Trine Security

Penetration Testing Report

Happy Accident Labs

Report Version 3

Lathan Birmingham

December 11, 2022

Table of Contents

Report Properties

Client Information

Happy Accident Labs

Bill Winnicott, CIO

- Develops miniature IoT devices for use as personal assistance
- Potential investor is concerned that intellectual property (IP) has been stolen

Company

Trine Security

Pentester Information

Lathan Birmingham
lbirmingham@my365.belleve.edu
(980) 522-9996

Report Distribution

Version	Name	Date	Notes
1	Lathan Birmingham	10/18/2022	Initial draft
2	Lathan Birmingham	12/10/2022	Add findings, details & appendix
3	Lathan Birmingham	12/17/2022	Finalize report

Executive Summary

Trine Security has been contracted by Happy Accident Labs to conduct a penetration test to determine vulnerabilities that may be present in internal networks or company owned assets. This test will simulate an attacker attempting to target Happy Accident Labs' internal network using a variety of attacks. We will identify the potential exploitation of security flaws that could allow a malevolent actor to alter the confidentiality, integrity, or availability of Happy Accident Labs' data. All procedures were conducted in a controlled environment and in compliance with NIST SP 800-115.

Project Objectives

- Identify any known vulnerabilities to Happy Accident Labs' company owned assets
- Develop a mitigation plan to address vulnerabilities
- Determine the impact of a security breach on:
    - Confidentiality and integrity of Happy Accident Labs' private data
    - Internal infrastructure and availability of Happy Accident Labs' systems

Scope

The following area(s) were included in the scope of the penetration test:

- Happy Accident Labs' Internal Networks
    - Testing against hosts in the networks
    - Testing against internet facing hosts

Authorization

Bill Winnicott, CIO of Happy Accident Labs has authorized Trine Security to perform a black-box penetration test only on Happy Accident Labs' internal network. This does not include the networks of their clients or suppliers.

This penetration test is compliant with NIST SP 800-115 and ISO 27001.

Assumptions

An investor is withholding his money until a penetration test is performed, because he is concerned that intellectual property has been stolen and is being used by competitors to beat them to the market. The penetration test has been conducted with this concern at the forefront.

Timeline

At the time of the penetration test, teams will be working so we will not impact the operations of the company.

Summary of Test

For this assessment, Happy Accident Labs provided minimal information about their company.

This test began with capturing a WPA handshake using a Wi-Fi Pineapple. After collecting the BSSID of the network, I cracked the PSK using aircrack-ng. Once connected to the network, I did various scans to collect information on the hosts and the setup of the network. Once I identified the hosts, I ran port scans on each host to identify where vulnerabilities might be present using nmap and sparta. Vulnerability scans were run on each host using OpenVAS and Greenborne Security Assistant, where I identified a variety of vulnerabilities.

One of the severe vulnerabilities identified was CVE-2017-0143-0148 which I exploited via Metasploit. From here, I collected password hashes and cracked the login credentials for several users and accessed the internal HAL network. Once inside the HAL network, I accessed SMB shares on various hosts where I collected critical company information. Once I finished exporting sensitive company files, I installed a backdoor using netcat to retain access to the HAL network in the case that the vulnerability I initially exploited was patched.

Critical Vulnerabilities

The two most critical vulnerabilities I identified are CVE-1999-0519 and CVE-2017-0143-0148. CVE-1999-0519 allows null session authentication in a SMB/NetBIOS share. CVE-2017-0143-0148 allows an attacker to access many Windows shares through the network and may possibly allow an attacker to read/write confidential data. During the penetration test, I exploited CVE-2017-0143 on host 10.19.99.10 and accessed the SMB shares on other hosts using the null session bypass vulnerability CVE-1999-0519.

Prioritized Recommendations

1. Patch CVE-1999-0519: restrict access to SMB/NetBIOS shares by a password. filter the NetBIOS port from outside access and restrict permissions on the share.
2. Patch CVE-2017-0143-0148: update Windows OS to the latest version.
3. Invest in IDS or SIEM to assist with monitoring and managing system access.
4. Strengthen password policy to require more complex passwords
5. Run vulnerability scans frequently, minimally on a monthly basis

List of Findings

Risk Analysis

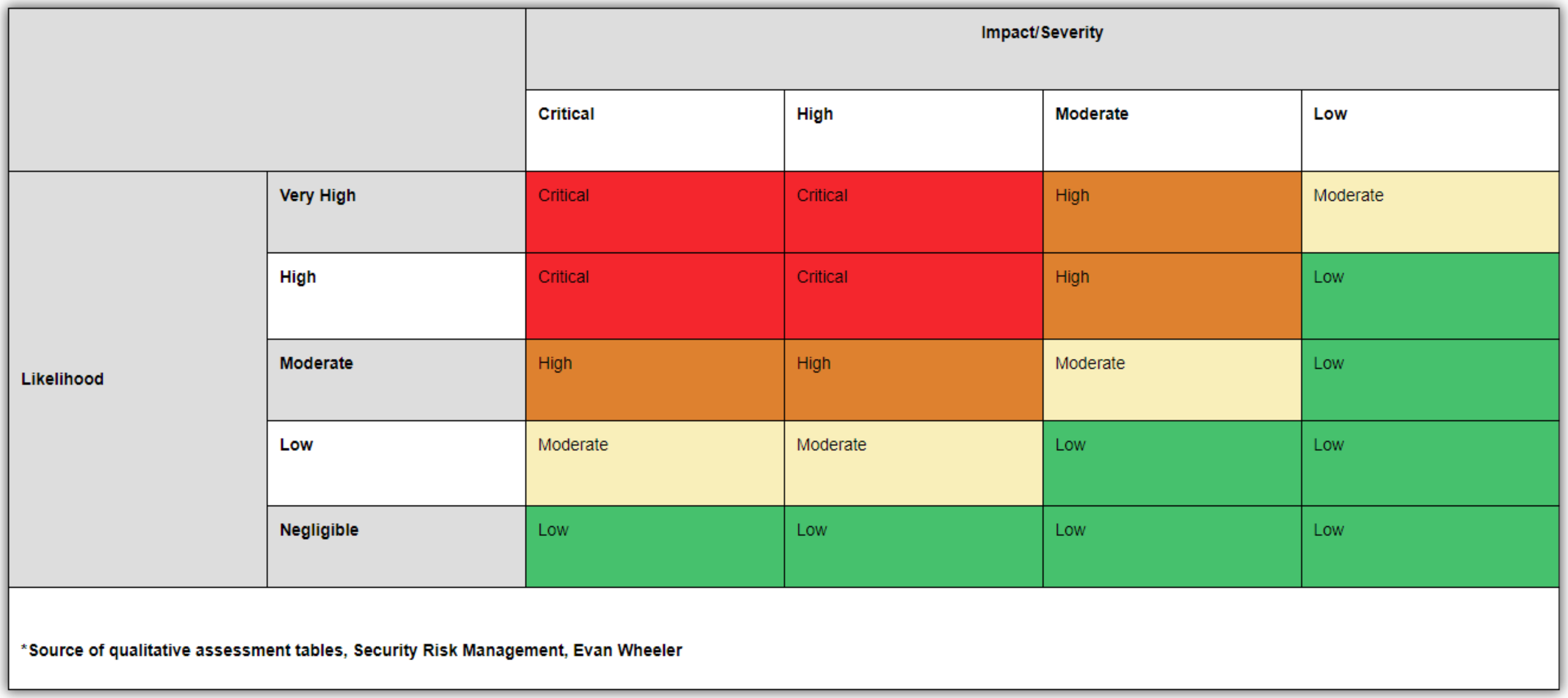
Determine the **impact and severity** of a vulnerability:

Level	*Description*
Low	May be a deviation from recommended practice or an emerging standard. May lack a security governance process or activity but have no direct exposure.
Moderate	May indirectly contribute to unauthorized activity or just have no known attack vector. May result in a degradation of service and/or a noticeable decrease in service performance.
High	May allow limited access to or control of the application, system, or communication, including only certain data and functionality. May result in a short disruption of service and/or denial of service for part of the user community.
Critical	May allow full access to or control of the application, system, or communication, including all data and functionality. May result in a prolonged outage affecting all users of the service.

Determine **likelihood** of the vulnerability being exploited:

Level	*Description*
Negligible	The threat source is part of a small and trusted group; controls prevent exploitation without physical access to the target; significant inside knowledge is necessary, or purely theoretical.
Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.
Moderate	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.

After determining the likelihood and impact/severity of a vulnerability, use the following chart to determine the final risk rating:



		Impact/Severity			
		Critical	**High**	**Moderate**	**Low**
Likelihood	**Very High**	Critical	Critical	High	Moderate
	High	Critical	Critical	High	Low
	Moderate	High	High	Moderate	Low
	Low	Moderate	Moderate	Low	Low
	Negligible	Low	Low	Low	Low

***Source of qualitative assessment tables, Security Risk Management, Evan Wheeler**

Vulnerability	Affected Hosts	Impact	Risk Severity
CWE-319	10.19.99.1	Sensitive information is transmitted in cleartext. If a malicious actor intercepts HTTP network traffic, they could view sensitive information such as user credentials or other company information.	**Medium**
TCP Timestamps	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	“The remote host implements TCP timestamps and therefore allows to compute the uptime. It was detected that the host implements RFC1323.” Location: general/tcp	**Low**
SSL/TLS Untrusted Certificate Authorities	10.19.99.5	The service is using an SSL/TLS certificate from a known untrusted certificate authority. An attacker could use this for MitM attacks, accessing sensitive data and other attacks.	**Medium**
CVE-1999-0519	10.19.99.10 10.19.99.12 10.19.99.14 10.19.99.16 10.19.99.18	Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability. Problem: “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.” Location: 445/tcp	**High**
CVE-2017-0143-0148	10.19.99.10	Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) **Problem**: “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.	**High**

Vulnerability Details

CWE-319	
Description	“The software transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors. Many communication channels can be "sniffed" by attackers during data transmission. For example, network traffic can often be sniffed by any attacker who has access to a network interface. This significantly lowers the difficulty of exploitation by attackers,” (MITRE, 2019). “The host/application transmits sensitive information (username, passwords) in cleartext via HTTP,” (GreeneBorne Security).
Root Cause	“This weakness is caused by missing a security tactic during the architecture and design phase,” (MITRE, 2019).
Proof of Concept	The following input fields were identified: *http://HAL_GW.happyaccidentlabs.com/:passwordfld* *http://HAL_GW.happyaccidentlabs.com/license.php:passwordfld*
Impact	According to MITRE, anyone can read the information by gaining access to the channel being used for communication. “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,” (Greeneborne Security).
Likelihood	The likelihood of this vulnerability being exploited is high. According to OpenCVE, the complexity of this vulnerability is low, no escalated privileges are required, and it has a high impact on confidentiality of data.
Mitigation	“**Architecture and Design** Encrypt the data with a reliable encryption scheme before transmitting. **Implementation** When using web applications with SSL, use SSL for the entire session from login to logout, not just for the initial login page. **Testing** Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow

	the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. **Operation** Configure servers to use encrypted channels for communication, which may include SSL or other secure protocols," (MITRE, 2019).
References	*MITRE. 2019. CWE-319: Cleartext Transmission of Sensitive Information. Common Weakness Enumeration. Retrieved December 10, 2022, from https://cwe.mitre.org/data/definitions/319.html* *OpenCVE. (2021). 2021-22703. OpenCVE. Retrieved December 11, 2022, from https://www.opencve.io/cve/CVE-2021-22703*

TCP Timestamps

Description	"The remote host implements TCP timestamps and therefore allows to compute the uptime. It was detected that the host implements RFC1323," (Greeneborne Security).
Root Cause	"The remote host implements TCP timestamps, as defined by RFC1323/RFC7323," (E-Soft Inc. n.d.).
Impact	A side effect of this feature is that the uptime of the remote host can sometimes be computed," (E-Soft Inc. n.d.).
Mitigation	"To disable TCP timestamps on Linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment," (E-Soft Inc. n.d.).
References	E-Soft Inc. (n.d.). *General : TCP TIMESTAMPS*. Security Space. Retrieved December 11, 2022, from http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.80091

SSL/TLS Untrusted Certificate Authorities

Description	“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,” (Greeneborne Security).
Root Cause	This vulnerability occurs when the certificate installation was not completed on the server hosting the site.
Proof of Concept	When visiting a website, if there is a locked icon on the left of the URL bar, this indicates that this website has a trusted SSL/TLS certificate authority. If there is not a locked icon, this indicates that the certificate authority is untrusted.
Impact	If there is not a valid trusted certificate for a website, it opens the potential for MITM attacks, SSL stripping attacks, and advanced persistent malware.
Likelihood	“Assaults on trust through the SSL/TLS-encrypted traffic are now common and growing in frequency, sophistication, and sheer brazenness. The low-risk, high-reward nature of SSL/TLS vulnerability ensures that these trends will continue, placing organizations at risk of breach, failed audits, and unplanned system downtime,” (Venafi, n.d.).
Mitigation	The mitigation for this vulnerability is to replace the untrusted SSL/TLS Certificate Authority with a signed & trusted certificate authority.
References	Venafi. (n.d.). *Common SSL attacks: SSL & TLS key vulnerability*. Venafi. (n.d.). Retrieved December 11, 2022, from https://www.venafi.com/education-center/ssl/common-ssl-attacks

CVE-1999-0519

Description	“A NETBIOS/SMB share password is the default, null, or missing,” (MITRE, 1999).
Root Cause	This vulnerability is present on unpatched versions of Windows 95 and Windows NT prior to Service Pack 3 (SP3).
Proof of Concept	I was able to bypass many shares on the system using no username or password.

