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

Sampat Dhakal

Word Count: 2200

Contents

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).

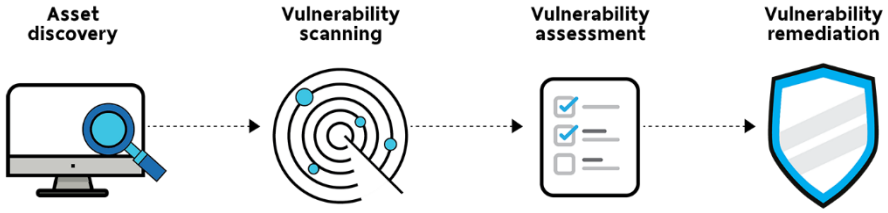


Fig1. Vulnerability Assessment

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.

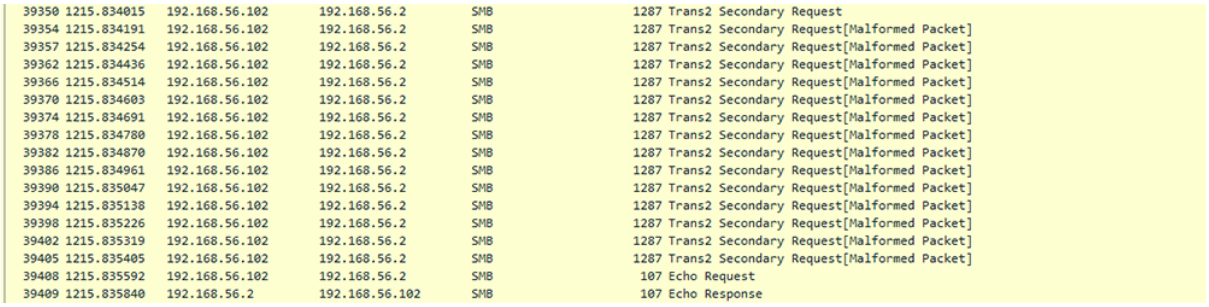
2.2 Exploit and Attack Software

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 TRANSCATION2 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	1215.834780	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.

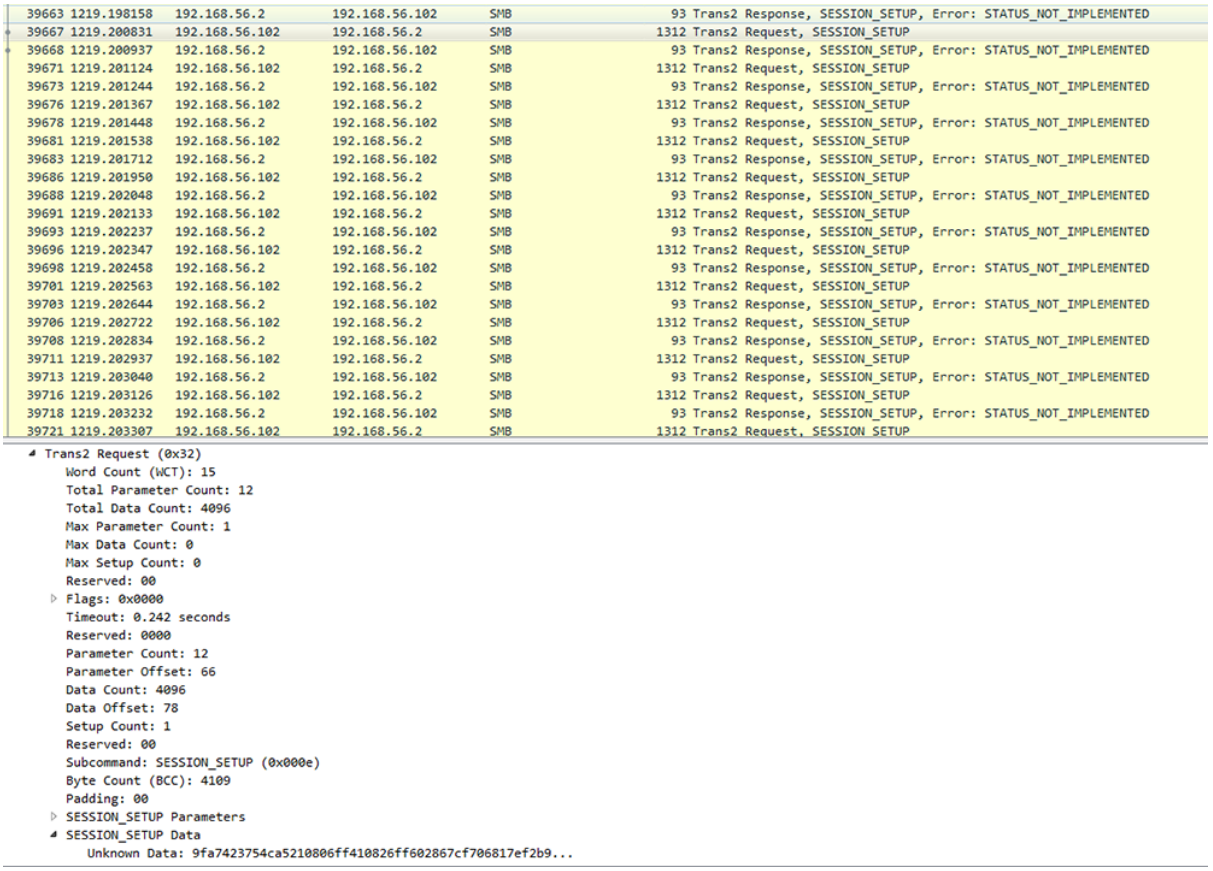


Fig4. Payload Transmissions

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.

