

CompTIA Security+ Exam SY0-701

Lesson 8



Explain Vulnerability Management

Lesson 8

Topic 8A

Device and OS Vulnerabilities

Operating System Vulnerabilities

- Vulnerabilities in an OS can lead to significant problems when successfully exploited
- Microsoft Windows Client and Server
- Apple macOS
- Linux
- Android
- iOS

Vulnerability Types

- Legacy Systems
- End-of-Life (EOL) Systems
- Firmware Vulnerabilities
- Virtualization Vulnerabilities
- Application Vulnerabilities

Zero-Day Vulnerabilities

- Previously unknown software or hardware flaws.
- Developers have "zero days" to fix once the vulnerability becomes known
- Traditional security measures like antivirus and firewalls are often ineffective
- Zero-day vulnerabilities have significant financial value
- Adversaries generally use a zero-day vulnerability against high-value targets

Misconfiguration Vulnerabilities

- Common cause of security vulnerabilities
- Default configurations
 - Hardware/devices
 - Software
 - Cloud services
- Using search engine results to solve technical problems

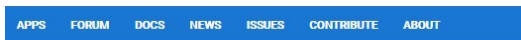
Cryptographic Vulnerabilities

- Cryptography forms the backbone of secure communication
- Weaknesses in cryptographic systems, protocols, or algorithms
 - Methods no longer deemed secure
 - Weak Keys
 - Misconfigured cipher suites
- Improperly protected keys

Sideloading, Rooting, and Jailbreaking

- Rooting and jailbreaking are methods used to gain elevated privileges on mobile devices
- Rooting - gaining root access or administrative privileges on an Android device
- Jailbreaking - gaining full access to an iOS device (iPhone or iPad)
- Sideloading - installing applications from sources other than the official app store
 - F-Droid
 - Android APK (Android Application Package) files

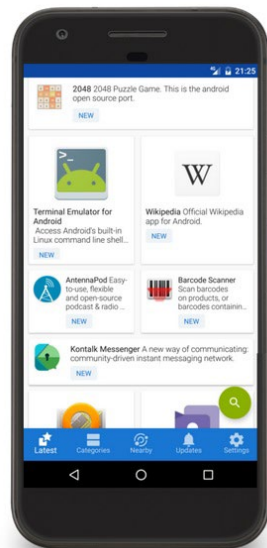
Sideloading, Rooting, and Jailbreaking



What is F-Droid?

F-Droid is an installable catalogue of FOSS (Free and Open Source Software) applications for the Android platform. The client makes it easy to browse, install, and keep track of updates on your device.

DOWNLOAD F-DROID
PGP Signature



The F-Droid Android application store. (Screenshot courtesy of www.opensecurityarchitecture.org.)

- Rooting and jailbreaking are methods used to gain elevated privileges on mobile devices
- Rooting
 - Gaining root access or administrative privileges on an Android device
- Jailbreaking
 - Gaining full access to an iOS device (iPhone or iPad)
- Sideloading
 - Installing applications from sources other than the official app store
 - F-Droid
 - Android APK (Android Application Package) files

Review Activity: Device and OS Vulnerabilities

- Operating System Vulnerabilities
- Vulnerability Types
- Zero-Day Vulnerabilities
- Misconfiguration Vulnerabilities
- Cryptographic Vulnerabilities
- Sideloading, Rooting, and Jailbreaking

