Question and Answers

Squadron 06

Name: *Narayan Ram Narayanan* , **Student ID:** *119398579*, **Email:** nana2011@umd.edu
Name: *Dhanush Devaladakere Arvind* , **Student ID:** *119151556*, **Email:** dagowda@umd.edu
Name: *Sumanth Vankineni* , **Student ID:** *119351130*, **Email:** svankine@umd.edu
Name: *Tanishq Javvaji* , **Student ID:** *119070185*, **Email:** tanishqj@umd.edu

Date: 07 - December - 2023

Please see the attached Pen-testing Report file for supporting screenshots and walk-through.

Adding the GDrive link with supporting files (custom word list and script). Google Drive Link

---

Task 1: Evaluate the security of a system

Using the ENPM 695 Project Evaluation System, you'll be evaluating the system's security from both inside and outside perspectives. You'll aim to identify running services, their vulnerabilities, and assess the system's resistance to intrusion.

Tasks:

1. **Determine the running and open services on the system (10 points)**

- We obtained information about the open ports and services using the following command:

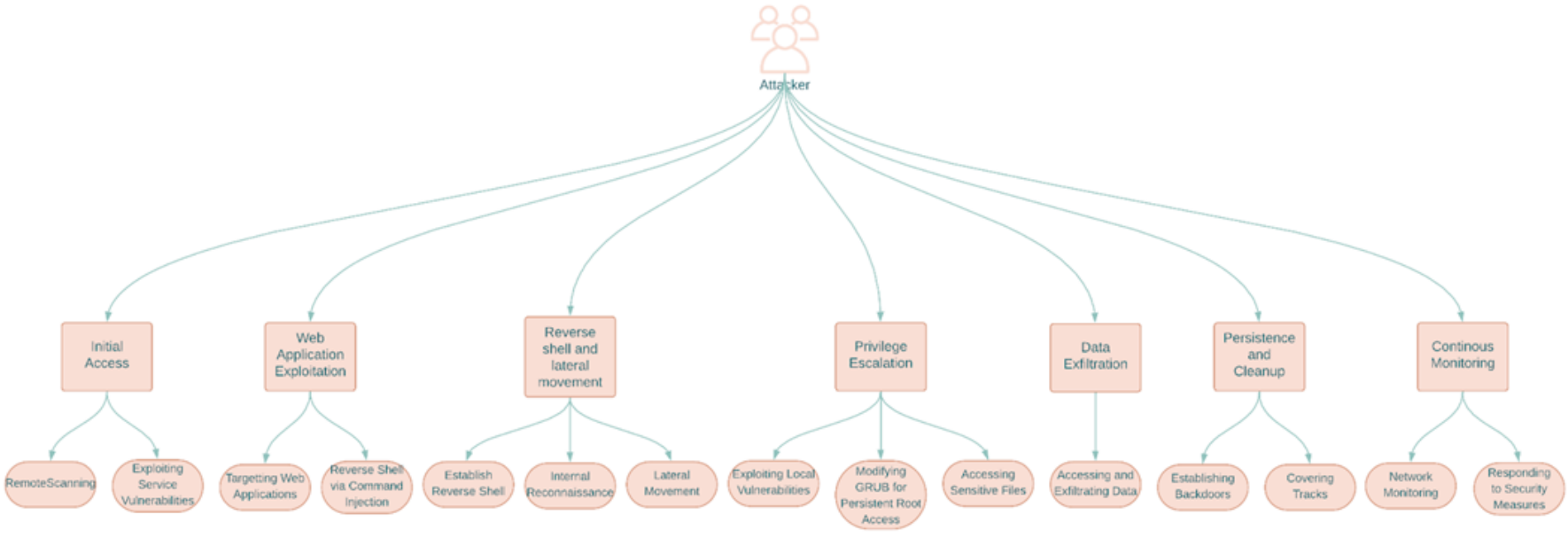
```
nmap -p- -sV 192.168.52.142
```

- Open Ports Analysis:
  - **Port 21 (FTP):** Running Service: FTP
  - **FTP Services:** vsftpd 3.0.3
  - **Port 22 (SSH):**
    - Running Service: SSH
    - SSH Services: OpenSSH 7.2p2 Ubuntu 4ubuntu 2.8
  - **Port 23 (Telnet):**
    - Running Service: Telnet
    - Telnet Services: Linux Telnetd
  - **Port 25 (SMTP):**
    - Running Service: SMTP (Simple Mail Transfer Protocol)
    - SMTP Services: Postfix
  - **Port 80 (HTTP):**
    - Running Service: HTTP
    - Possible HTTP Services: Apache httpd 2.4.18