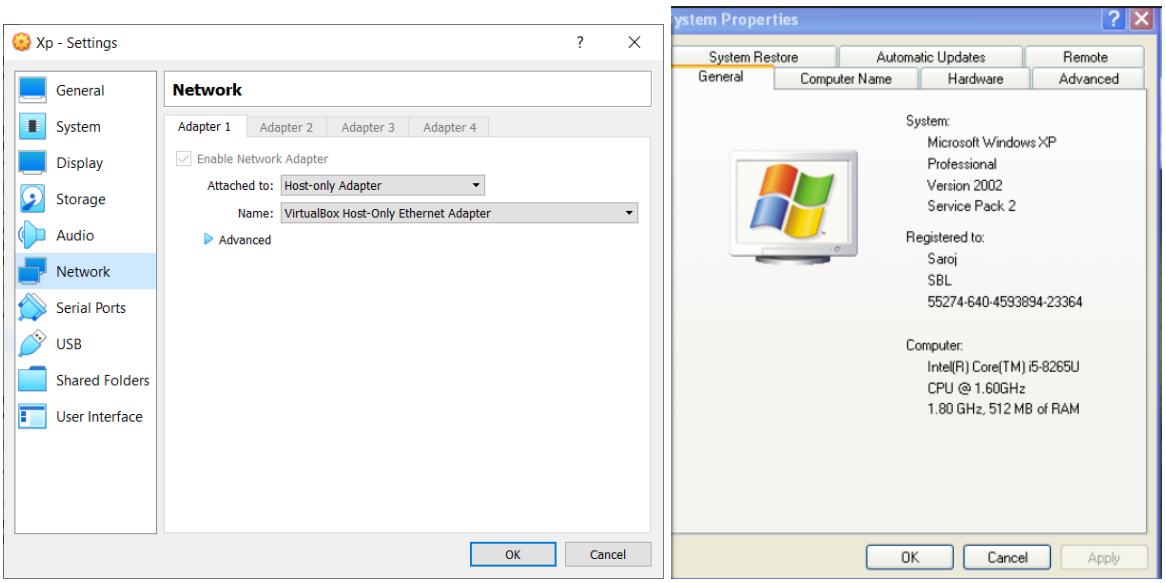


Fig5. Adapter setting and software version

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

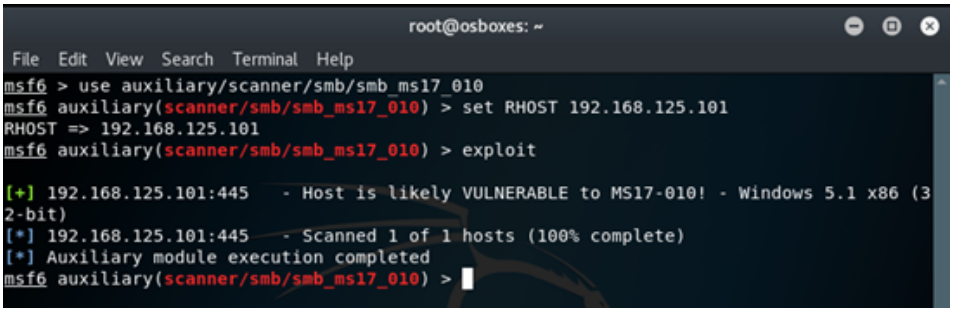


Fig6. Auxiliary Scan

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.

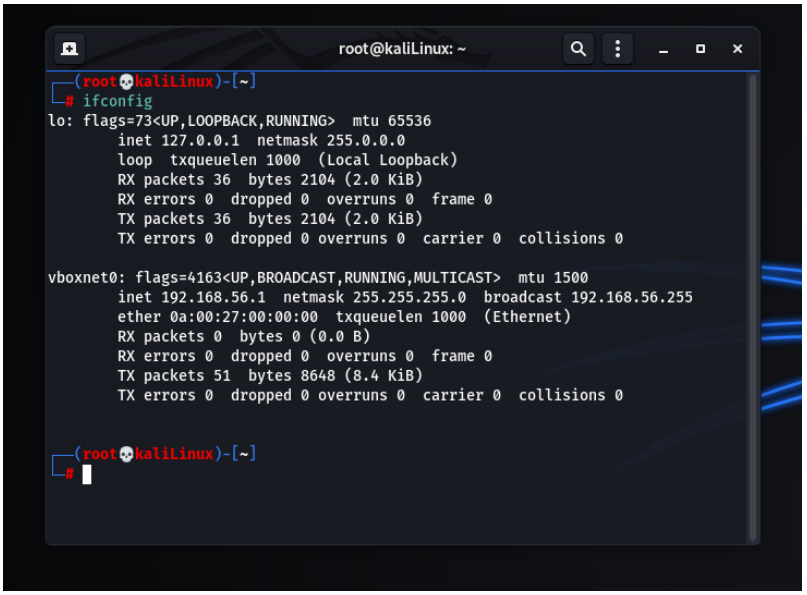


Fig7. Executing ifconfig

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.

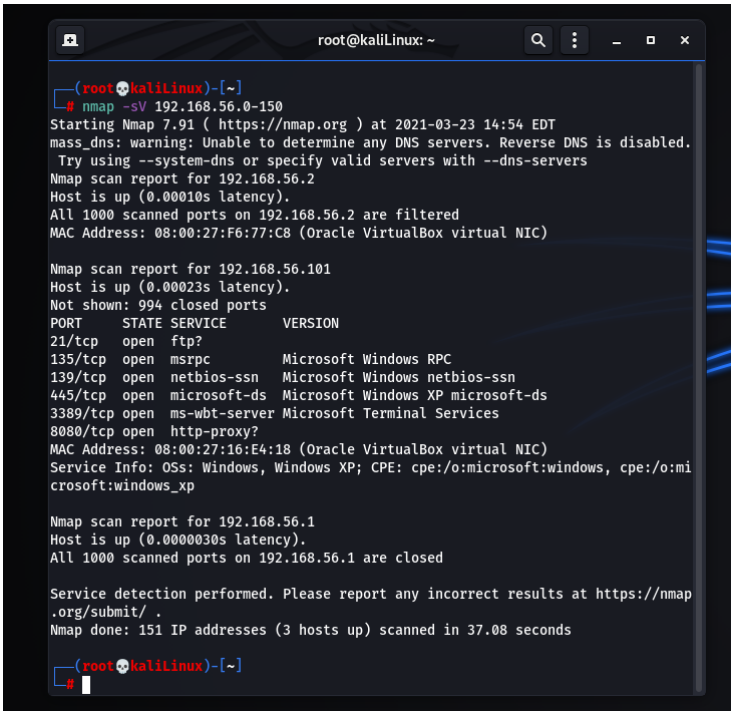


Fig8. Nmap Scan

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.