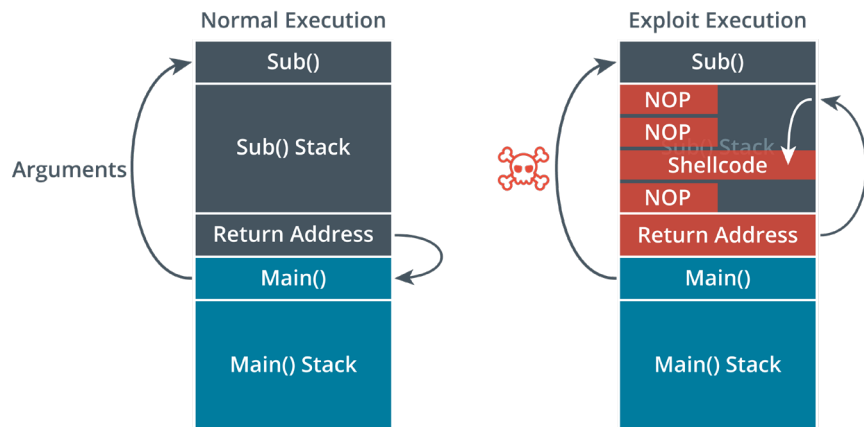
Lesson 8

Topic 8B

Application and Cloud Vulnerabilities

Application Vulnerabilities

- Race Condition
- Time-of-check to time-of-use (TOCTOU)
- Memory Injection
- Buffer Overflow
- Type-Safe Programming Languages
- Malicious Update



When executed normally, a function will return control to the calling function. If the code is vulnerable, an attacker can pass malicious data to the function, overflow the stack, and run arbitrary code to gain a shell on the target system.

Evaluation Scope

- Scope refers to the product, system, or service being analyzed for potential security vulnerabilities
- Practices
 - Security Testing
 - Documentation Review
 - Source Code Analysis
 - Configuration Assessment
 - Cryptographic Analysis
 - Compliance Verification
 - Security Architecture Review

Web Application Attacks

- Specifically target applications accessible over the Internet
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- SQL Injection (SQLi)

Cloud-based Application Attacks

- Target applications hosted on cloud platforms
 - Exploit potential vulnerabilities within the hosted applications
 - Exploit cloud infrastructure the applications run on
- Cloud As an Attack Platform
- Cloud Access Security Brokers

Supply Chain

- Potential risks and weaknesses introduced into products during their development, distribution, and maintenance lifecycle
- Hardware Suppliers
- Software Providers
 - Software Bill of Materials
 - Dependency Analysis and SBOM Tools

Review Activity: Application and Cloud Vulnerabilities

- Application Vulnerabilities
- Evaluation Scope
- Web Application Attacks
- Cloud-based Application Attacks
- Supply Chain

Lab Activity

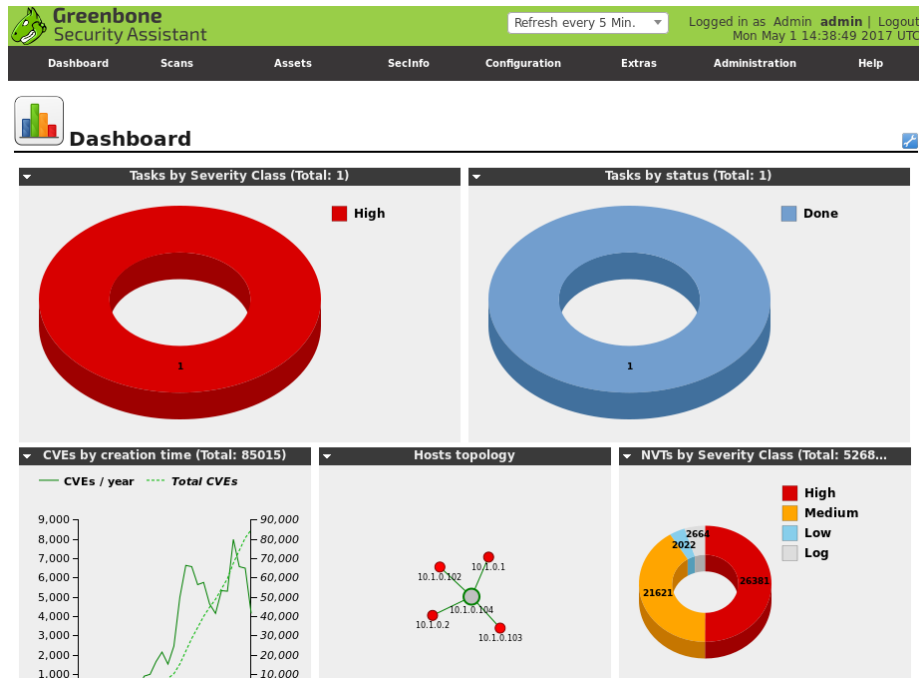
- Assisted Lab: Exploiting and Detecting SQLi