Impact	“This misconfiguration can allow access to the entire hard drive on unpatched versions of Windows 95 and Windows NT. If this vulnerability was detected on a version of Windows NT prior to Service Pack 3 (SP3), an attacker can use shares to cause the system to crash,” (IBM, n.d.).
Likelihood	The likelihood of this vulnerability being exploited is high. According to OpenCVE, the complexity of this vulnerability is low, no authentication is required, and it has a partial impact on confidentiality, integrity, and availability. This risk can be repeated until the vulnerability is mitigated. The exploit is publicly available and requires WAN/LAN access.
Mitigation	According to IBM, the remedy is to either set permissions explicitly or remove the share. IBM recommends explicitly setting the access control list on shares as a best practice. “Set the permissions explicitly or remove the share. **Grant share access only to approved users.** 1. From the local computer, open Windows NT Explorer. 2. Navigate to the shared folder. 3. Right-click the shared folder name and select Sharing to display the Properties dialog box. 4. Click Permissions. **Use these guidelines to review the listed permissions:** ▪ Remove or change any permissions such as Everyone - Full Control. This default permission allows all users to read, modify, and even change ownership and permissions on the items in the share. ▪ Review any names with Change or Full Control permissions and determine if the permission is appropriate. Consider using Read Only or No Access if these names do not need to modify items in the share. ▪ Review any names that should not be in the list, and remove the name or change their permission as appropriate,” (IBM, 1997).
References	*IBM. (1997). SMB Share Full Access CVE-1999-0519 Vulnerability Report. IBM X-Force Exchange. Retrieved December 10, 2022, from https://exchange.xforce.ibmcloud.com/vulnerabilities/1*

CVE-2017-0143-0148

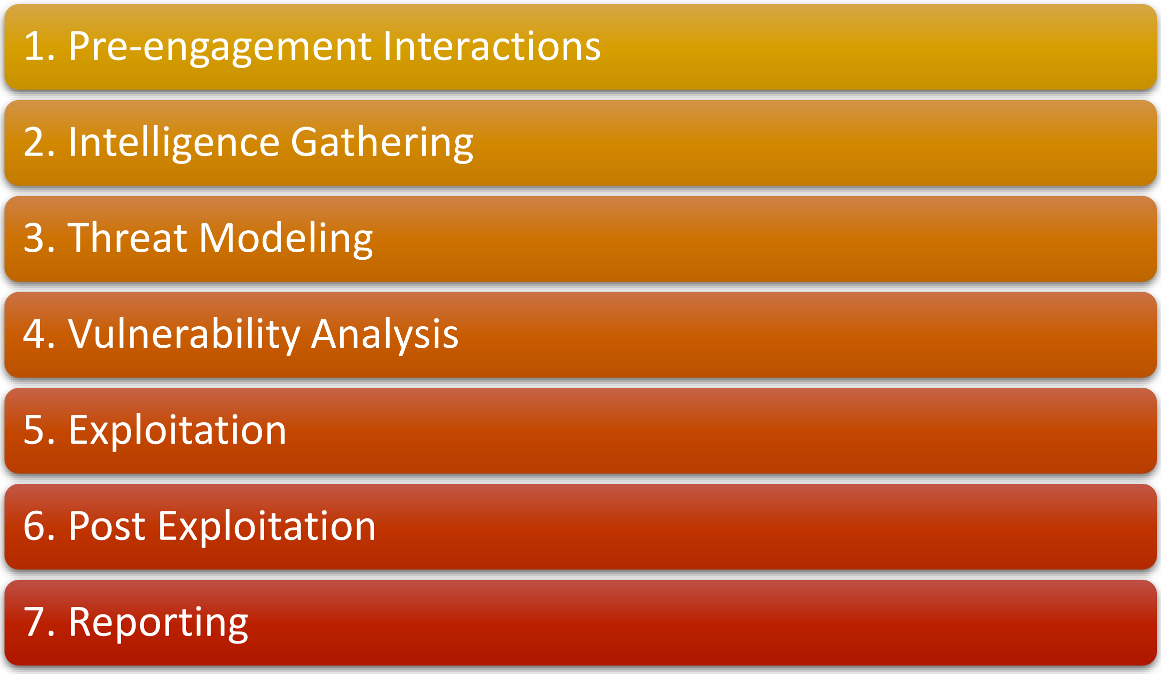
Description	This vulnerability “allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability,” (MITRE, n.d.).
Root Cause	This vulnerability is present in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 (MITRE, n.d.).
Proof of Concept	“A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests,” (Microsoft, n.d.).
Impact	“An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server,” (Microsoft, n.d.).
Likelihood	According to Microsoft, the attack complexity of this vulnerability is high, but no privileges or user interaction are required. The impact is high on confidentiality, integrity, and availability.
Mitigation	According to Microsoft, a complete vendor solution is available – the vendor has issued an official patch or upgrade.
References	*MITRE. (n.d.). CVE-2017-0148. CVE. Retrieved December 11, 2022, from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0148* *Microsoft. (n.d.). Windows SMB Remote Code Execution Vulnerability. Retrieved December 11, 2022 from https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0148*

Supporting Documentation

Methodology

This penetration tests follows the **Penetration Testing Execution Standard (PTES)**.