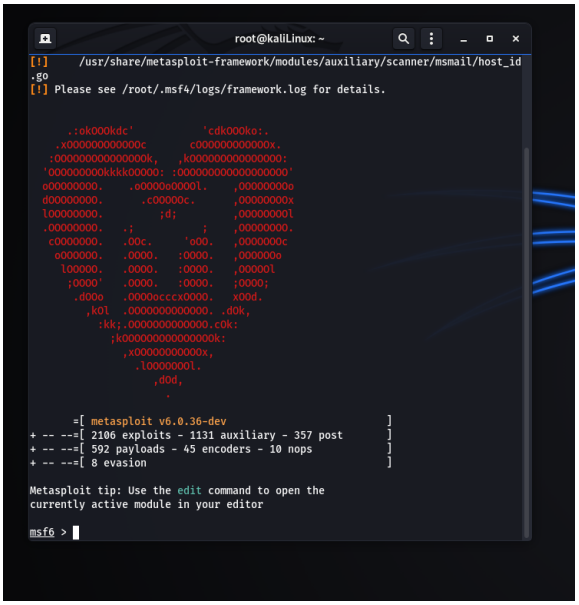


Fig9. MSF Running

Finding modules and payloads

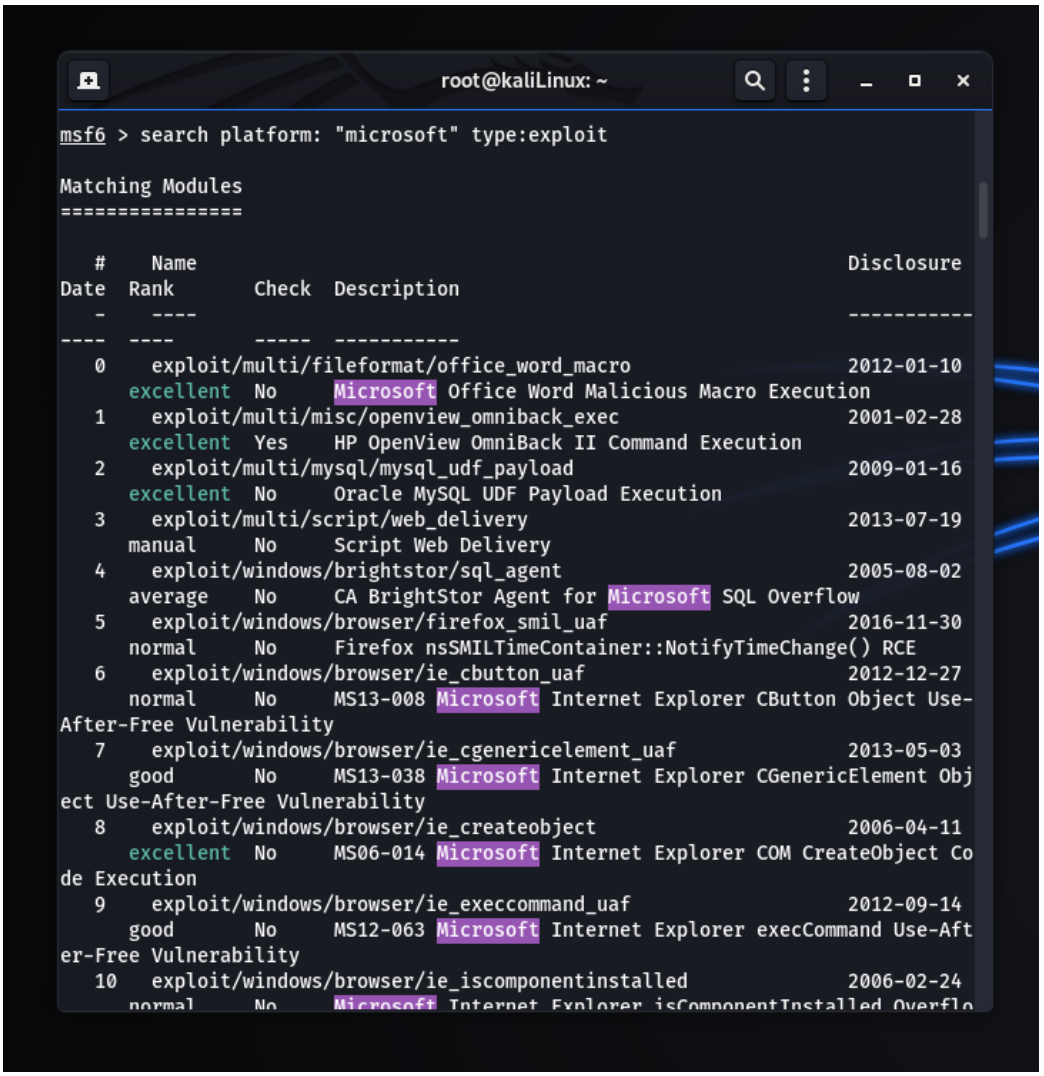


Fig 10. Searching for platform supports and exploits

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.

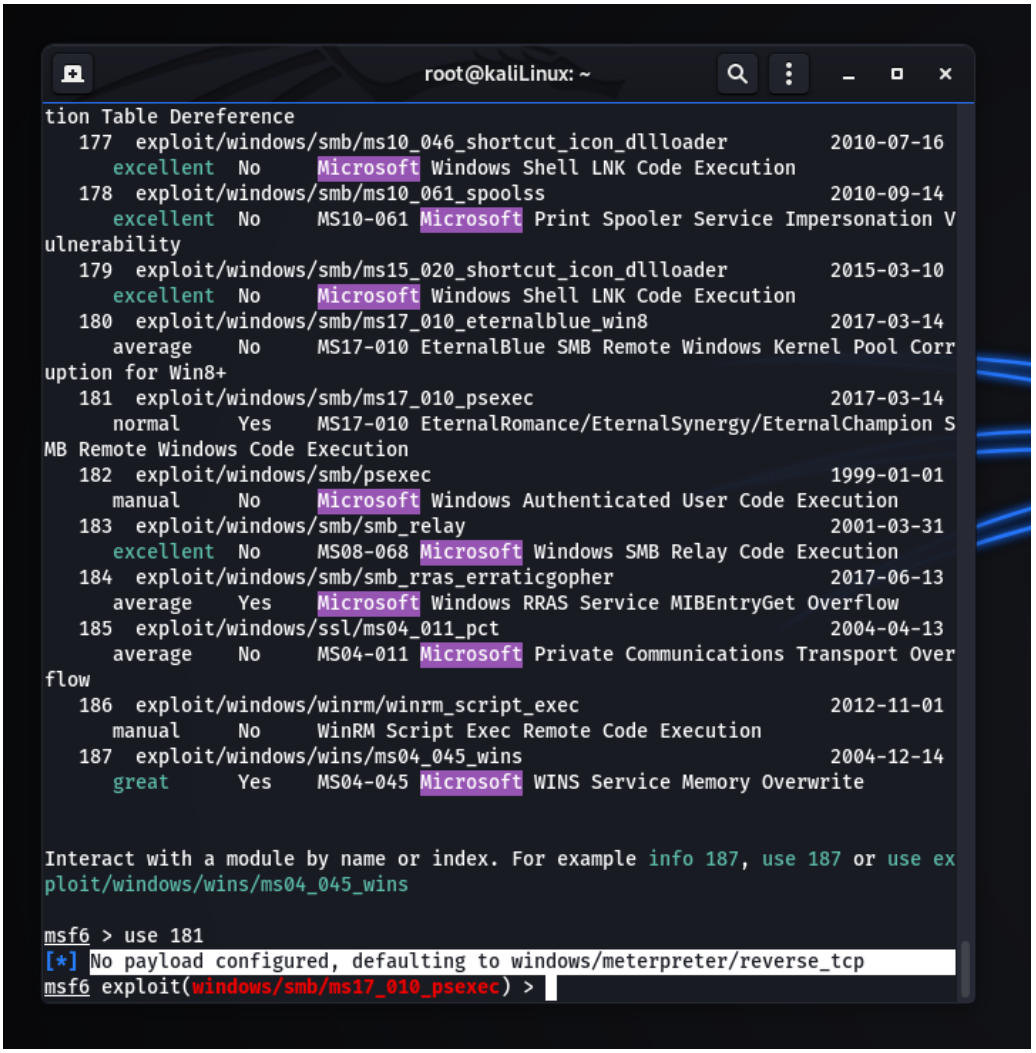


Fig11. Selecting the exploits

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.