Lesson 8

Topic 8C

Vulnerability Identification Methods

Vulnerability Scanning

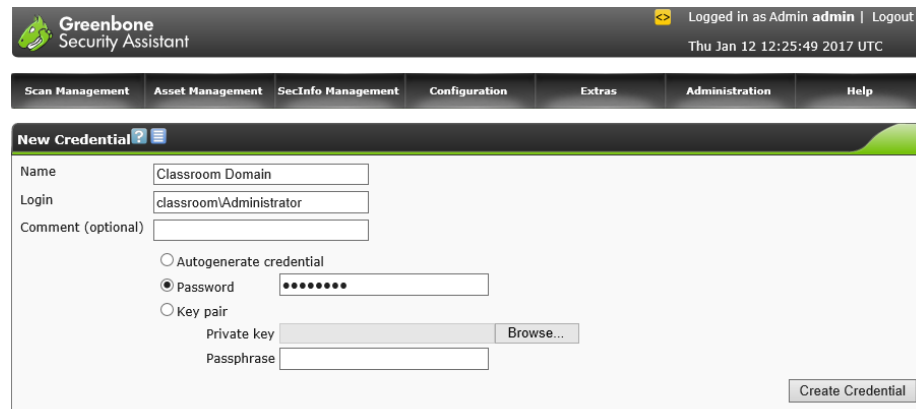


Greenbone OpenVAS vulnerability scanner with Security Assistant web application interface as installed on Kali Linux. (Screenshot used with permission from Greenbone Networks, <http://www.openvas.org>.)

- Cornerstone of modern cybersecurity practices
- Focused on identifying, classifying, remediating, and mitigating vulnerabilities
- Helps to locate and identify misconfigurations

Vulnerability Scanning

- Network Vulnerability Scanners
- Tenable Nessus
- OpenVAS
- Credentialed and Non-Credentialed Scans
- Application and Web Application Scanners
- Package Monitoring



The screenshot displays the Greenbone Security Assistant (GSA) web interface. At the top, a dark header bar contains the Greenbone logo, the text 'Greenbone Security Assistant', and a user status bar indicating 'Logged in as Admin admin | Logout' and the timestamp 'Thu Jan 12 12:25:49 2017 UTC'. Below the header is a navigation menu with tabs for 'Scan Management', 'Asset Management', 'SecInfo Management', 'Configuration', 'Extras', 'Administration', and 'Help'. The main content area is titled 'New Credential' and features a form for creating a new credential. The form includes fields for 'Name' (filled with 'Classroom Domain'), 'Login' (filled with 'classroom\Administrator'), and 'Comment (optional)'. Below these fields are three radio buttons: 'Autogenerate credential', 'Password' (which is selected), and 'Key pair'. The 'Password' option has a corresponding password input field filled with dots. The 'Key pair' option has fields for 'Private key' and 'Passphrase', with a 'Browse...' button next to the 'Private key' field. A 'Create Credential' button is located at the bottom right of the form.

Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

Configuring credentials for use in target (scope) definitions in Greenbone OpenVAS as installed on Kali Linux. (Screenshot used with permission from Greenbone Networks, <http://www.openvas.org>.)

Threat Feeds

The screenshot shows the IBM X-Force Exchange dashboard. At the top, there's a navigation bar with the IBM X-Force Exchange logo, a search bar, and links for 'Create IBMid' and 'Log In'. Below the navigation bar, a dark blue banner contains the text 'Research, Collaborate and Act on threat intelligence' and a search bar with the placeholder 'Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...'. To the right of the search bar is a 'Scan file' button. Below the banner, the dashboard is divided into several sections. On the left, there's a 'Dashboard' section with a 'Recent IBM X-Force Advisories' list, including 'New Monero Cryptominer Discovered' and 'Anchor Targeting PoS Systems'. In the center, there's a 'Threat Activity' section showing a line graph of 'Malicious IP addresses in the last hour' with a table of statistics: Total (976), Command and Control (0), Spam (670), Malware (0), and Scans (333). On the right, there's a 'Trending' section with a table of trending threats: #blacklist (185,153,196.97), #malware (149,202,251.78), #malware-loc-utl (62,210,54.33), and #malware-loc-utl (66,240,205.34). Below the trending section, there's a 'Free IRIS Threat Reports' section with links to 'ITG06 Analysis Report', 'Pharmaceutical Manufacturing Industry Profile', and 'BadFlick Analysis Report'. At the bottom right, there's a 'Premium IRIS Threat Reports' section with links to 'Enfourks Analysis Report', 'ChChes Analysis Report', 'Retail Industry Profile', 'ITG06 Analysis Report', and 'Hive0052 Analysis Report'.