This methodology includes 7 phases:



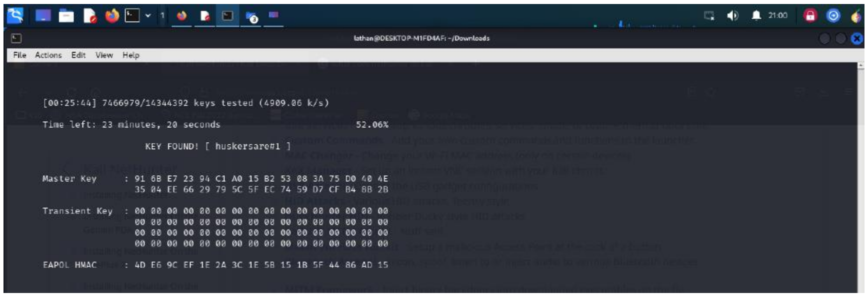
1. Pre-engagement Interactions
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting

Appendix

Details from Penetration Test

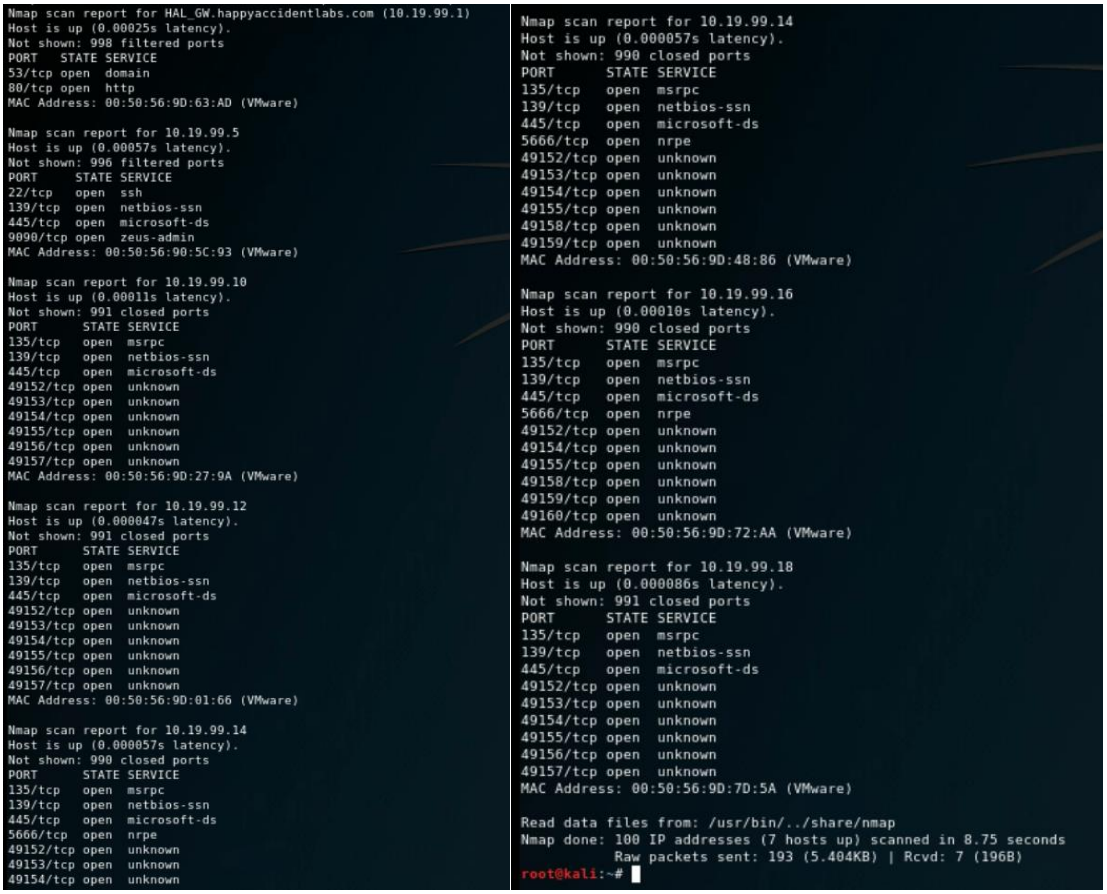
It appears that you are not auditing access to the file system, registry, file shares, changes in process termination and creation, or directory service access. If you were collecting logs on these and checking the security logs, HAL likely would have indicated my presence.

I have accessed the system's network after cracking the wireless password from a WPA handshake.


lathan@DESKTOP-M1FD4AF: ~/Downloads
File Actions Edit View Help

```
[00:25:44] 7466979/14344392 keys tested (4909.06 k/s)

Time left: 23 minutes, 20 seconds                     52.06%

                  KEY FOUND! [ huskersare#1 ]


Master Key     : 91 6B E7 23 94 C1 A0 15 B2 53 08 3A 75 D0 40 4E
                 35 04 EE 66 29 79 5C 5F EC 74 59 D7 CF B4 8B 2B

Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 4D E6 9C EF 1E 2A 3C 1E 5B 15 1B 5F 44 86 AD 15
```

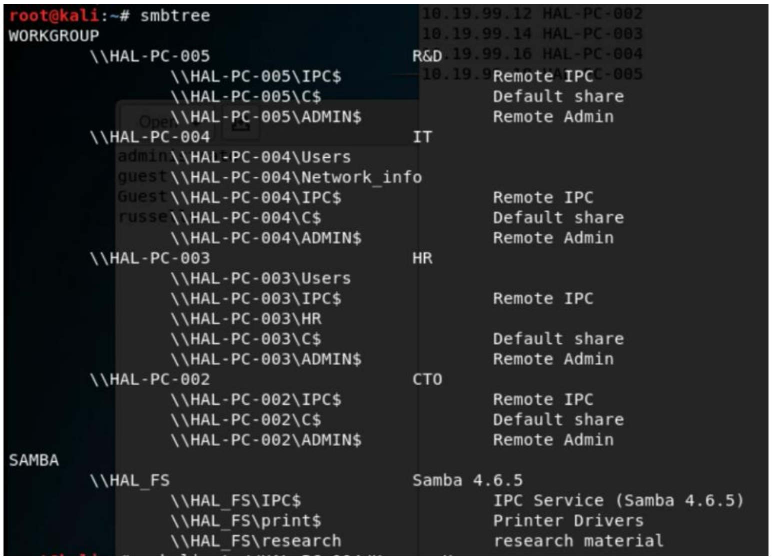
I conducted a full open scan on the network which identified 7 hosts along with their open ports.



