Final Engagement

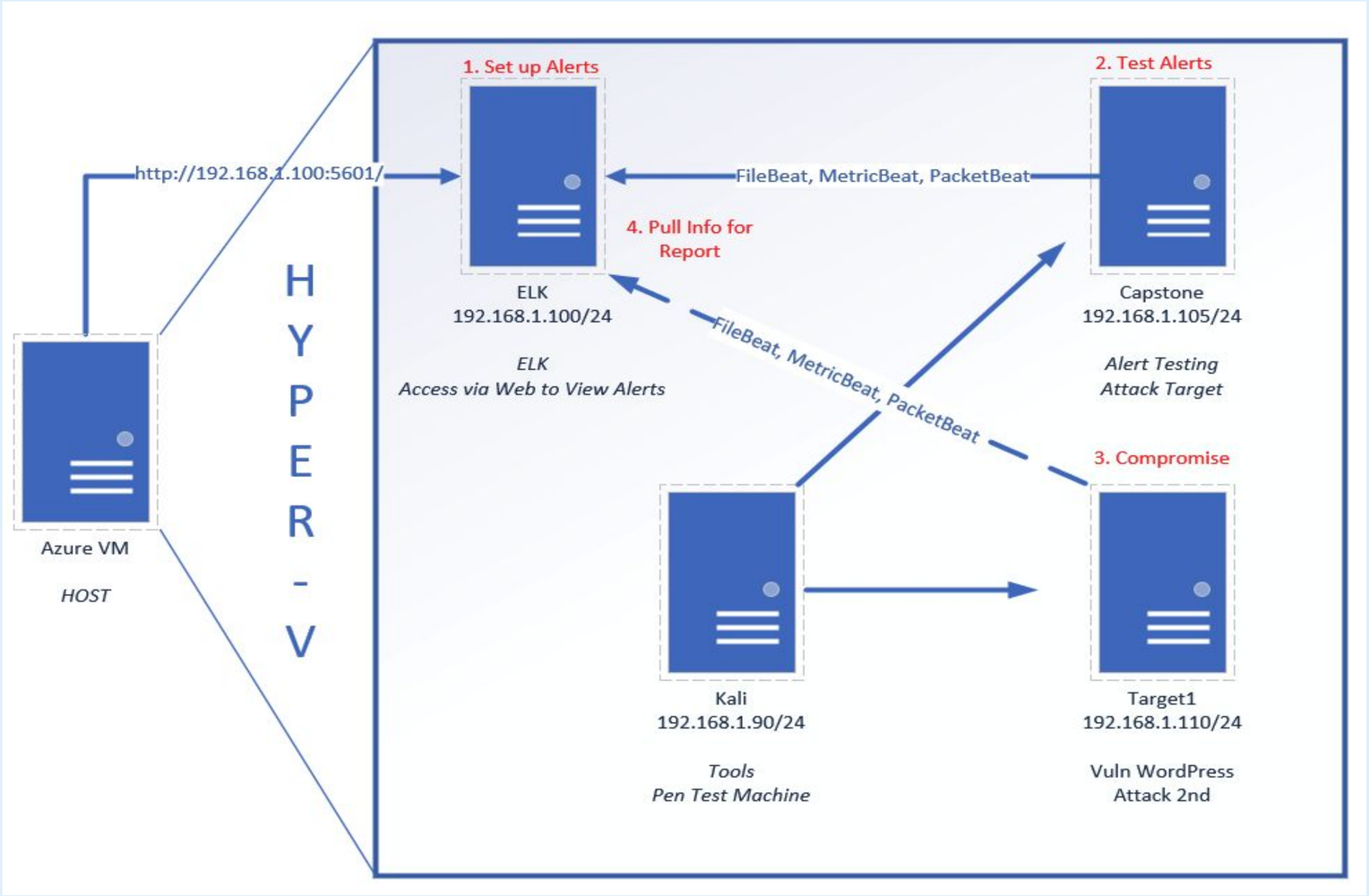
Attack, Defense & Analysis of a Vulnerable Network

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
Hostname: ML-REFVM-684427

Machines

IPv4: 192.168.1.100
OS: Ubuntu 18.04.4 LTS
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04.4 LTS
Hostname: Capstone

