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

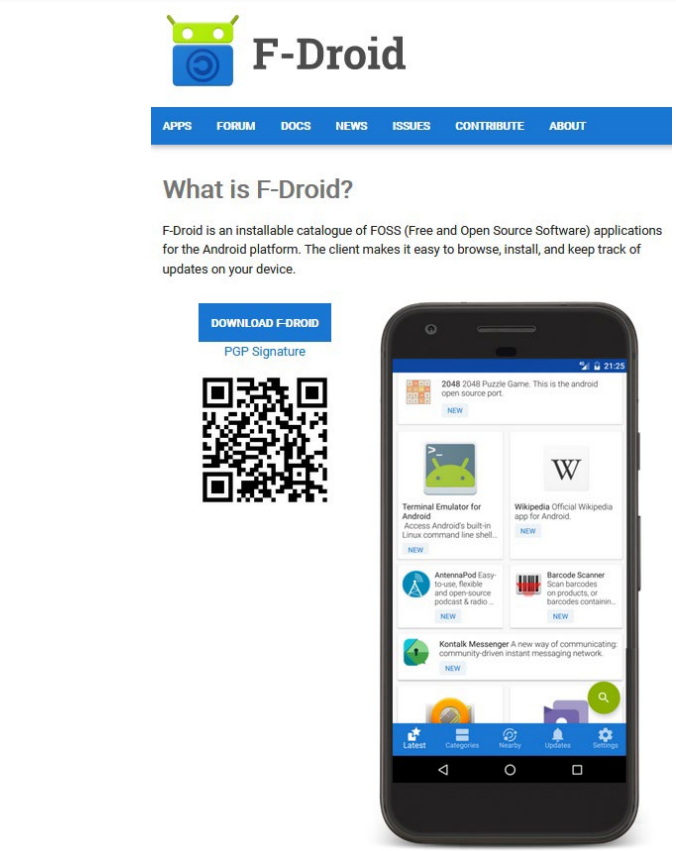
- Cryptography forms the backbone of secure communication

- Weaknesses in cryptographic systems, protocols, or algorithms
  - Methods no longer deemed secure
  - Weak Keys
  - Misconfigured cipher suites
- Improperly protected keys

