



# SEC+

## 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

# Sideload, 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)
- Sideload - installing applications from sources other than the official app store
  - F-Droid
  - Android APK (Android Application Package) files

# Sideload, Rooting, and Jailbreaking

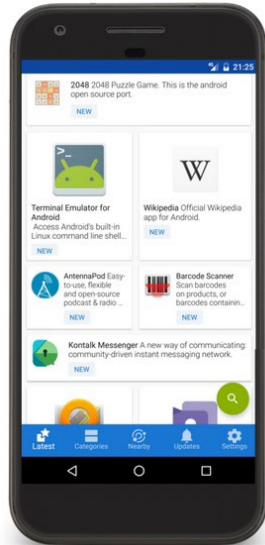


APPS FORUM DOCS NEWS ISSUES CONTRIBUTE ABOUT

## 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



- 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)
- Sideload
  - Installing applications from sources other than the official app store
  - F-Droid
  - Android APK (Android Application Package) files

# Device and OS Vulnerabilities

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

Lesson 8

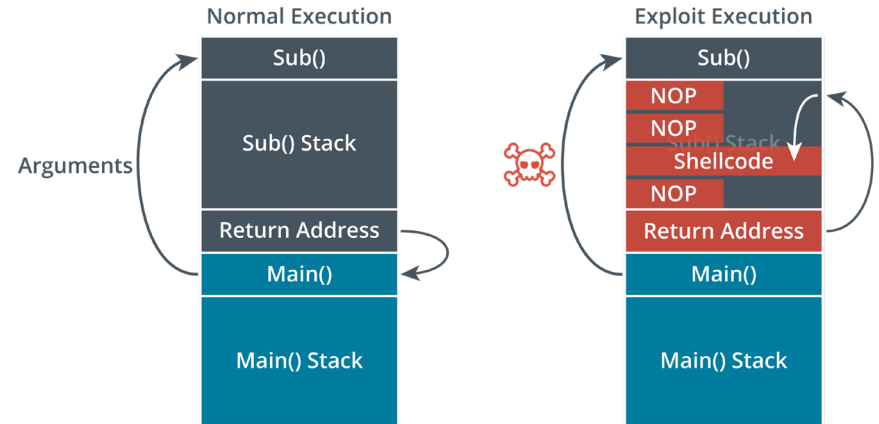
# Topic 8B

## 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

# Application and Cloud Vulnerabilities

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

Lesson 8

# Topic 8C

Vulnerability

Identification Methods



# Vulnerability Scanning

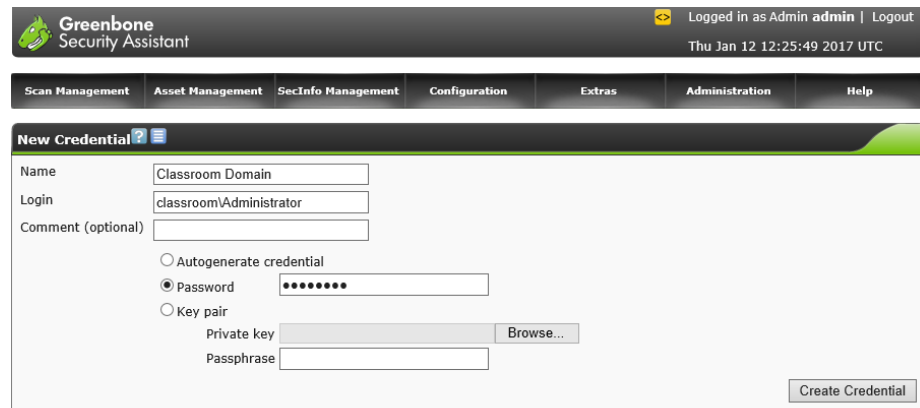


Greenbone OpenVAS vulnerability scanner with Security Assistant web application interface as installed on Kali Linux. (Screenshot used with permission from Greenbone Networks, <http://www.openvas.org>.)