2. **Access the system by exploiting a vulnerable running or open service (15 points)**
   - Accessed the vulnerable DVWA (Damn Vulnerable Web Application) webpage by navigating to the master directory with the assistance of Gobuster.
   - Successfully exploited the DVWA through a command injection attack, resulting in the establishment of a reverse shell on my local machine.
   - Subsequently, we utilized Linpeas to perform privilege escalation, ultimately gaining root privileges.
   - From this point, we conducted enumeration and uncovered all the required flags and other user credentials.
   - To transfer the exploit files from my local machine to the target machine, I set up a server locally and downloaded the files from the target machine using the `wget` command.
3. **Detail the flaws in the web server running on the system (10 points)**
   - Unsecured SSH Access:
     - The server allowed SSH access using the weak password **"judgement"** for the **"emaw"** user. This exposes the server to brute-force attacks and unauthorized access through SSH.
   - Lack of Secure Password Storage:
     - The web server stored user authentication data in the `/etc/shadow` file. Storing passwords in this manner is insecure as it exposes the hashed passwords, which can be subject to brute-force attacks or dictionary attacks.
   - Inadequate Directory Permissions:

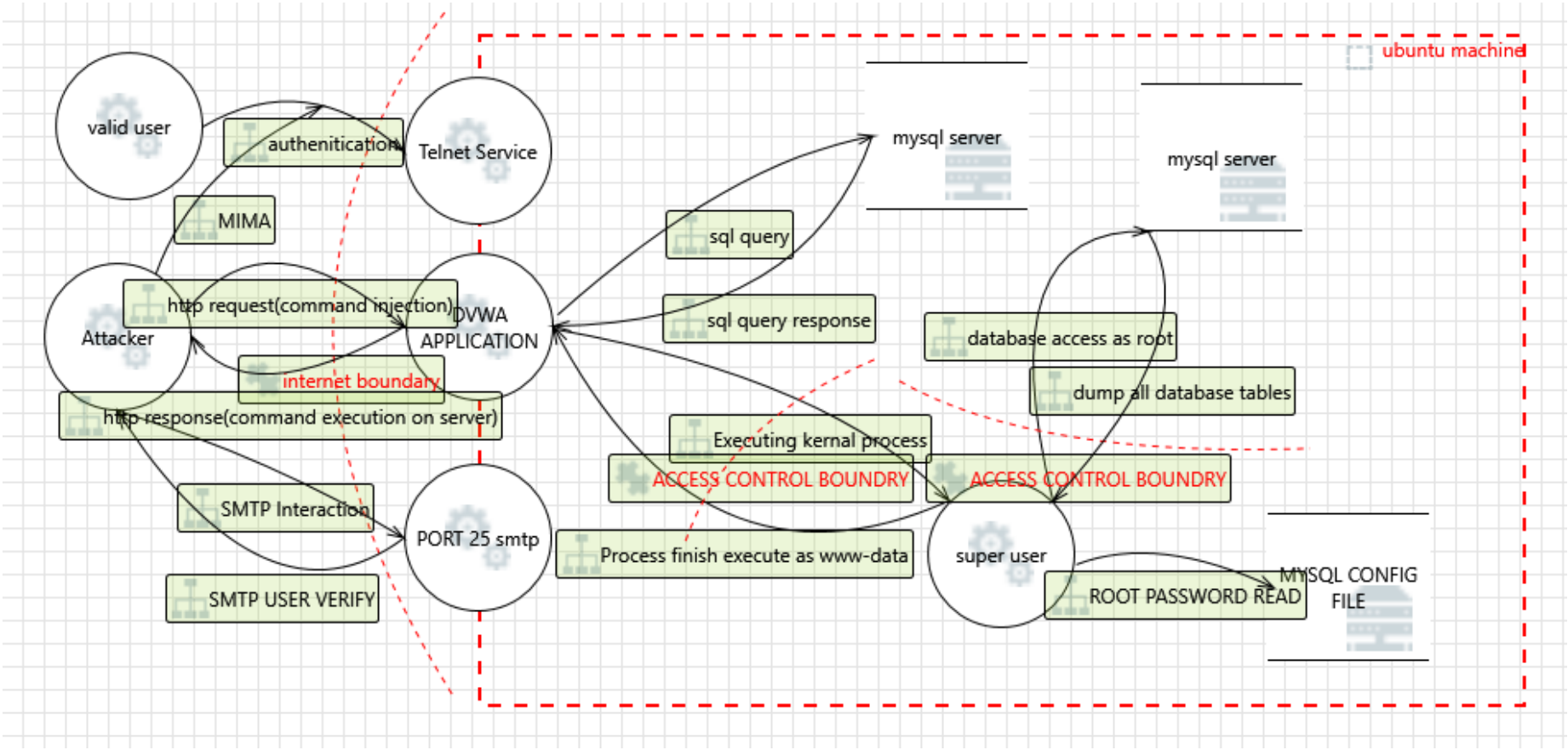
    - The web server had directories with insufficient access controls.
    - For example, directories like '/master/' and user folders did not have proper permissions, which could lead to unauthorized access and information disclosure.
- Lack of Encryption for Sensitive Data:
    - Sensitive data, such as database credentials, were stored in configuration files without encryption.
    - In a production environment, sensitive information should be encrypted to protect it from unauthorized access in case of a breach.
- Unrestricted Root Access:
    - The penetration test demonstrated the ability to escalate privileges and gain root access on the server.
    - This suggests insufficient security controls and potential vulnerabilities that could be exploited to compromise the entire system.
- Insecure Steganography:
    - The use of steganography to hide messages within images on the website could be considered a security flaw.
    - While steganography itself is not necessarily a vulnerability, it can be used to hide malicious content or instructions, making it a potential security risk.
- Outdated Software:
    - The report mentions specific versions of software like vsftpd and OpenSSH.
    - If these are not updated to the latest versions, they may be vulnerable to known exploits.
    - Maintaining up-to-date software is crucial for mitigating security risks.
- Unpatched Vulnerabilities:
    - The report identifies specific vulnerabilities like CVE-2017-16995 and CVE-2016-5195. These vulnerabilities should be patched as soon as possible to prevent attackers from exploiting them.

