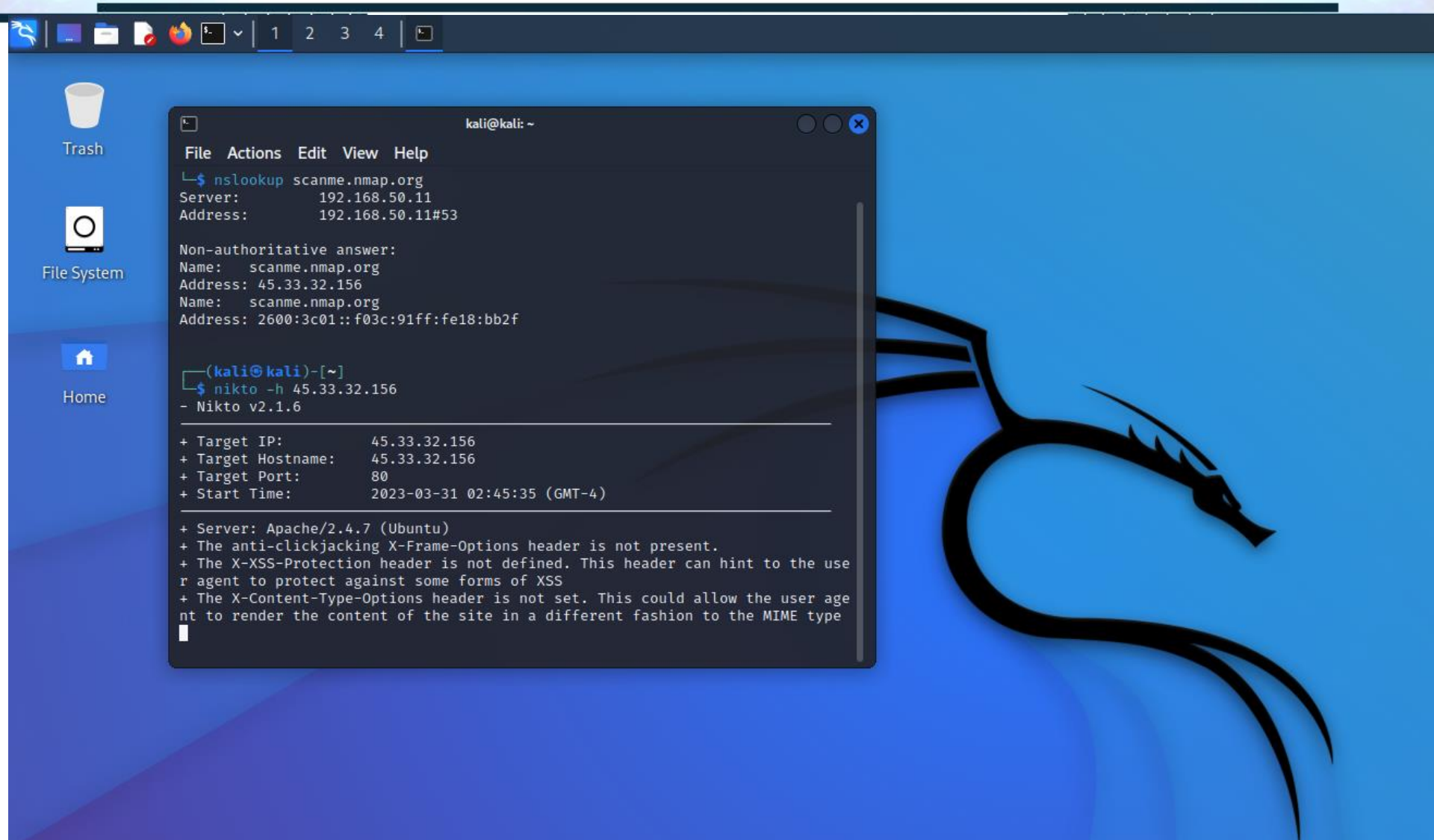


File System



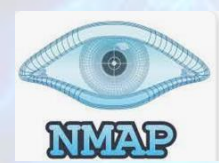
Home

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nslookup scanme.nmap.org  
Server:      192.168.50.11  
Address:     192.168.50.11#53  
  
Non-authoritative answer:  
Name:   scanme.nmap.org  
Address: 45.33.32.156  
Name:   scanme.nmap.org  
Address: 2600:3c01::f03c:91ff:fe18:bb2f  
  