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



- 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

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

Device and OS Vulnerabilities

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

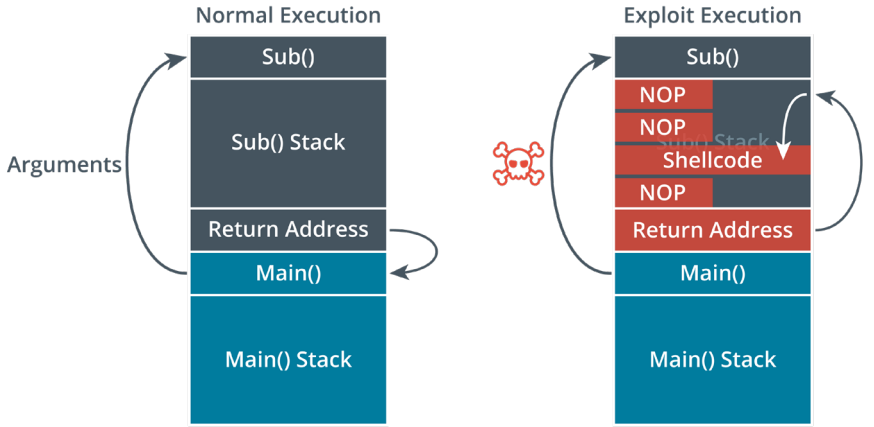
Lesson 8

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

Application and Cloud Vulnerabilities

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

Lesson 8

Topic 8C

Vulnerability Identification Methods

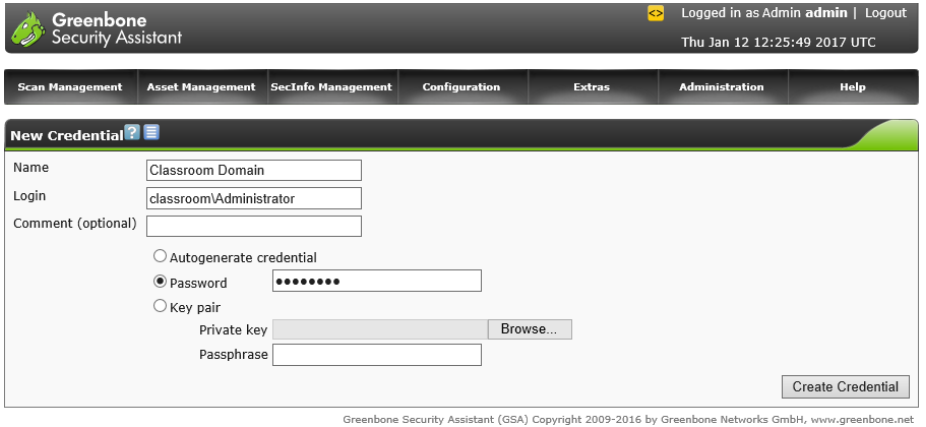
Vulnerability Scanning

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

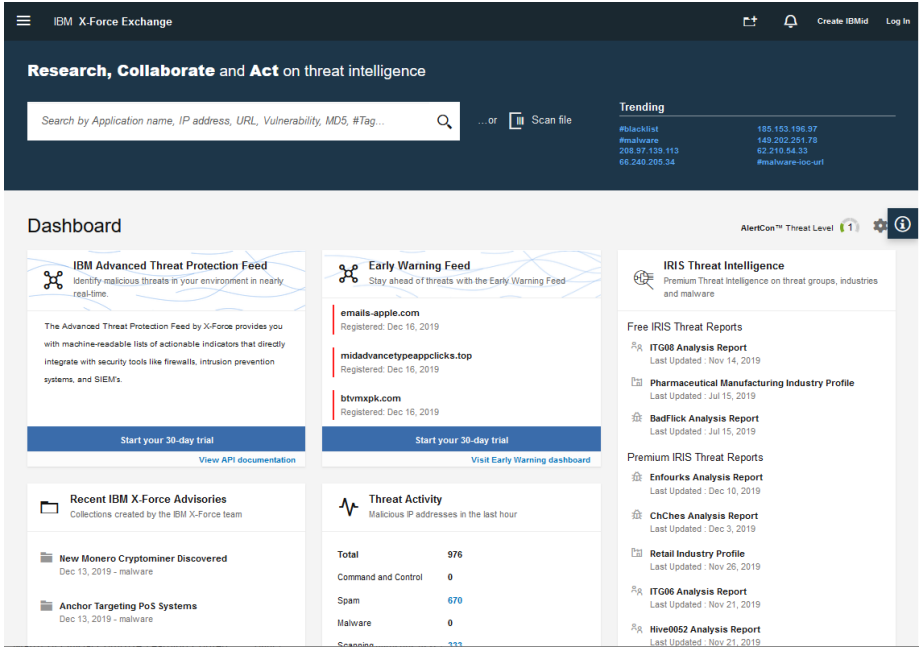
Vulnerability Scanning

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



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



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

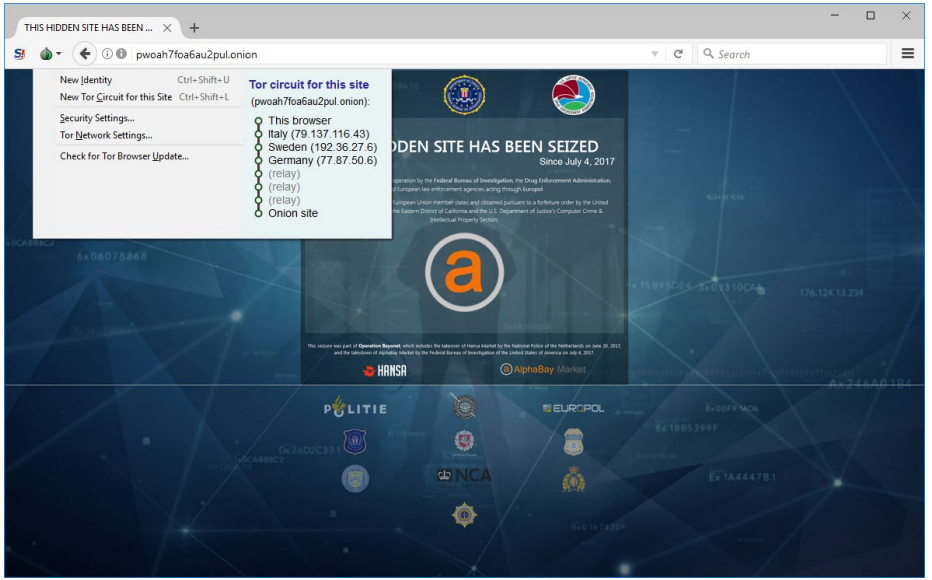
- Real-time, continuously updated sources of information about potential threats and vulnerabilities
- Provide timely information and context about new threats

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

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 (135 of 1148) | Hosts (1 of 254) | Ports (17 of 30) | Applications (19 of 44) | Operating Systems (1 of 6) | CVEs (48 of 48) | Closed CVEs (56 of 56) | TLS Certificates (3 of 5) | Error Messages (2 of 2) | User Tags (0)

1 - 10 of 135

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
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

Vulnerability Analysis and Remediation

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

Lesson 8

Summary