4. **Crack passwords (15 points)**
    - **User: emaw**
        - **Method:** Decoded an image found on the homepage.
        - **Password Found:** judgement
        - We successfully cracked the password for the user 'emaw' by carefully analyzing and decoding a cryptic image displayed on the homepage.
        - Using the online tool 'stylesuxx.github.io/steganography', we aimed to decode any concealed messages within the image.
        - The tool revealed a hidden string "*judgement*" within the image.
    - **User: thanos**
        - **Method:** Exploited a command injection vulnerability and accessed MySQL database.
        - **Password Discovery:** Accessed through database credentials.
        - For the user 'thanos' we identified and exploited a command injection vulnerability.
        - This breach allowed me to gain access to the database credentials.
        - Subsequently, we retrieved the user’s password directly from the MySQL database.
        - The password was "*infinitystones*".
    - **User: cobsidian**
        - **Method:** Employed hash cracking and brute force attack with a custom wordlist.
        - **Password Found:** blackdwarf
        - For the user cobsidian I took a more complex approach by generating a custom Marvel-themed wordlist and developing a specialized script to optimize it.
        - Utilizing hash cracking techniques in conjunction with a targeted brute force attack using this wordlist.
        - We successfully deciphered the password which is "*blackdwarf*".
    - **User: pmidnight**
        - **Method:** Similar approach as with 'cobsidian' using hash cracking and brute force.
        - **Password Found:** carriecoon
        - Same methodology as above user.
5. **Define the external attack surface of the system (10 points)**