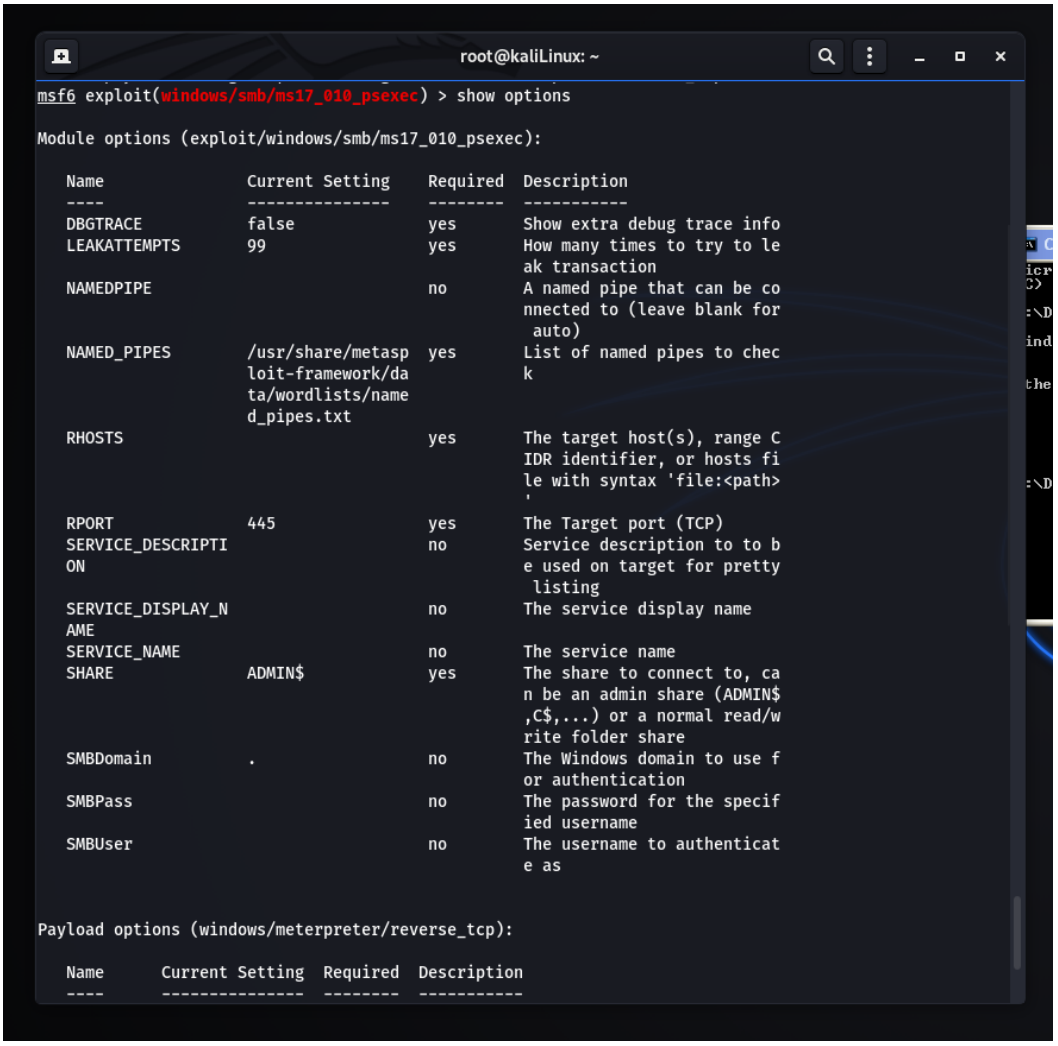


Fig12. Listing Options

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.