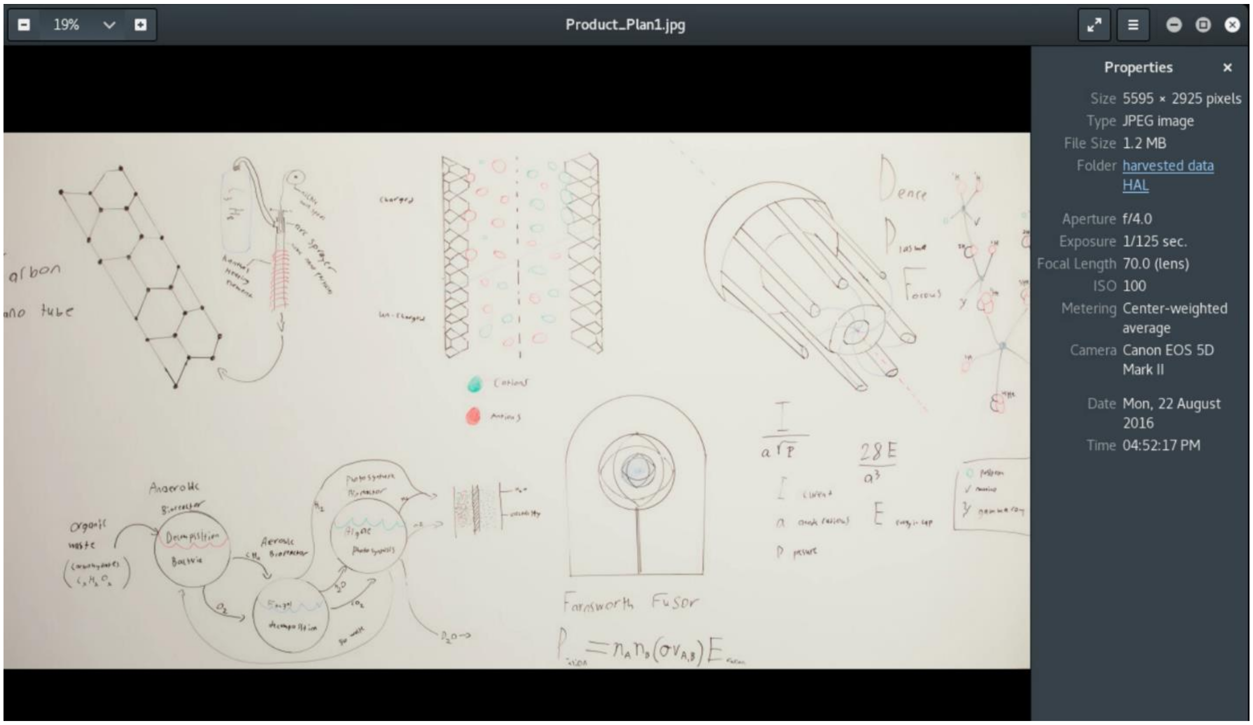
```
Nmap scan report for HAL_GW.happyaccidentlabs.com (10.19.99.1)
Host is up (0.00025s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 00:50:56:9D:63:AD (VMware)

Nmap scan report for 10.19.99.5
Host is up (0.00057s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
9090/tcp open  zeus-admin
MAC Address: 00:50:56:90:5C:93 (VMware)

Nmap scan report for 10.19.99.10
Host is up (0.00011s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:50:56:9D:27:9A (VMware)

Nmap scan report for 10.19.99.12
Host is up (0.000047s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:50:56:9D:01:66 (VMware)

Nmap scan report for 10.19.99.14
Host is up (0.000057s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5666/tcp  open  nrpe
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
```

```
Nmap scan report for 10.19.99.14
Host is up (0.000057s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5666/tcp  open  nrpe
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
MAC Address: 00:50:56:9D:48:86 (VMware)

Nmap scan report for 10.19.99.16
Host is up (0.00010s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5666/tcp  open  nrpe
49152/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown
MAC Address: 00:50:56:9D:72:AA (VMware)

Nmap scan report for 10.19.99.18
Host is up (0.000086s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:50:56:9D:7D:5A (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 100 IP addresses (7 hosts up) scanned in 8.75 seconds
           Raw packets sent: 193 (5.404KB) | Rcvd: 7 (196B)
root@kali:~# 
```

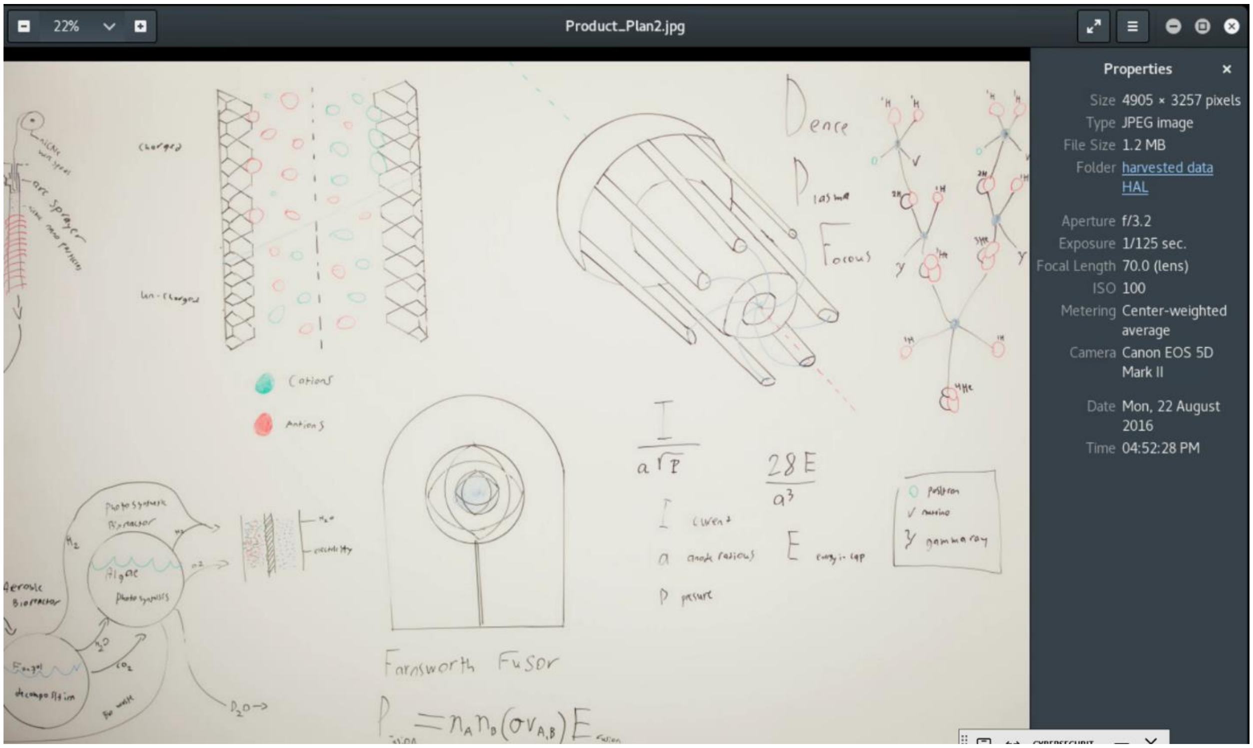
I then used tools such as OpenVAS and Greenborne Security Assistant to identify several vulnerabilities and exploit MS17-010 (also known as CVE-2017-0143) using Metasploit. I accessed the shared drives through host 10.19.99.10 and downloaded sensitive files from the IT, HR, and HAL_FS systems.



```
root@kali:~# smbtree
WORKGROUP
        \\HAL-PC-005                     R&D
                \\HAL-PC-005\IPC$                Remote IPC
                \\HAL-PC-005\C$                  Default share
                \\HAL-PC-005\ADMIN$              Remote Admin
        \\HAL-PC-004                     IT
                \\HAL-PC-004\Users
                \\HAL-PC-004\Network_info
                \\HAL-PC-004\IPC$                Remote IPC
                \\HAL-PC-004\C$                  Default share
                \\HAL-PC-004\ADMIN$              Remote Admin
        \\HAL-PC-003                     HR
                \\HAL-PC-003\Users
                \\HAL-PC-003\IPC$                Remote IPC
                \\HAL-PC-003\HR
                \\HAL-PC-003\C$                  Default share
                \\HAL-PC-003\ADMIN$              Remote Admin
        \\HAL-PC-002                     CTO
                \\HAL-PC-002\IPC$                Remote IPC
                \\HAL-PC-002\C$                  Default share
                \\HAL-PC-002\ADMIN$              Remote Admin
SAMBA
        \\HAL_FS                         Samba 4.6.5
                \\HAL_FS\IPC$                    IPC Service (Samba 4.6.5)
                \\HAL_FS\print$                  Printer Drivers
                \\HAL_FS\research                research material
```