(kali@kali)-[~]  
$
```





Nmap(Network Mapper)

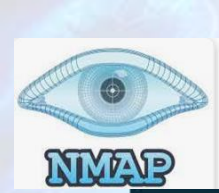


Nmap

Nmap, short for Network Mapper, is a free and open source utility network discovery and security auditing tool.

It is the world's leading port scanner, known for its simple and easy to remember flags that provide powerful scanning options.

- Guess the operating system running on a target machine
- Get accurate packet routes till the target machine
- Discovering connected hosts on a network
- Analyzing free ports on a target host
- Detecting running services on a system along with version number
- Uncovering network vulnerabilities and system loopholes



Nmap

Network administrators often use

- to detect the devices that are presently working on the system
- the port number to which the devices are attached
- the free ports that may be used.
- what services (application name and version) those hosts are offering
- what operating systems (and OS versions) they are running



Nmap

- helpful while performing network penetration testing.
- not only gives network information but also assists in discovering security issues in the system.
- Nmap is platform-agnostic and may be run on various standard operating systems, including Linux, Windows, macOS.
- It is straightforward to use and includes both a command-line interface(CLI) and a graphical user interface(GUI).

Nmap is Used to Scan:



- Enterprise-scale networks
- Small business networks
- Connected devices
- IoT devices and traffic



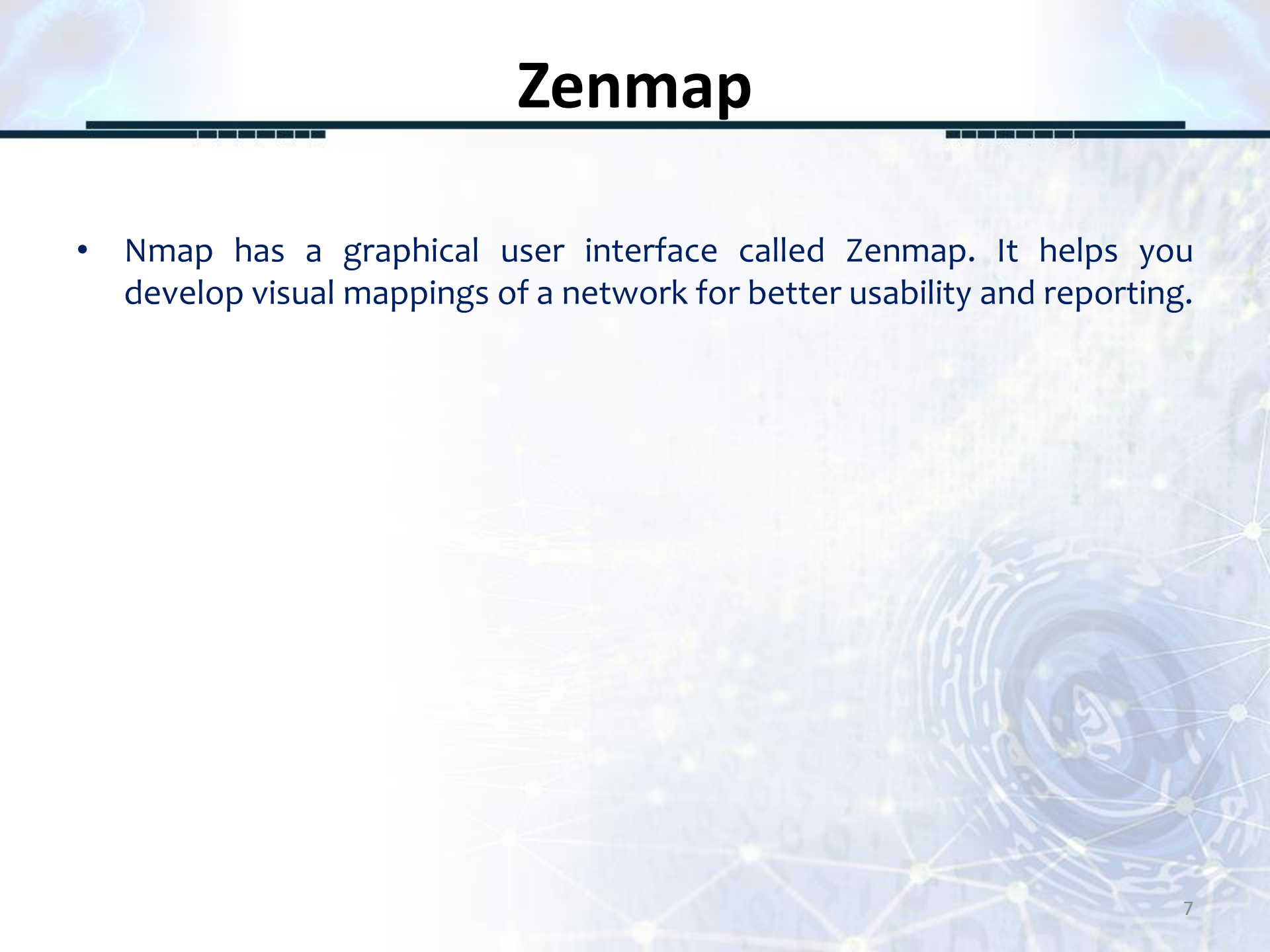
Nmap Commands

Common Nmap Functions



- Ping Scanning
- Port Scanning
- Host Scanning
- OS Scanning
- Scan Top Ports
- Output to Files
- Disable DNS Resolution

Zenmap



- Nmap has a graphical user interface called Zenmap. It helps you develop visual mappings of a network for better usability and reporting.

NAME	DATE	SCORE	GRADE	TEACHER	PERIOD	SECTION
------	------	-------	-------	---------	--------	---------





Nmap Commands

- various commands you can use in Nmap along with their flag and usage description with an example on how to use it.

Basic Nmap Scan against IP or host

nmap 1.1.1.1

- Now, if you want to scan a hostname, simply replace the IP for the host, as you see below:

nmap scanme.com



Nmap Commands with flags

Flag	Use	Example
-Pn	only port scan	nmap -Pn 192.168.1.1
-sn	only host discover	nmap -sn 192.168.1.1
-PR	arp discovery on a local network	nmap -PR 192.168.1.1
-n	disable DNS resolution	nmap -n 192.168.1.1

Flag	Use	Example
-p	specify a port or port range	nmap -p 1-30 192.168.1.1
-p-	scan all ports	nmap -p- 192.168.1.1
-F	fast port scan	nmap -F 192.168.1.1

Flag	Use	Example