- **Initial Access**
  - **Remote Scanning:**
    - Utilize Nmap or Shodan to perform reconnaissance, scanning the target's IP range to identify open ports and services. This step is crucial for gathering information about the network infrastructure, including identifying services like FTP, SSH, SMTP, telnet, or HTTP.
    - Example: Scanning the IP range 192.168.52.0/24 revealed open ports for various services, suggesting possible entry points for exploitation.
  - **Exploiting Service Vulnerabilities:**
    - Target identified services for known vulnerabilities. For example, an outdated FTP service or SSH version might have known exploits available.
    - Leverage these vulnerabilities to gain initial access to the system. This could involve brute-forcing passwords, exploiting a service misconfiguration, or using a known exploit against a specific service version.
- **Web Application Exploitation**
  - **Targeting Web Applications:**
    - Focus on common web application vulnerabilities in platforms like DVWA (Damn Vulnerable Web Application).
    - Identify SQL Injection, Cross-Site Scripting (XSS), or Command Injection vulnerabilities which are common and often lead to significant security breaches.
  - **Reverse Shell via Command Injection:**
    - Exploit Command Injection vulnerabilities to execute arbitrary commands on the server.
    - Example: A vulnerable parameter in a web application was used to inject a shell command, allowing the establishment of a reverse shell.
- **Reverse Shell and Lateral Movement**
  - **Establish Reverse Shell:**
    - Use the established reverse shell to interact with the compromised system, providing a command-line interface to the attacker.
    - This step is critical for deeper access and control over the target system.
  - **Internal Reconnaissance and Lateral Movement:**
    - Perform internal reconnaissance to map the network and identify additional targets.
    - Use lateral movement techniques to expand control within the network, targeting other systems and increasing the attacker's foothold.
- **Privilege Escalation**
  - **Exploiting Local Vulnerabilities:**
    - Identify and exploit local vulnerabilities like CVE-2017-16995 or Dirty COW for escalating privileges to root or administrative level.
    - Example: Utilizing a known exploit for CVE-2017-16995 on an outdated kernel version provided root access.
  - **Modifying GRUB for Persistent Root Access:**
    - Edit GRUB configuration to boot into single-user mode, providing root access without authentication.
    - This method can be used for persistent, unrestricted access to the system.
  - **Accessing Sensitive Files:**
    - With elevated privileges, access critical files like /etc/passwd and /etc/shadow to extract user credentials and other sensitive data.
- **Data Exfiltration**
  - **Accessing and Exfiltrating Data:**
    - Access the MySQL database to extract sensitive information.
    - Decrypt encrypted files to uncover valuable data.
- **Persistence and Cleanup**
  - **Establishing Backdoors:**
    - Install backdoors for persistent access. This could involve adding SSH keys, creating hidden user accounts, or installing remote access tools.
  - **Covering Tracks:**
    - Clean up logs and traces of the attack to avoid detection. This includes clearing command history, log files, and any artifacts left by the tools used.
- **Continuous Monitoring**
  - **Network Monitoring:**
    - Continuously monitor the network for changes, new vulnerabilities, or security updates that might affect the established foothold.
    - Adapt to these changes by modifying tactics or exploiting new vulnerabilities.
  - **Responding to Security Measures:**
    - Stay ahead of network defenses and security updates. If the target patches a vulnerability, find new methods to maintain access or exploit different weaknesses.

6. **Develop a threat model of the system and detail the 5 threat vectors (10 points)**



