Final Engagement

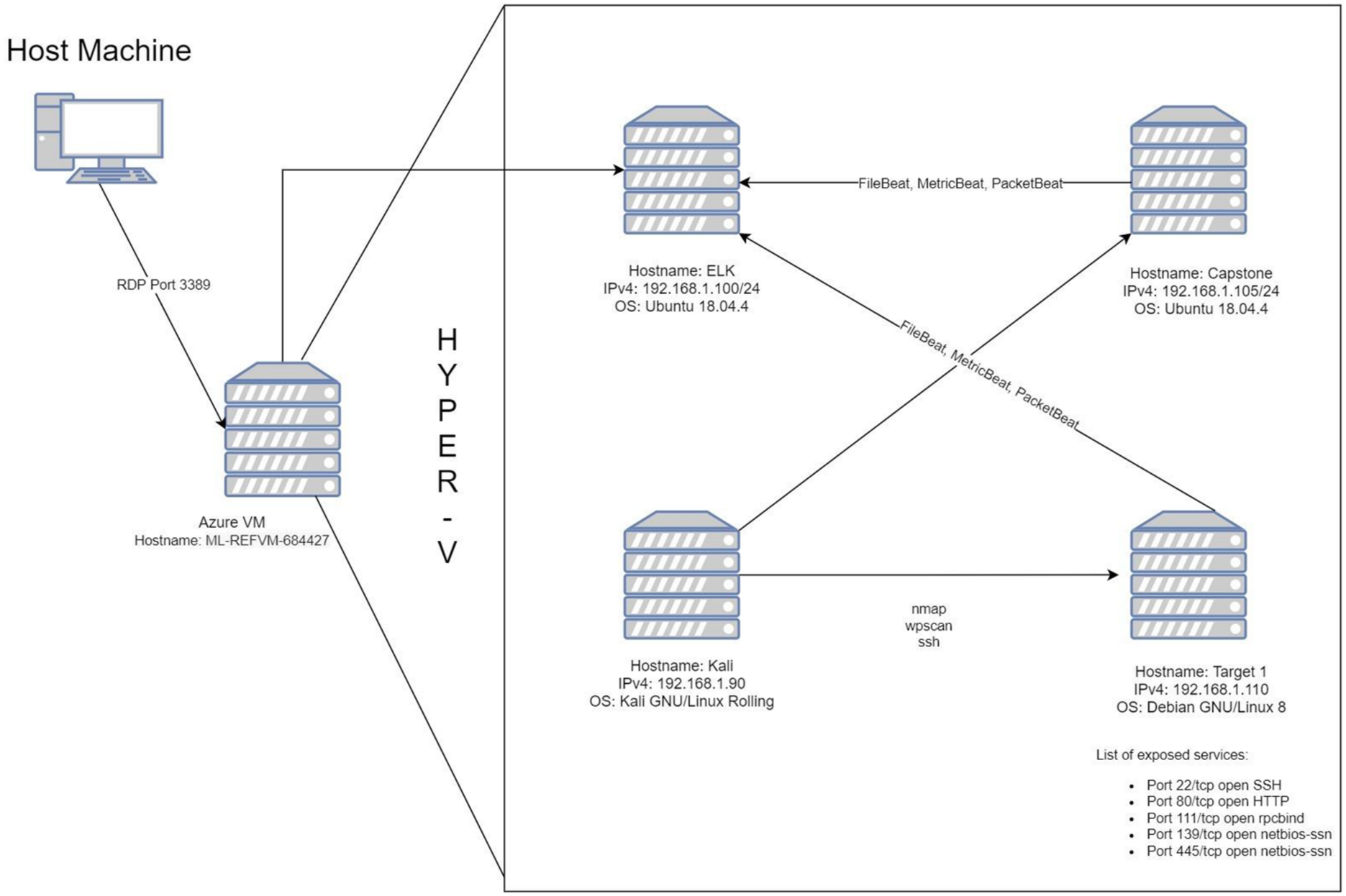
Attack, Defense & Analysis of a Vulnerable Network

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
Host name: ML-REFVM-684427

Machines
IPv4: 192.168.1.100
OS: Ubuntu 18.04.4
Host name: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04.4
Host name: Capstone

IPv4: 192.168.1.110
OS: Debian GNU / Linux 8
Host name: Target 1

IPv4: 192.168.1.90
OS: Kali GNU / Linux Rolling
Host name: Kali

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Weak Password Vulnerability	Passwords didn't require special characters/symbols, and length.	This will make brute force attacks more successful since the password is easy to crack. We were able to guess a user's password.
Security Misconfiguration (ie privilege escalation)	Misconfiguration exposes unprotected files/directories, default account credentials etc	This allows unprivileged users access to files they shouldn't be allowed to view. Example: users shouldn't be able to view the "wp-config.php" file which has the mysql password.
User Enumeration	Enumeration is used to gather information	This allows bad actors to gather valid usernames to gain access and exploit through brute force attacks.