IBM X-Force Exchange

Research, Collaborate and Act on threat intelligence

Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...

...or Scan file

Trending

Threat	Count
#blacklist	185,153,196.97
#malware	149,202,251.78
#malware-loc-utl	62,210,54.33
#malware-loc-utl	66,240,205.34

Dashboard

AlertCon™ Threat Level 1

IBM Advanced Threat Protection Feed

Identify malicious threats in your environment in nearly real-time.

The Advanced Threat Protection Feed by X-Force provides you with machine-readable lists of actionable indicators that directly integrate with security tools like firewalls, intrusion prevention systems, and SIEMs.

Start your 30-day trial

View API documentation

Early Warning Feed

Stay ahead of threats with the Early Warning Feed

emails.apple.com
Registered: Dec 16, 2019

midadvancetypeappclicks.top
Registered: Dec 16, 2019

btvmxpik.com
Registered: Dec 16, 2019

Start your 30-day trial

Visit Early Warning dashboard

IRIS Threat Intelligence

Premium Threat Intelligence on threat groups, industries and malware

Free IRIS Threat Reports

- ITG06 Analysis Report
Last Updated: Nov 14, 2019
- Pharmaceutical Manufacturing Industry Profile
Last Updated: Jul 15, 2019
- BadFlick Analysis Report
Last Updated: Jul 15, 2019

Premium IRIS Threat Reports

- Enfourks Analysis Report
Last Updated: Dec 10, 2019
- ChChes Analysis Report
Last Updated: Dec 3, 2019
- Retail Industry Profile
Last Updated: Nov 28, 2019
- ITG06 Analysis Report
Last Updated: Nov 21, 2019
- Hive0052 Analysis Report
Last Updated: Nov 21, 2019

Recent IBM X-Force Advisories

Collections created by the IBM X-Force team

- New Monero Cryptominer Discovered
Dec 13, 2019 - malware
- Anchor Targeting PoS Systems
Dec 13, 2019 - malware

Threat Activity

Malicious IP addresses in the last hour

Category	Count
Total	976
Command and Control	0
Spam	670
Malware	0
Scans	333

IBM X-Force Exchange threat intelligence portal. (Image copyright 2019 IBM Security exchange.xforce.ibmcloud.com.)

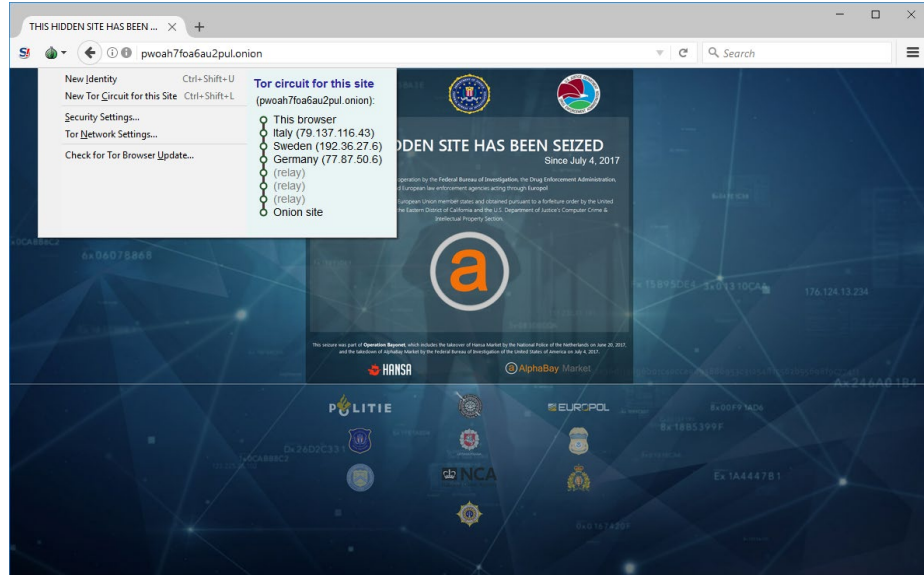
- Real-time, continuously updated sources of information about potential threats and vulnerabilities
- Provide timely information and context about new threats