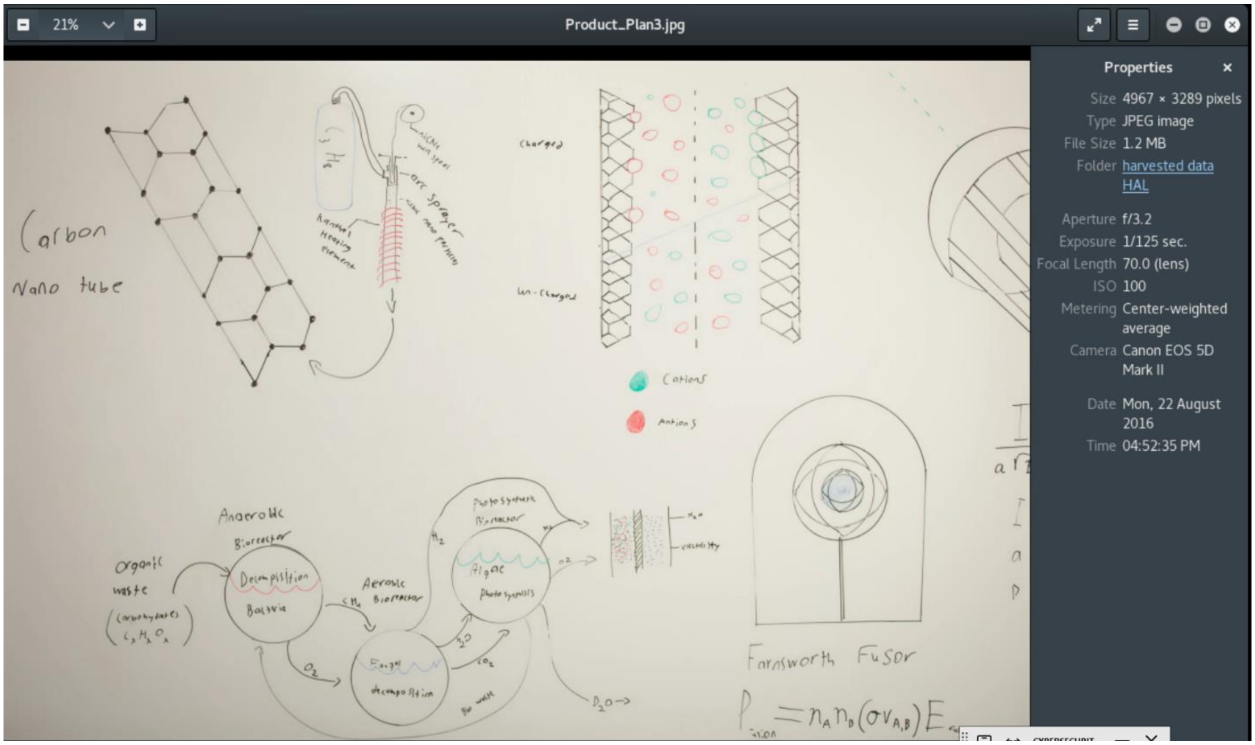


Size 5595 × 2925 pixels
Type JPEG image
File Size 1.2 MB
Folder harvested data HAL
Aperture f/4.0
Exposure 1/125 sec.
Focal Length 70.0 (lens)
ISO 100
Metering Center-weighted average
Camera Canon EOS 5D Mark II
Date Mon, 22 August 2016
Time 04:52:17 PM