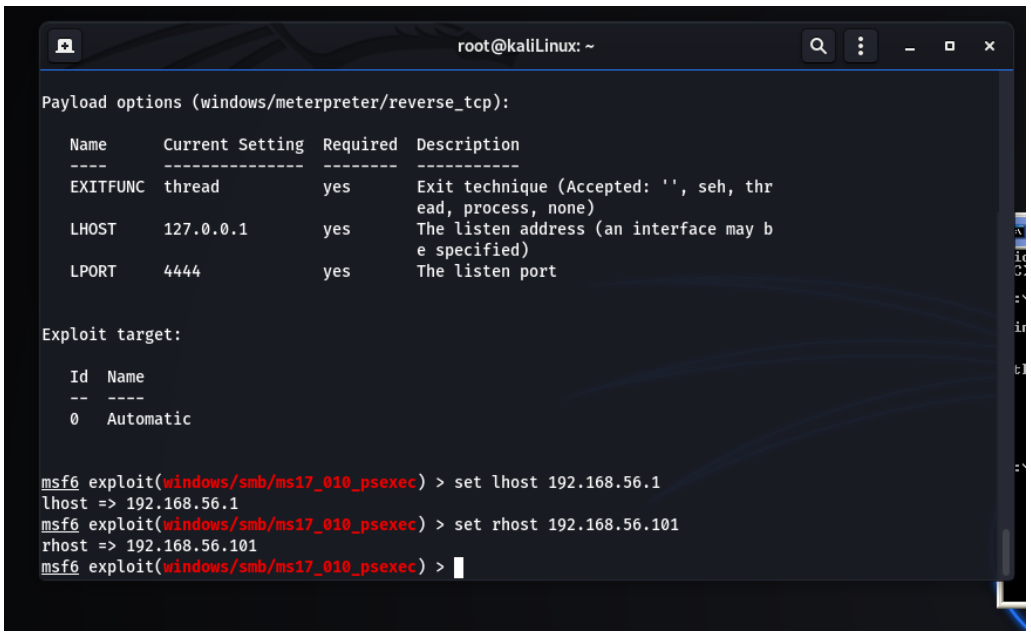


Fig 13. Setting up LHOST and RHOST

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

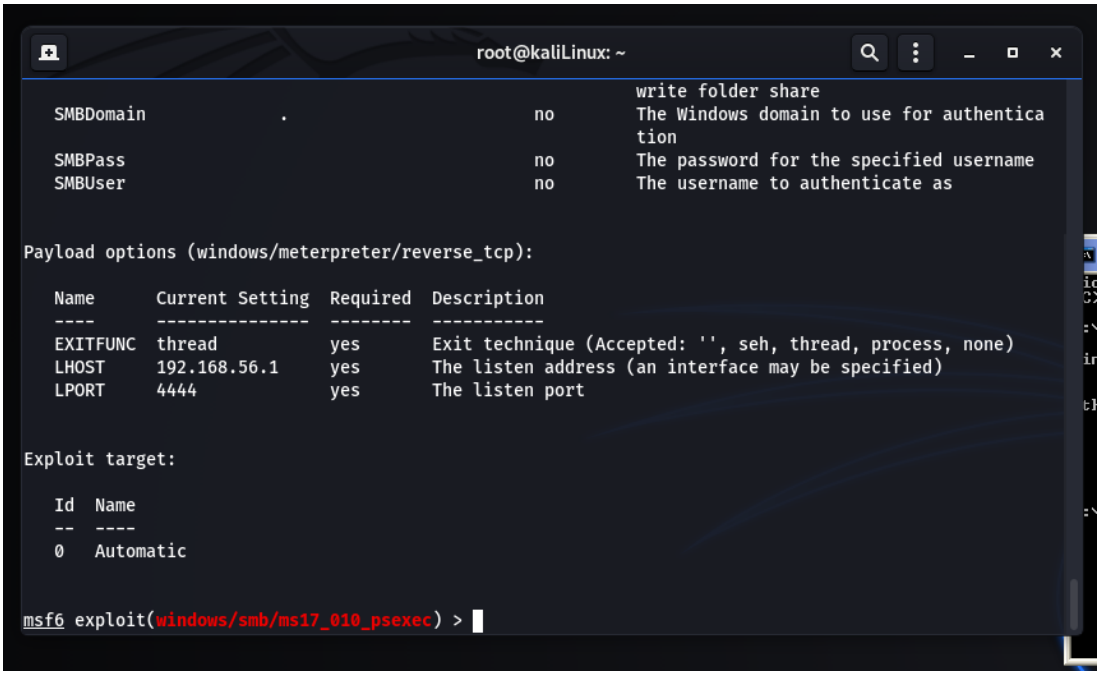


Fig14. Checking entered parameters

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

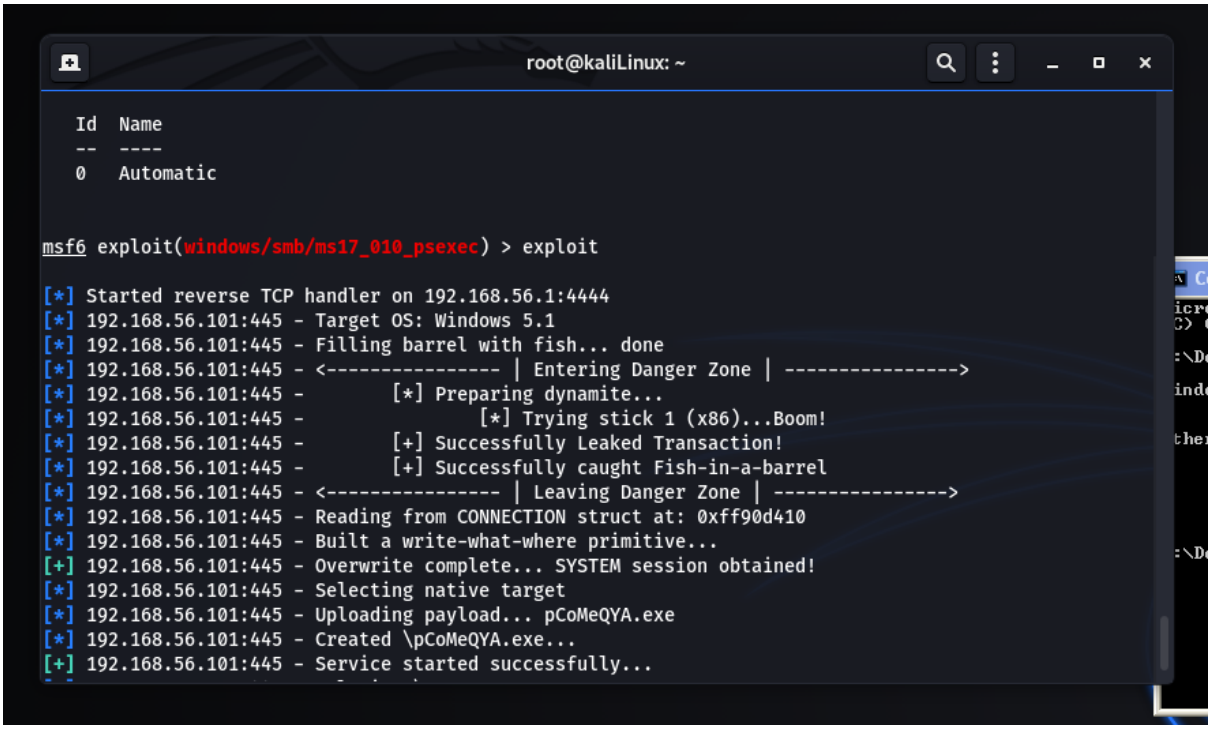


Fig 15. Running Exploit

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

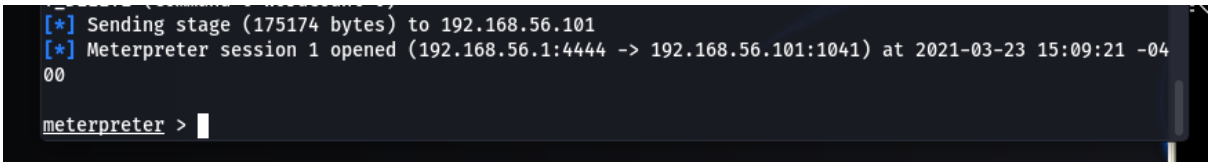


Fig 16. Meterpreter Session

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