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

IPv4: 192.168.1.90
OS: Kali GNU/Linux Rolling
Hostname: Kali

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Weak Password	Passwords were simple to break as they were short in length and did not require special characters.	Brute force attack on passwords were made simple by using John to crack passwords.
User Enumeration	Enumeration was gathered to expose account usernames and unprotected files and directories.	Allowed us to gain to access to usernames which could then be used in the brute force attack.
Privilege Escalation	File permissions and exposed files allowed access to sensitive files.	Allowed access to wp_config.php which had the database password in plain text, which allowed further escalation.

Exploits Used

Exploitation: User Enumeration

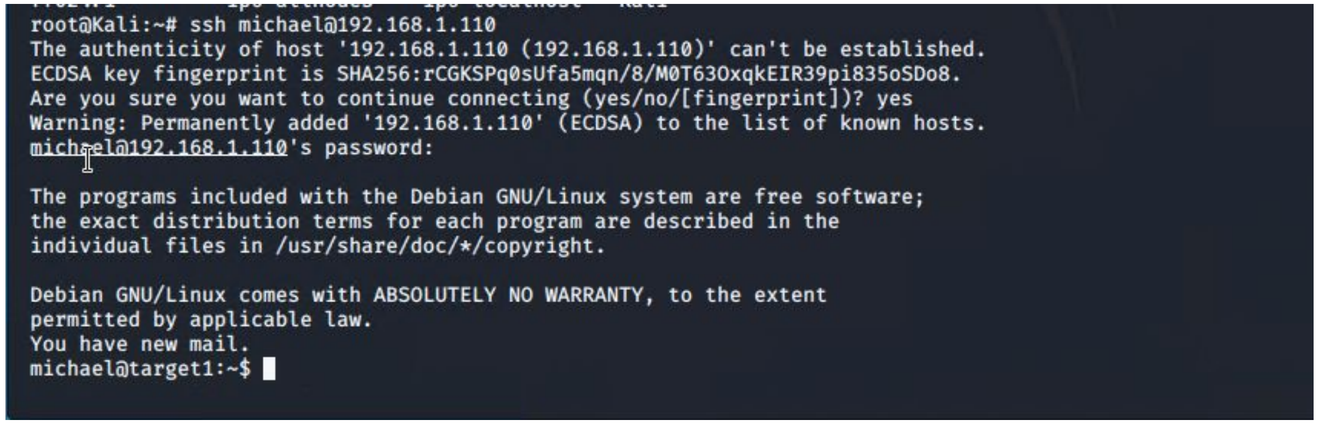
Summarize the following:

- How did you exploit the vulnerability?
  - wpscan was used to enumerate users
- What did the exploit achieve?
  - The exploit provided usernames which were then used to gain access to the server via SSH.
- Include a screenshot or command output illustrating the exploit.

Exploitation: Weak Password

Summarize the following:

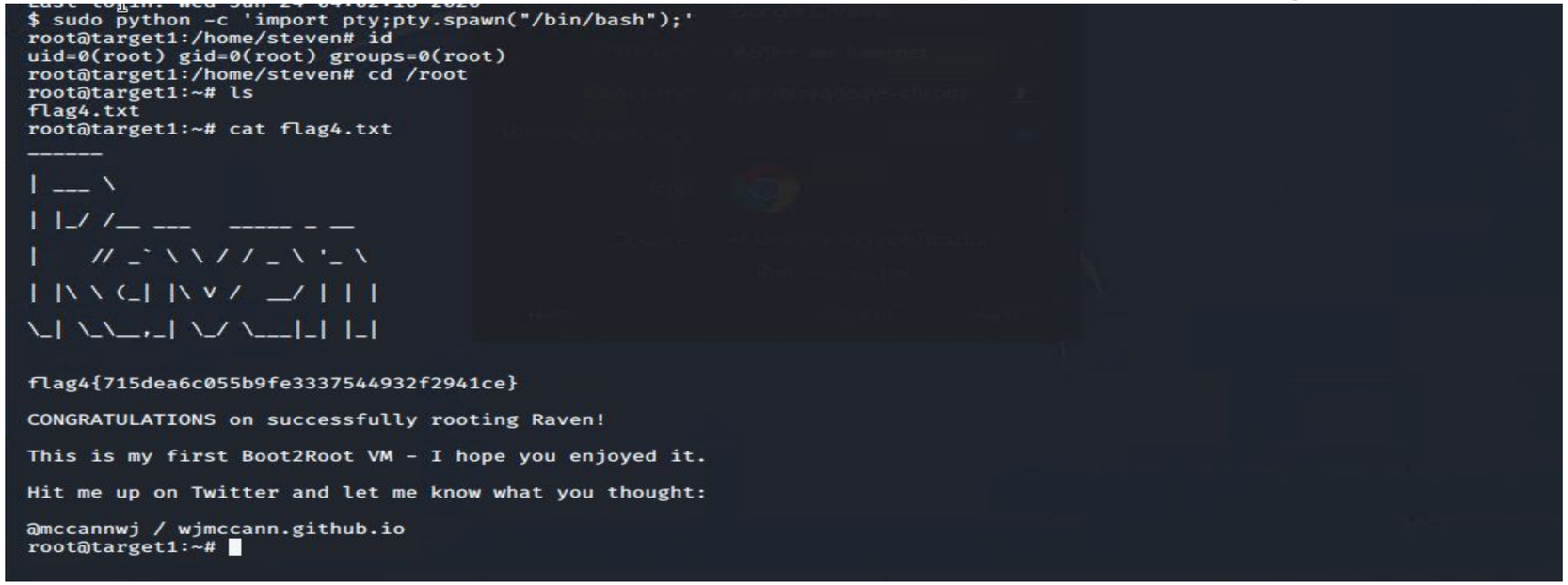
- How did you exploit the vulnerability?
  - We simply used the weak password to brute force the account. In this case, Michael used a password identical to his name: “michael”
- What did the exploit achieve?
  - Really the exploit was just manually trying weak passwords like ‘password’ and ‘michael’
- Include a screenshot or command output illustrating the exploit.



Exploitation: Privilege Escalation

Summarize the following:

- How did you exploit the vulnerability? Two parts, first was to gain access to MySQL database and second was to use Python script to escalate privileges.
- What did the exploit achieve? After brute forcing Steven's password from MySQL hash, we were able to use Python to escalate to root.
- Include a screenshot or command output illustrating the exploit.



Avoiding Detection

Stealth Exploitation of Weak Passwords

Monitoring Overview

- Which alerts detect this exploit? Excessive HTTP Errors
- Which metrics do they measure? WHEN count() GROUPED OVER top 5 ‘http.response.status_code’ IS ABOVE 400 FOR LAST 5 minutes
- Which thresholds do they fire at? The first when threshold is exceeded in a 5 minute period

Mitigating Detection

- How can you execute the same exploit without triggering the alert? Same exploit can be used as long as attempts stay under threshold
- Are there alternative exploits that may perform better? A dictionary attack is a better alternative, but you would really need to manage number of errors

Stealth Exploitation of User Enumeration

Monitoring Overview

- Which alerts detect this exploit? Excessive HTTP Errors
- Which metrics do they measure? WHEN count() GROUPED OVER top 5 ‘http.response.status_code’ IS ABOVE 400 FOR LAST 5 minutes
- Which thresholds do they fire at? The first when threshold is exceeded in a 5 minute period

Mitigating Detection

- How can you execute the same exploit without triggering the alert? You could technically look at the blog posts to gain access to username associated to the site
- Are there alternative exploits that may perform better? The above would get you username information but you would still need to brute force the password

Stealth Exploitation of Privilege Escalation

Monitoring Overview

- Which alerts detect this exploit? Alert that detects when account uses sudo who is not part of the sudoers group
- Which metrics do they measure? Measurement is when a non-sudo account attempts to use sudo
- Which thresholds do they fire at? Fires immediately when detected

Mitigating Detection

- How can you execute the same exploit without triggering the alert?
  - Access to an account that already has sudo access would be necessary
- Are there alternative exploits that may perform better?
  - Use a different exploit to try to escalate privileges without using sudo