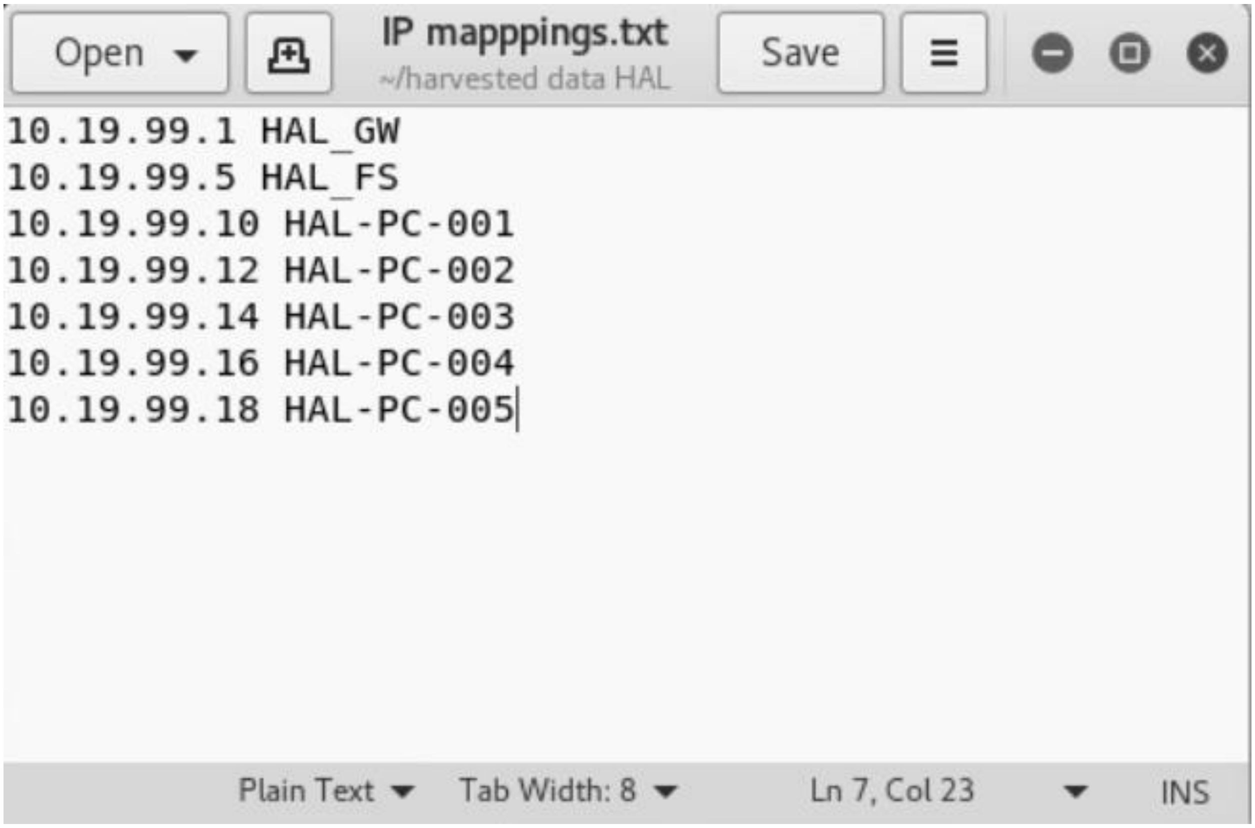
Properties

Size	4905 × 3257 pixels
Type	JPEG image
File Size	1.2 MB
Folder	harvested data HAL
Aperture	f/3.2
Exposure	1/125 sec.
Focal Length	70.0 (lens)
ISO	100
Metering	Center-weighted average
Camera	Canon EOS 5D Mark II
Date	Mon, 22 August 2016
Time	04:52:28 PM

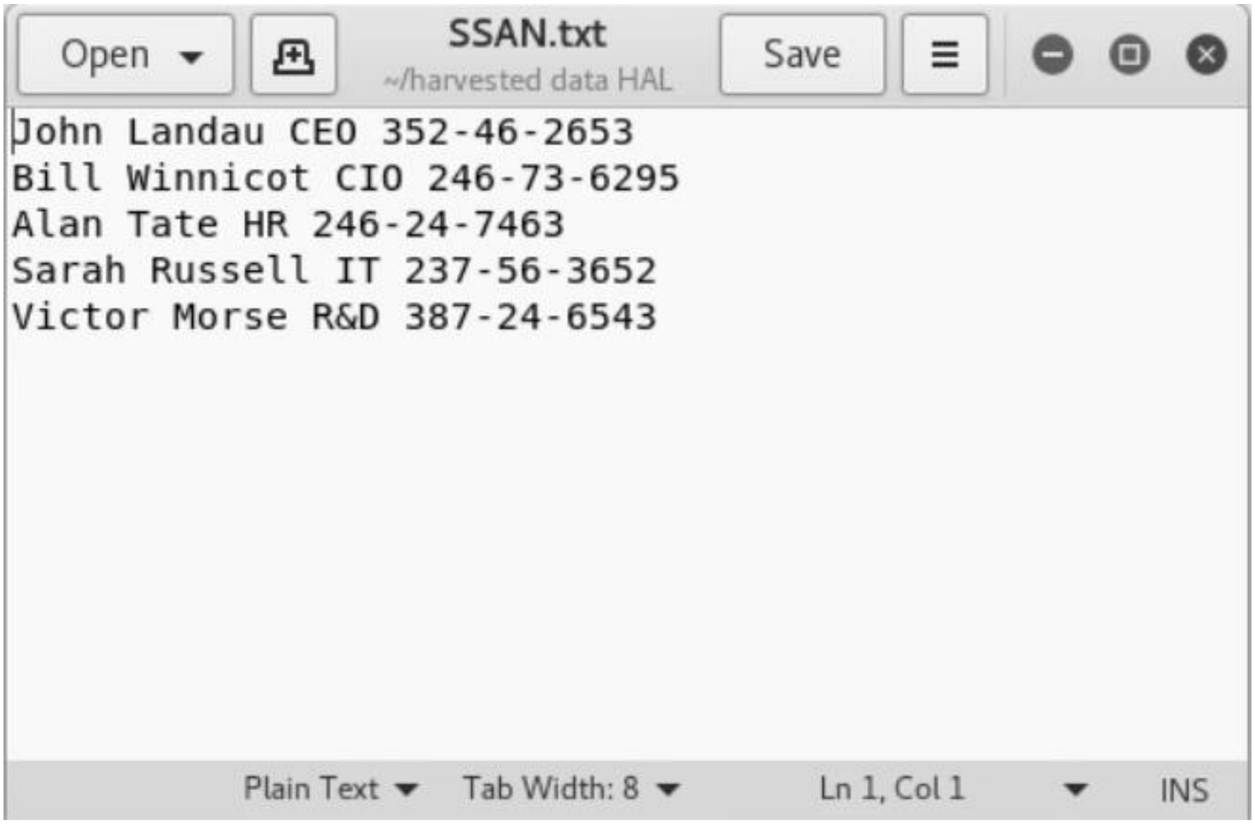


Properties

Size	4967 × 3289 pixels
Type	JPEG image
File Size	1.2 MB
Folder	harvested data HAL
Aperture	f/3.2
Exposure	1/125 sec.
Focal Length	70.0 (lens)
ISO	100
Metering	Center-weighted average
Camera	Canon EOS 5D Mark II
Date	Mon, 22 August 2016
Time	04:52:35 PM