-sV	detect the version of services running	nmap -sV 192.168.1.1
-A	aggressive scan	nmap -A 192.168.1.1
-O	detect operating system of the target	nmap -O 192.168.1.1

Nmap Benefits and Installation

- Time tested security and networking tool
- Open source package with large community
- Available for most operating systems
- Free!

■ Download Link

<https://nmap.org/download>

[Download](#)[Reference Guide](#)[Book](#)[Docs](#)[Zenmap GUI](#)[In the Movies](#)

Downloading Nmap

Get the latest Nmap for your system:

- [Windows](#)
- [macOS](#)
- [Linux \(RPM\)](#)
- [Any other OS \(source code\)](#)

Older versions (and sometimes newer test releases) are available from the [Nmap release archive](#) (and really old ones are in [dist-old](#)). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the [sigs directory](#) ([verification instructions](#)). Before downloading, be sure to read the relevant sections for your platform from the [Nmap Install Guide](#). The most important changes (features, bugfixes, etc) in each Nmap version are described in the [Changelog](#). Using Nmap is covered in the [Reference Guide](#), and don't forget to read the other [available documentation](#), particularly the official book [Nmap Network Scanning](#)!

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

(or subscribe with custom options from the [Nmap-hackers list info page](#))

to get updates by liking [Nmap on Facebook](#) or following us [@nmap on Twitter](#).

[illegible]

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install [the latest Npcap release](#).

We have written [post-install usage instructions](#). Please [notify us](#) if you encounter any problems or have suggestions for the installer.

Many popular Linux distributions (Redhat, Mandrake, Suse, etc) use the [RPM](#) package management system for quick and easy binary package installation. We have written a detailed [guide to installing our RPM packages](#), though these simple commands usually do the trick:

```
rpm -vhU https://nmap.org/dist/nmap-7.93-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/zenmap-7.93-1.noarch.rpm
rpm -vhU https://nmap.org/dist/ncat-7.93-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/nping-0.7.93-1.x86_64.rpm
```

You can also download and install the RPMs yourself:

Latest stable release:

x86-64 (64-bit Linux) Nmap RPM: [nmap-7.93-1.x86_64.rpm](#)

x86-64 (64-bit Linux) Ncat RPM: [ncat-7.93-1.x86_64.rpm](#)

x86-64 (64-bit Linux) Nping RPM: [nping-0.7.93-1.x86_64.rpm](#)

Optional Zenmap GUI (all platforms): [zenmap-7.93-1.noarch.rpm](#)

Source RPM (includes Nmap, Zenmap, Ncat, and Nping): [nmap-7.93-1.src.rpm](#)