Exploits Used

Exploitation: User Enumeration

- **How did you exploit the vulnerability?**
  - Used wpscan to enumerate users.
- **What did the exploit achieve?**
  - This exploit provided us with valid usernames which helped us to gain access to the server via SSH.

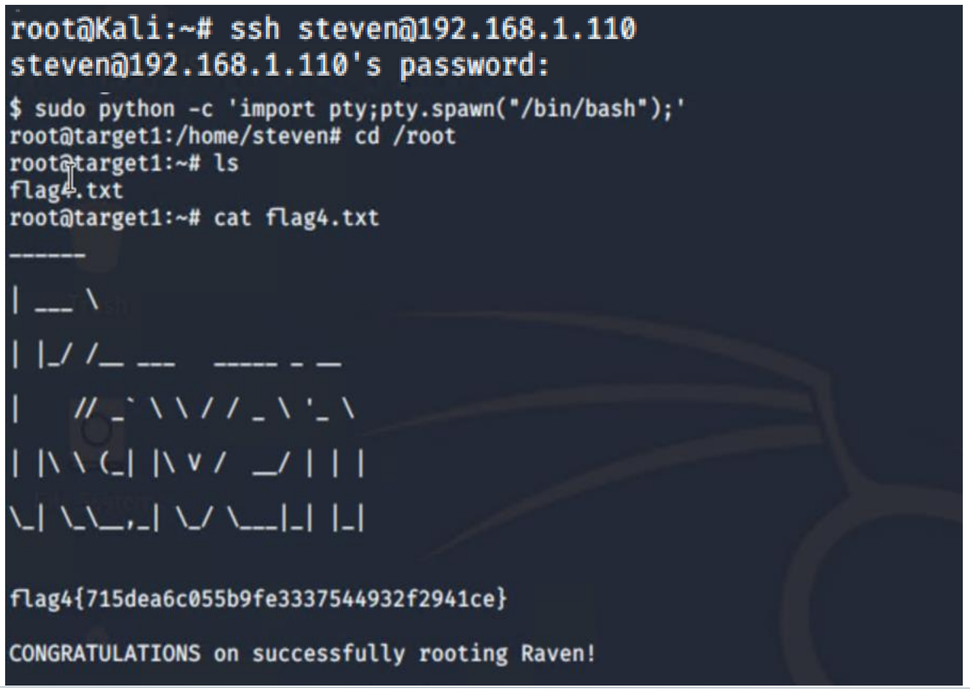
```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate u

[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Exploitation: Weak Password

- **How did you exploit the vulnerability?** We were able to guess Michael's weak password by brute force. Michael's password is "michael".
- **What did the exploit achieve?** Access to Michael's account, his password was michael.

Exploitation: Security Misconfiguration

- **How did you exploit the vulnerability?**
  - Logged into Steven’s account and used sudo Python to escalate to root access .
- **What did the exploit achieve?**
  - This exploit gave us root access from Steven’s account.



Avoiding Detection

Stealth Exploitation of Weak Passwords

Monitoring Overview

- **Which alerts detect this exploit?** Excessive HTTP Errors Threshold Alert
- **Which metrics do they measure?** WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- **Which thresholds do they fire at?** 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes

Mitigating Detection

- **How can you execute the same exploit without triggering the alert?**
  - By making sure to not reach the threshold of 400 attempts.
- **Are there alternative exploits that may perform better?**
  - Utilize a dictionary attack.

Stealth Exploitation of Security Misconfiguration (ie privilege escalation)

Monitoring Overview

- **Which alerts detect this exploit?** Alert that detects when python is utilized with sudo to escalate privileges.
- **Which metrics do they measure?** The use of python in the command line/terminal.
- **Which thresholds do they fire at?** Alerts any time python is paired with sudo.

Mitigating Detection

- **How can you execute the same exploit without triggering the alert?**
  - Gain access to an admin account.
- **Are there alternative exploits that may perform better?**
  - Gain root privileges without using python.

Stealth Exploitation of User Enumeration

Monitoring Overview

- **Which alerts detect this exploit?** An alert that detects when wpscan is used against an ip address
- **Which metrics do they measure?** The use of wpscan.
- **Which thresholds do they fire at?** When an non-admin account runs wpscan.

Mitigating Detection

- **How can you execute the same exploit without triggering the alert?**
  - Utilizing wpscan through an admin account.
- **Are there alternative exploits that may perform better?**
  - Enumerate usernames through author archives or wp-login.php.