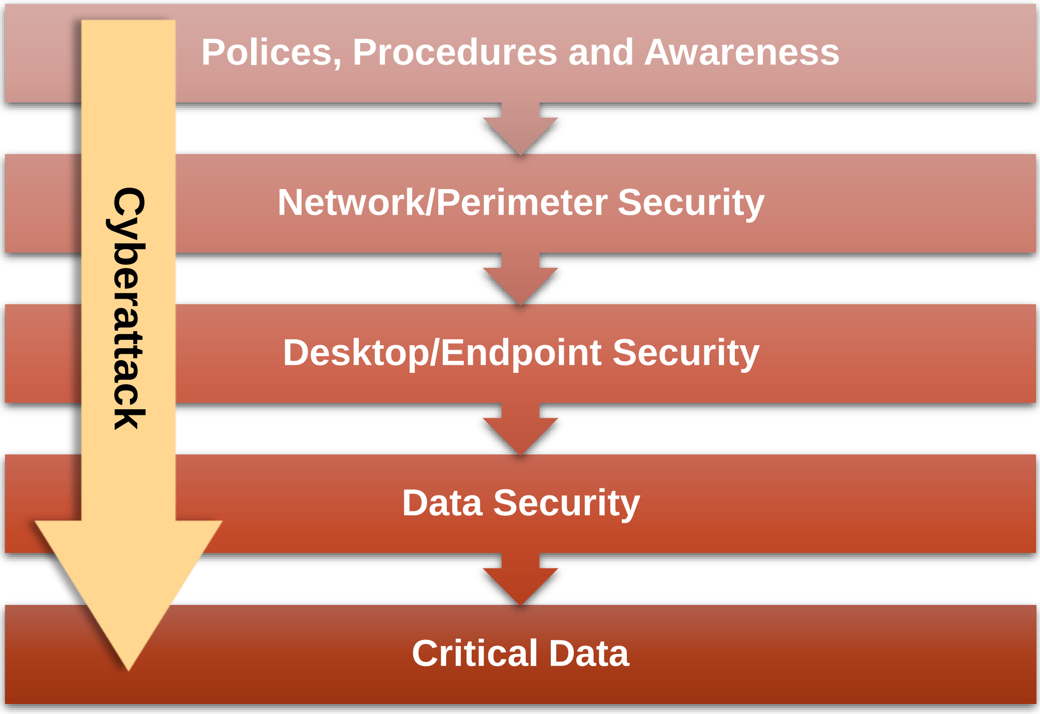
```
10.19.99.1 HAL_GW
10.19.99.5 HAL_FS
10.19.99.10 HAL-PC-001
10.19.99.12 HAL-PC-002
10.19.99.14 HAL-PC-003
10.19.99.16 HAL-PC-004
10.19.99.18 HAL-PC-005
```



```
John Landau CEO 352-46-2653
Bill Winnicot CIO 246-73-6295
Alan Tate HR 246-24-7463
Sarah Russell IT 237-56-3652
Victor Morse R&D 387-24-6543
```

Multi-Layer Defense

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*. By employing defense in depth, a malicious actor must bypass several layers of security precautions to access the critical data. Each layer has several methods and techniques to strengthen the cybersecurity for that layer. The below diagram shows how defense in depth works.


Polices, Procedures and Awareness
Network/Perimeter Security
Desktop/Endpoint Security
Data Security
Critical Data
Cyberattack

Indicating a Network Intrusion

There are several necessary tools that can help indicate signs of a potential breach. These include an IDS, firewalls, an EDR, and/or a SIEM. Happy Accident Labs should utilize a combination of these tools to increase the ability and speed at which they identify a breach.

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.

An **EDR** stands for 'Endpoint Detection & Response'. According to Palo Alto Networks, "Endpoint detection and response refers to a category of tools used to detect and investigate threats on endpoints. EDR tools typically provide detection, investigation, threat hunting, and response capabilities. Endpoint detection and response has become a critical component of any endpoint security solution because there's simply no better way to detect an intrusion than by monitoring the target environment being attacked, and the telemetry collected by an EDR platform enables full triage and investigation," (Palo Alto Networks, n.d.).

SIEM (pronounced 'sim') stands for 'Security Information and Event Management'. 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.

Mitigations to Prevent a Breach

To improve Happy Accident Lab’s security posture, I would recommend implementing a defense-in depth plan such as the following:

Polices, Procedures and Awareness

- Security Awareness Training
- Risk Management
- Threat Modeling
- Separation of Duties
- Mandatory Vacation
- Least Privilege

Network/Perimeter Security

- Multi-Factor Authentication
- VPN Utilization
- Network Access Control
- Wireless Security
- Secure DMZs
- Managed Network Firewalls
- Network-Based IDS/IPS
- Secure Email Gateways
- Honeypots

Desktop/Endpoint Security

- OS Software Updates
- Utilizing Endpoint Detection and Response (EDR)
- Host-Based Firewalls
- Host-Based Intrusion Detection Systems (IDS)
- Access Control
- Secure Passwords

Data Security

- File and Disk Encryption
- File Integrity Monitoring
- Data Classification
- Secure Data Destruction
- Identity and Access Control

References

MITRE. 2019. *CWE-319: Cleartext Transmission of Sensitive Information*. Common Weakness Enumeration. Retrieved December 10, 2022, from https://cwe.mitre.org/data/definitions/319.html

IBM. (1997). *SMB Share Full Access CVE-1999-0519 Vulnerability Report*. IBM X-Force Exchange. Retrieved December 10, 2022, from https://exchange.xforce.ibmcloud.com/vulnerabilities/1

OpenCVE. (2021). *2021-22703*. OpenCVE. Retrieved December 11, 2022, from https://www.opencve.io/cve/CVE-2021-22703

MITRE. (n.d.). *CVE-2017-0148*. CVE. Retrieved December 11, 2022, from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0148

US Signal. (2021, September 21). *Moving Beyond "Blinky Box" Security to Defense-in-Depth*. US Signal. Retrieved December 16, 2022, from https://ussignal.com/blog/moving-beyond-blinky-box-security-to-defense-in-depth-security

Palo Alto Networks. (n.d.). *What is Endpoint Detection and Response (EDR)?* Palo Alto Networks. Retrieved December 17, 2022, from https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-detection-and-response-edr

Microsoft. (n.d.). *What is SIEM?* Microsoft Security. Retrieved December 17, 2022, from https://www.microsoft.com/en-us/security/business/security-101/what-is-siem