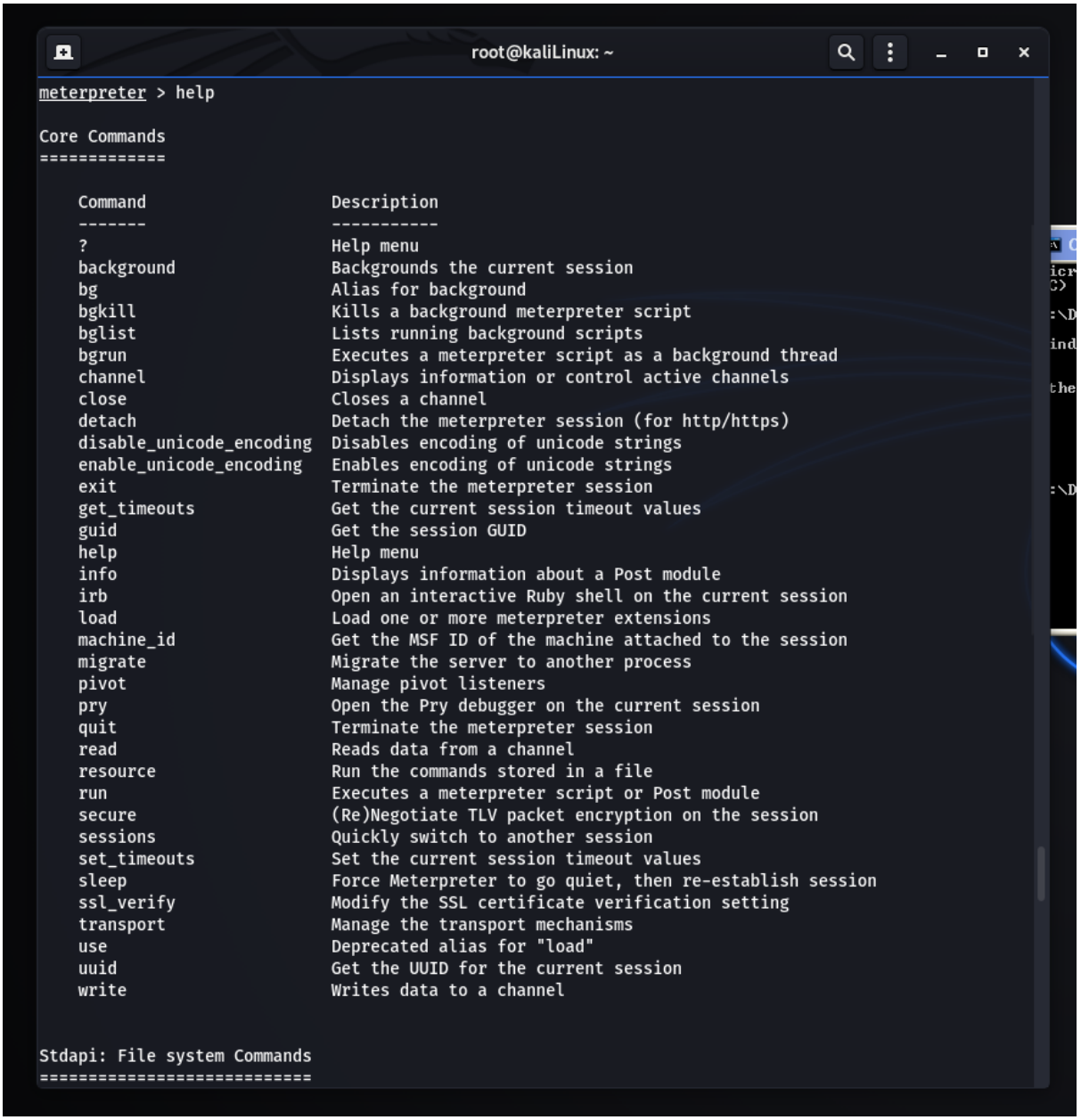


Fig 17. Help command

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

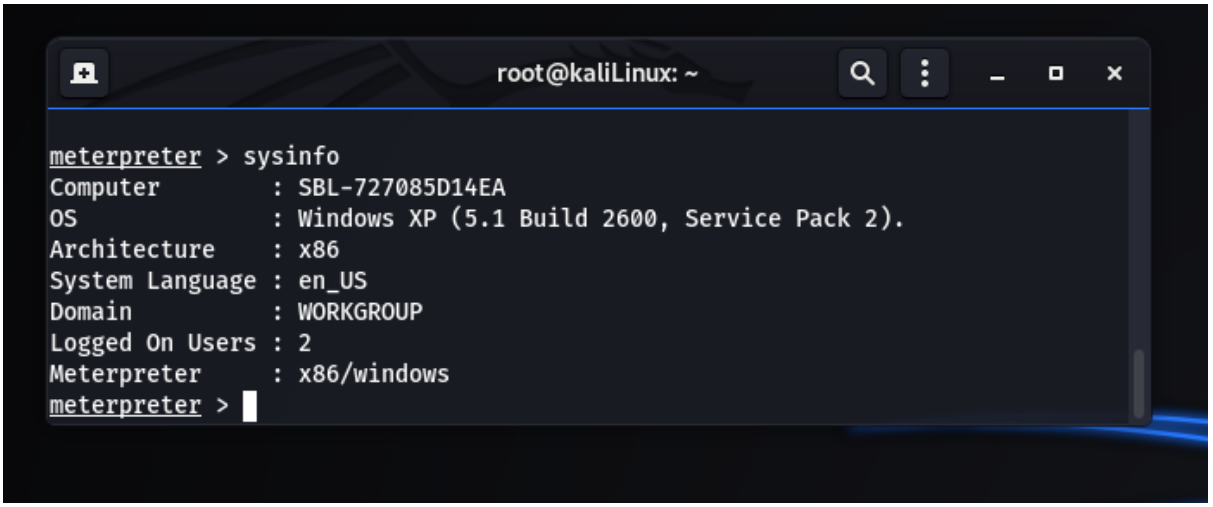


Fig18. Getting system information

And getuid to fetch the running username

```
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.

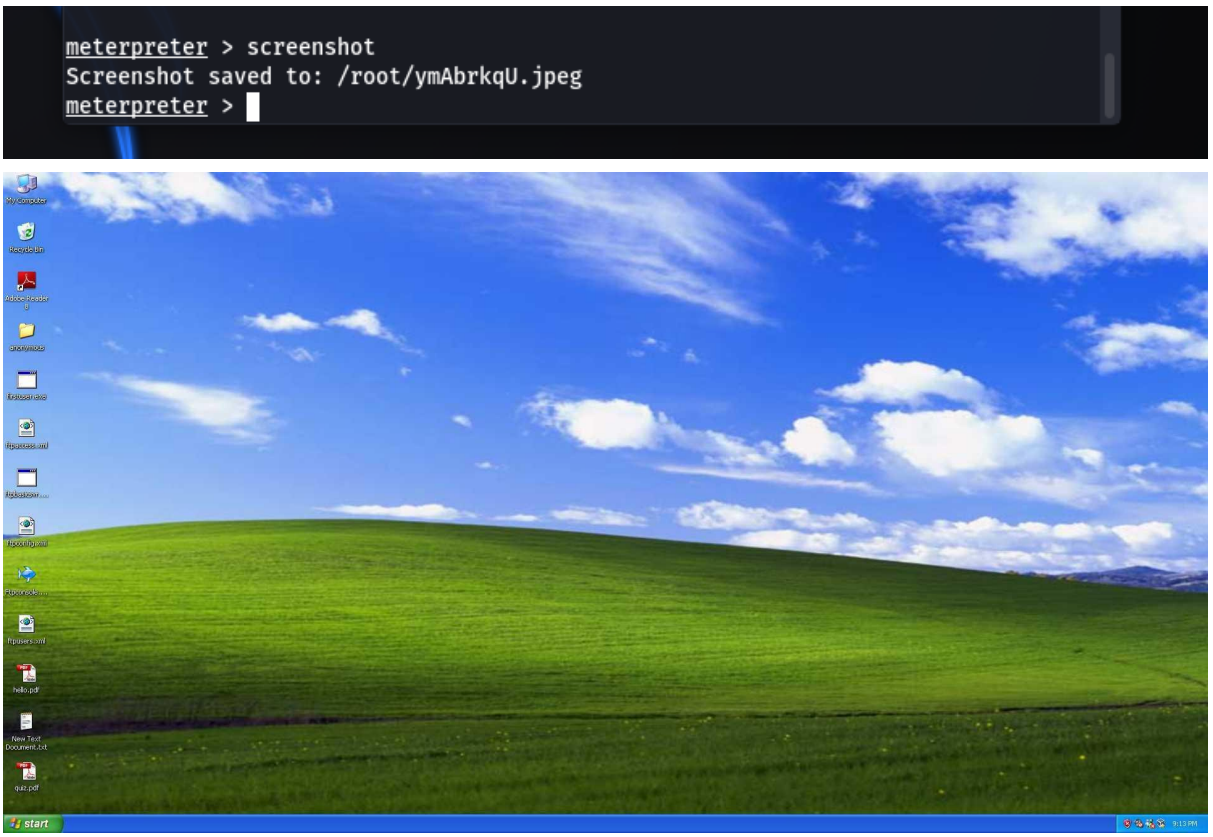


Fig20. Getting screenshot remotely

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.

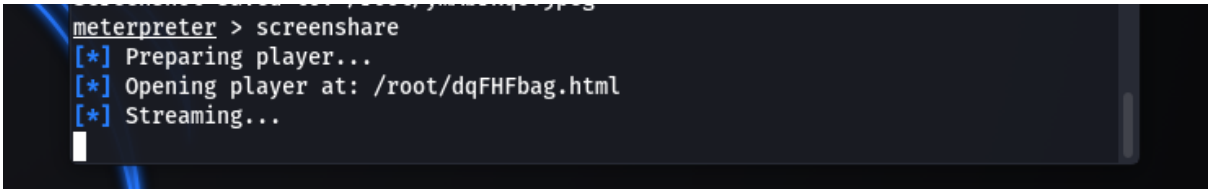


Fig21. Screensharing command execution