- **Telnet Man-in-the-Middle (MITM) Attack**
  - **Nature:** Telnet is an older network protocol used for remote communication, which does not encrypt data. This makes it vulnerable to MITM attacks, where an attacker intercepts the communication between the Telnet client and server.
  - **Exploitation:** Attackers can eavesdrop on unencrypted Telnet sessions, capturing sensitive information like login credentials. They can also potentially alter the communication data in real-time.
  - **Impact:** The primary risks include unauthorized access to sensitive information, account compromise, and the potential for further network intrusion or data manipulation.
- **SMTP Command Execution to Verify Users Externally**
  - **Nature:** This involves exploiting vulnerabilities in the Simple Mail Transfer Protocol (SMTP), used for sending emails, to execute commands or verify user accounts externally.
  - **Exploitation:** Attackers can use specially crafted SMTP commands to extract information about email accounts or potentially execute unauthorized commands on the mail server.
  - **Impact:** Such vulnerabilities can lead to information disclosure, unauthorized access to email accounts, and could be a precursor to more severe attacks like spear-phishing or broader network compromise.
- **DVWA Command Execution**
  - **Nature:** Damn Vulnerable Web Application (DVWA) is intentionally insecure for educational purposes. Command execution vulnerabilities in DVWA can be exploited if present in a live environment.
  - **Exploitation:** Attackers can execute arbitrary commands on the server hosting DVWA, typically by exploiting input validation flaws.
  - **Impact:** This can lead to unauthorized access to the server, data breaches, and the possibility of further attacks on the network infrastructure.
- **Privilege Escalation Using Outdated Linux Kernel (Kernel Exploit)**
  - **Nature:** Vulnerabilities in outdated Linux kernels can be exploited for privilege escalation, allowing a user with limited privileges to gain higher-level access.
  - **Exploitation:** Attackers who have gained initial access to the system can exploit these kernel vulnerabilities to escalate their privileges to root level.
  - **Impact:** Gaining root access can lead to complete system control, data compromise, installation of malicious software, and using the system for further attacks.
- **Plain text Password Stored in MySQL Server**
  - **Nature:** This involves storing user passwords in plaintext in a MySQL database, which is a significant security risk.
  - **Exploitation:** If attackers gain access to the database, they can easily read and use these plaintext passwords. Additionally, finding the MySQL root password in a configuration file can give complete control over the database.
  - **Impact:** The risks include unauthorized access to user accounts, potential data breaches, and the ability for attackers to manipulate or destroy database contents.

7. **Gain root access to the server (5 points)**
   - Gaining through running the exploit.
     - Gaining root access involved several key steps.
     - Initially, a stable shell was established using a Python command.
     - This stable shell was then leveraged to exploit a known vulnerability **CVE-2017-16995** which is an eBPF vulnerability.
     - To exploit this a specific script was downloaded from the Exploit Database and executed on the target system.
     - Upon successful execution of this exploit the **whoami** command was used which confirmed the escalation to root user privileges.
     - This process transitioned the access level from a normal www-data user shell to root access.
   - Hack method.
     - We can login into the VM machine as single user mode.

- we can do that by going into recovery mode in grub and add a new user into sudo (wheel) group.
- In single-user mode we by default have root access without the need for a password.
- After that we can add a new user to the sudo ers group by `adduser -a -G <new-user> sudo`.
- After completing this we can modify the grub setting to login as single user mode by default or login as new user we created cause we will have sudo privileges.

Task 2: Find the Hacker and his secret

Your mission is to identify the hacker who infiltrated the server and uncover specific information about their activities:

1. **The hacker’s name (5 points)**
   - The Hackers name is "*thanos*".
   - "wwonka" is not related to marvel so he is a potential suspect.
2. **The password protecting the hacker’s file (3 points)**
   - The password protecting the hacker's file `thoughts.enc` is "*destiny*".
3. **Contents of an encrypted file left behind by the hacker (5 points)**
   - The encrypted file was left behind in the user's home directory at `/home/thanos/thanos.enc`
   - The message reads: *I have hidden the infinity stones on this server and encrypted them so that I can make sure they are protected from prying eyes. I will have to come back once I have the gauntlet that the dwarves of Nidavelier are making for me. Each stone is protected by its name. Once I gather them, I will be able to fulfill my destiny - to bring balance to the universe once again.*
4. **Contents and location of each special file hidden on the server (12 points)**
   - File1: stone1.enc
     - Key: power
     - Contents: Power
     - Path: `/xandar/stone1.enc`
   - File2: stone2.enc
     - Key: space
     - Contents: Space
     - Path: `/var/log/asgard/stone2.enc`
   - File3: stone3.enc
     - Key: reality
     - Contents: Reality
     - Path: `/home/knowhere/stone3.enc`
   - File4: stone4.enc
     - Key: soul
     - Contents: Soul
     - Path: `/etc/vormir/stone4.enc`
   - File5: stone5.enc
     - Key: time
     - Contents: Time
     - Path: `/usr/lib/titan/stone5.enc`
   - File6: stone6.enc
     - Key: mind
     - Contents: Mind
     - Path: `/var/www/earth/stone6.enc`