- 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 shows the Greenbone Security Assistant (GSA) interface. At the top, it displays the logo and name 'Greenbone Security Assistant', the user 'Admin admin', and the date '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 contains a form with the following fields and options:

- Name: Classroom Domain
- Login: classroom\Administrator
- Comment (optional):
- Autogenerate credential:
- Password:  Password: [masked]
- Key pair:
- Private key: [input field] Browse...
- Passphrase: [input field]
- Create Credential button

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

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

The screenshot shows the IBM X-Force Exchange interface. At the top, there's a navigation bar with 'IBM X-Force Exchange', a search bar, and user options like 'Create IBMid' and 'Log In'. Below this is a header with the text 'Research, Collaborate and Act on threat intelligence'. A search bar is present with the placeholder 'Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...'. To the right, there's a 'Trending' section with a table of items:

| Item           | Value            |
|----------------|------------------|
| #blacklist     | 185,153,196.97   |
| #malware       | 149,202,251.78   |
| 208.97.139.113 | 42,210.54.33     |
| 66.240.205.34  | #malware-loc-url |

The main dashboard area is divided into several sections:

- IBM Advanced Threat Protection Feed:** Identifies malicious threats in nearly real-time. Includes a 'Start your 30-day trial' button and a link to 'View API documentation'.
- Early Warning Feed:** Stay ahead of threats with the Early Warning Feed. Lists domains like 'emails.apple.com', 'midadvancetypeappclicks.top', and 'btvmpk.com' with their registration dates.
- IRIS Threat Intelligence:** Premium Threat Intelligence on threat groups, industries and malware. Lists reports such as 'ITG06 Analysis Report', 'Pharmaceutical Manufacturing Industry Profile', and 'BadFlick Analysis Report'.
- Threat Activity:** Malicious IP addresses in the last hour. A table shows counts for various categories:

| Category            | Count |
|---------------------|-------|
| Total               | 976   |
| Command and Control | 0     |
| Spam                | 670   |
| Malware             | 0     |
| Scamming            | 333   |

Other sections include 'Recent IBM X-Force Advisories' (e.g., 'New Monero Cryptominer Discovered') and 'Premium IRIS Threat Reports' (e.g., 'Enfourks Analysis Report').

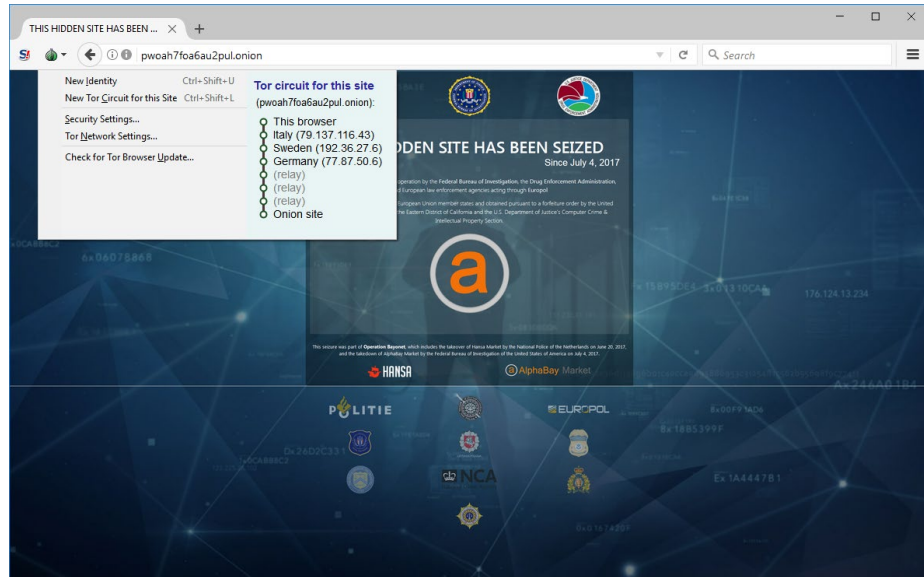
IBM X-Force Exchange threat intelligence portal. (Image copyright 2019 IBM Security exchange.xforce.ibmcloud.com.)

# 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

# Vulnerability Identification Methods

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

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

# Vulnerability Analysis and Remediation

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

CompTIA Security+ Exam SY0-701

# Lesson 8



## Summary