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

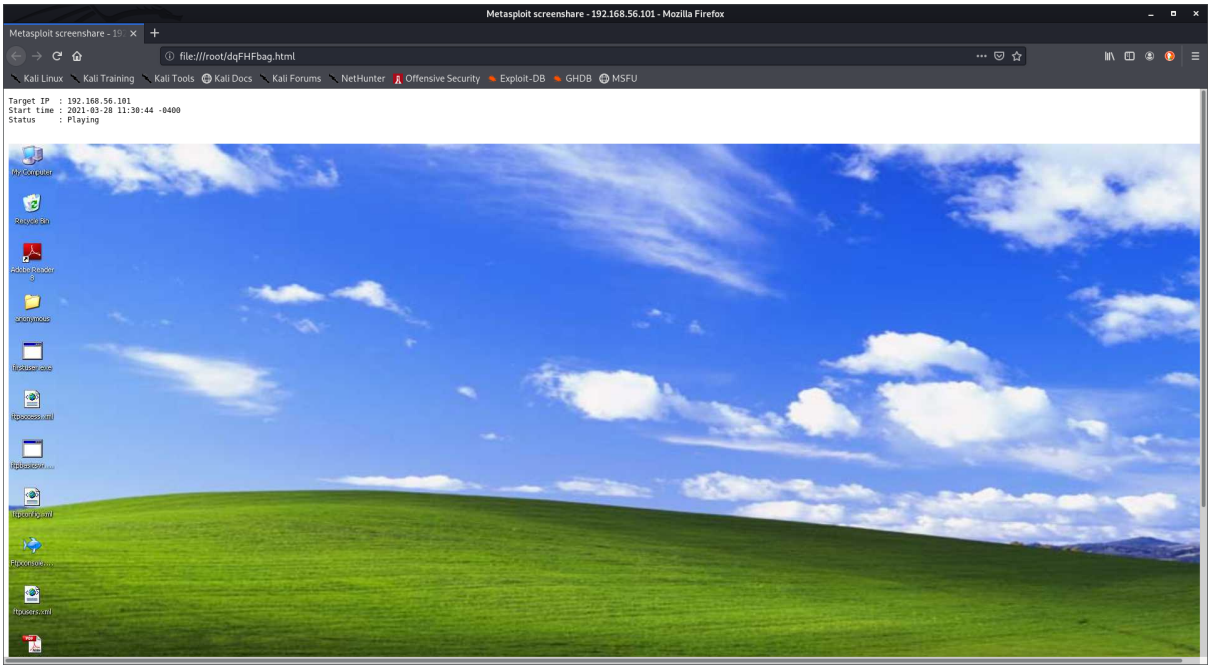


Fig22. Web-based live player

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

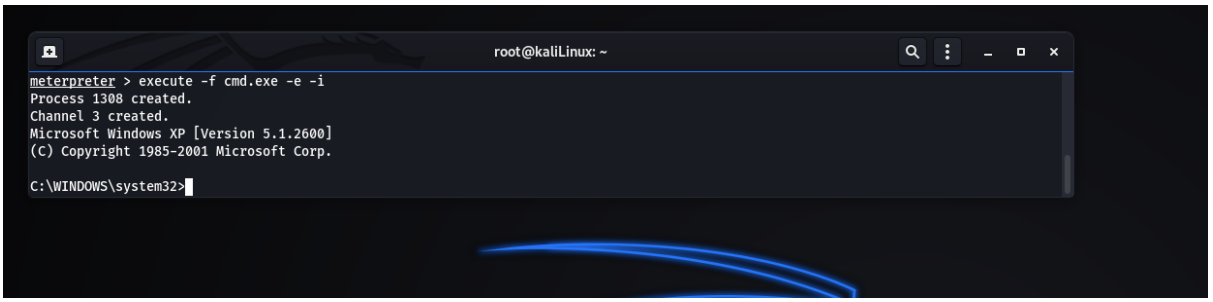


Fig 23. Execution of shell/ command-line

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)

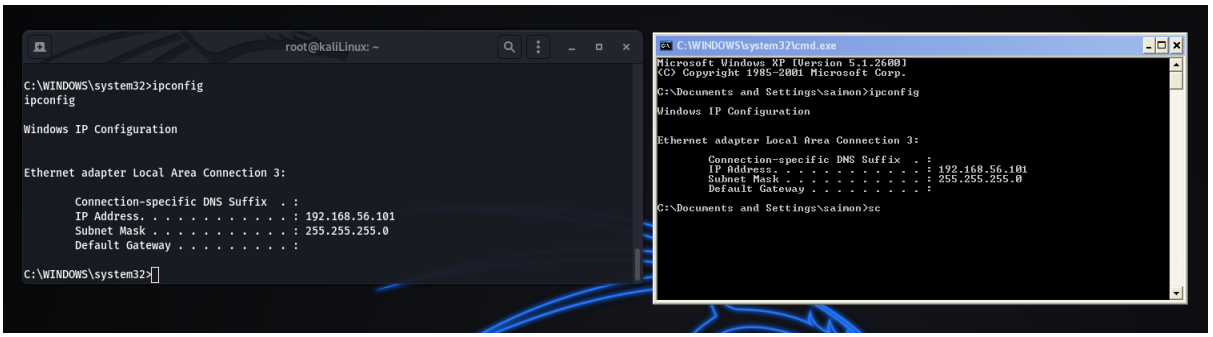


Fig24. Matching of IP's

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

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.

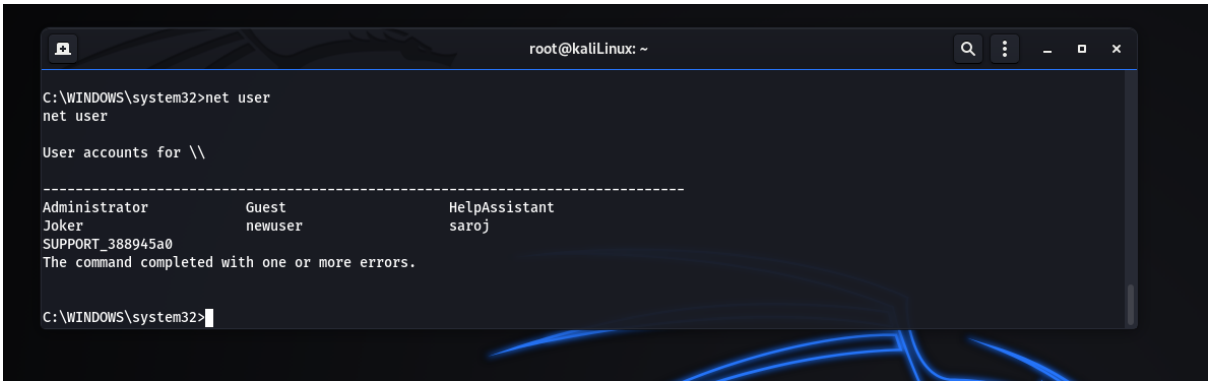