Threat Feeds

- Open-source and proprietary threat feeds
 - IBM X-Force Exchange
 - Mandiant's FireEye
 - Recorded Future
 - Proofpoint Emerging Threats
 - Abuse.ch
- Information-Sharing Organizations
 - Information Sharing and Analysis Centers (ISACs)
- Open-Source Intelligence
 - Search engines, blogs, forums, social media platforms, and the dark web

Deep and Dark Web

- Deep Web
 - Any part of the World Wide Web that is not indexed by a search engine
- Dark Net
 - A network established as an overlay to Internet infrastructure, such as The Onion Router (TOR), Freenet, or I2P, that acts to anonymize usage
- Dark Web
 - Sites, content, and services accessible only over a dark net



Using the TOR browser to view the AlphaBay market, now closed by law enforcement.
(Screenshot used with permission from Security Onion.)

Other Vulnerability Assessment Methods

- Penetration Testing
 - Unknown environment (previously black box) testing
 - Known environment (previously white box) testing
 - Partially known environment (previously gray box) testing
- Bug Bounties
- Auditing

Review Activity: Vulnerability Identification Methods

- Vulnerability Scanning
- Threat Feeds
- Deep and Dark Web
- Other Vulnerability Assessment Methods

Lab Activity

- Assisted Lab: Working with Threat Feeds

Lesson 8

Topic 8D








Vulnerability Analysis and Remediation

Common Vulnerabilities and Exposures

- Vulnerability Feed
- National Vulnerability Database (NVD)
- Security Content Automation Protocol (SCAP)
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS)

CVSS Score	Description
0.1+	Low
4.0+	Medium
7.0+	High
9.0+	Critical

False Positives, False Negatives, and Log Review

Information	Results <small>(135 of 1148)</small>	Hosts <small>(1 of 254)</small>	Ports <small>(17 of 30)</small>	Applications <small>(19 of 44)</small>	Operating Systems <small>(1 of 6)</small>	CVEs <small>(48 of 48)</small>	Closed CVEs <small>(56 of 56)</small>	TLS Certificates <small>(3 of 5)</small>	Error Messages <small>(2 of 2)</small>	User Tags <small>(0)</small>
<div>◀◁ 1 - 10 of 135 ▷▶</div>										
Vulnerability		Severity ▼	QoD	Host		Location	Created			
				IP	Name					
Microsoft Windows Multiple Vulnerabilities (KB4457131)		10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 9:58 PM UTC			
Microsoft Windows Multiple Vulnerabilities (KB4467691)		10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:20 PM UTC			
Microsoft Windows Multiple Vulnerabilities (KB4471321)		10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:40 PM UTC			
Microsoft Windows Multiple Vulnerabilities (KB4512517)		10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:27 PM UTC			
Microsoft Malware Protection Engine on Windows Defender Multiple Remote Code Execution Vulnerabilities		9.3 (High)	97 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:19 PM UTC			
Microsoft Malware Protection Engine on Windows Defender Multiple Vulnerabilities		9.3 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:09 PM UTC			

Scan report listing multiple high-severity vulnerabilities found in a Windows host.
(Screenshot: Greenbone Community Edition greenbone.net/en/community-edition.)

- False Positive
- Scanner or another assessment tool incorrectly identifies a vulnerability
- False Negatives
- Vulnerabilities that go undetected in a scan
- Validate vulnerability reports by examining logs

Vulnerability Analysis

- Prioritization
- Classification
- Exposure Factor
- Impacts
- Environmental Variables
- Risk Tolerance

Vulnerability Response and Remediation

- Remediation Practices
 - Patching
 - Cybersecurity insurance
 - Segmentation
 - Compensating controls
 - Exceptions and exemptions
- Validation
 - Re-scanning
 - Auditing
 - Verification
 - Reporting

Review Activity: Vulnerability Analysis and Remediation

- Common Vulnerabilities and Exposures
- False Positives, False Negatives, and Log Review
- Vulnerability Analysis
- Vulnerability Response and Remediation

Lab Activity

- Assisted Lab: Performing Vulnerability Scans

CompTIA Security+ Exam SY0-701

Lesson 8



Summary