Fig26. Listings of users

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

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).

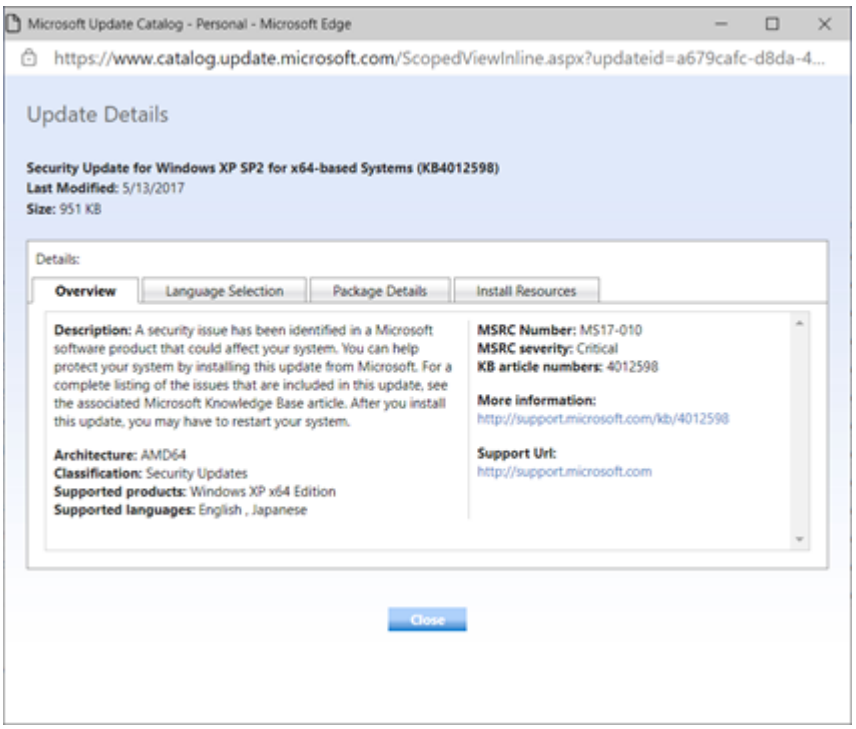


Fig28. Patch available for prevention

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.

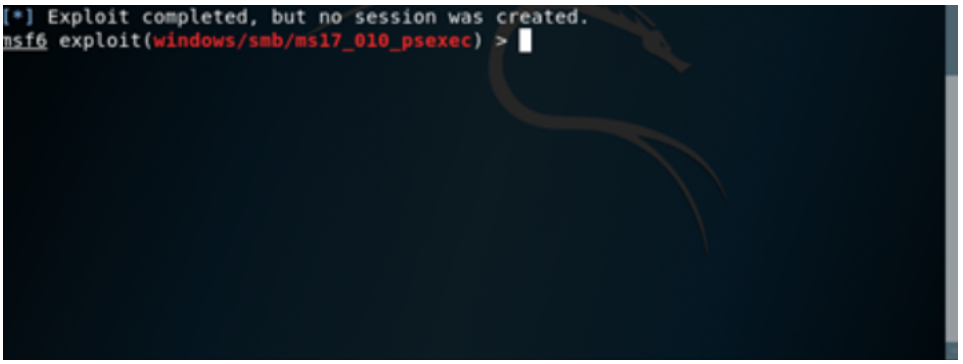


Fig29. Exploitation failed

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.

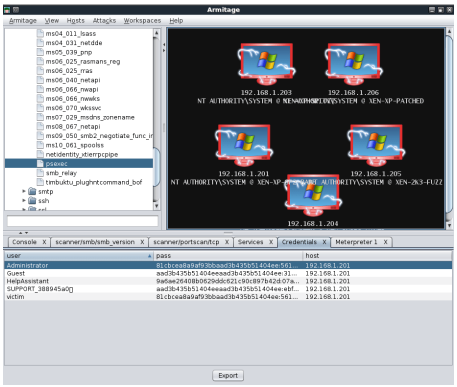


Fig 30. Tools available

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].