Sri Lanka Institute of Information Technology

Individual Assignment

System Networking and Programming

CVE-2019-0708

Remote Desktop Services Remote Code Execution Vulnerability

Blue Keep DOS

IT19010236

Balendrarajah Kajanthan

Table of Content

ABSTRACT

This is about Blue Keep vulnerability exploit which perform a denial os service attack on the target machine. The National Security Agency alerts users that recent Windows 7 vulnerabilities can be "wormable" so that they can be abused and protected by malware. A vulnerability, CVE-2019-0708, that can affect Windows 7 was released by Microsoft in the middle of May.

It didn't seem to happen much for some months. However, an attack was recently seen in the wild which tried to install cryptomining software on non-patched RDP servers and exposed the Internet to port 3389.

In later versions such as windows 8, windows 10, this vulnerability is fixed. And the development of security patches. For more up-to-date version. This article includes all the facts and information about the weakness and assault as well as the use of a python package Codes which available in github and Exploit DB.

INTRODUCTION

I’m Balendrarajah Kajanthan doing cyber security specialization at SLIIT. For SNP module we need to exploit vulnerable Operating System. So I took windows 7 to exploit. I run windows 7 on VM ware as virtual machine. I took CVE-2019-0708 Remote Desktop Services Remote Code Execution Vulnerability called as Blue Keep Dos. A weakness in remote-execution coding occurs when an unauthenticated intruder logs to a target device using RDP and sends explicitly created requests in Remote Desktop Services formerly known as Terminal Services. It is a pre-authentication weakness and does not require user interaction. An attacker who successfully exploited this vulnerability could use the target program to execute arbitrary code. An intruder can then install programs; view, modify or remove data; or build new user permission accounts.

An intruder could send a specially designed request to the Remote Desktop Service target systems using RDP to exploit this vulnerability. Blue Keep (CVE-2019-0708) is a security vulnerability that affecting Microsoft Windows' older versions. This vulnerability includes all 32 or 64-bit and all versions of Service Pack that exist in the following Microsoft Windows Operating Systems (OSs), such as

Windows 2000

Windows Vista

Windows XP

Windows 7

Windows Server 2003

Windows Server 2003 R2

Windows Server 2008

Windows Server 2008 R2

Within the Microsoft Windows OSs mentioned above, Blue Keep exists in a remote desktop protocol (RDP). This weakness can be taken advantage of by an attacker to remotely execute code on an insecure device.

History Of Blue Keep.

The UK National Cyber Security Center first noticed. Blue Keep security weakness and Microsoft confirmed it on 14 May 2019. The technology expert from the machine Kevin Beaumont on Twitter called a Blue Keep vulnerability.

Microsoft notes that an attacker can send packets to one of the systems that are specially designed and have RDP enabled. The intruder will be able to perform a variety of activities after packages are submitted successfully: inserting accounts with full user rights, accessing, modifying, or removing information or downloading programs.

This task, without any contact between the user, must take place before authentication succeeds.Blue Keep is called "wormable" due to the fact that malware will spread to other compromised systems using this vulnerability on a system, and a Blue Keep exploit will be able to spread rapidly in a way close to 2017's WannaCry attacks. Cybersecurity and Infrastructure Security Agency worked with external stakeholders and found that Windows 2000 is Blue Keep vulnerable.

what makes the Blue Keep vulnerability so critical?

1. It affects RDP services used by millions of machines worldwide.
2. It allows remote code execution.
3. It can be weaponized to be worm able.

What is a Vulnerability

A vulnerability is a weakness that a threat actor, such as an attacker, may exploit in order to carry out unauthorized activities within a computer system. To exploit a vulnerability, an attacker must have at least one device or technique that can attach to a weakness in the program. Vulnerabilities in this frame are also known as the surface of attack.

What is an Exploit?

Exploitation is the next move after discovering a loophole in an attacker's playbook. Exploits are the means by which hackers can manipulate a vulnerability for malicious activity; these include pieces of software, command sequences, or even open-source exploit kits.

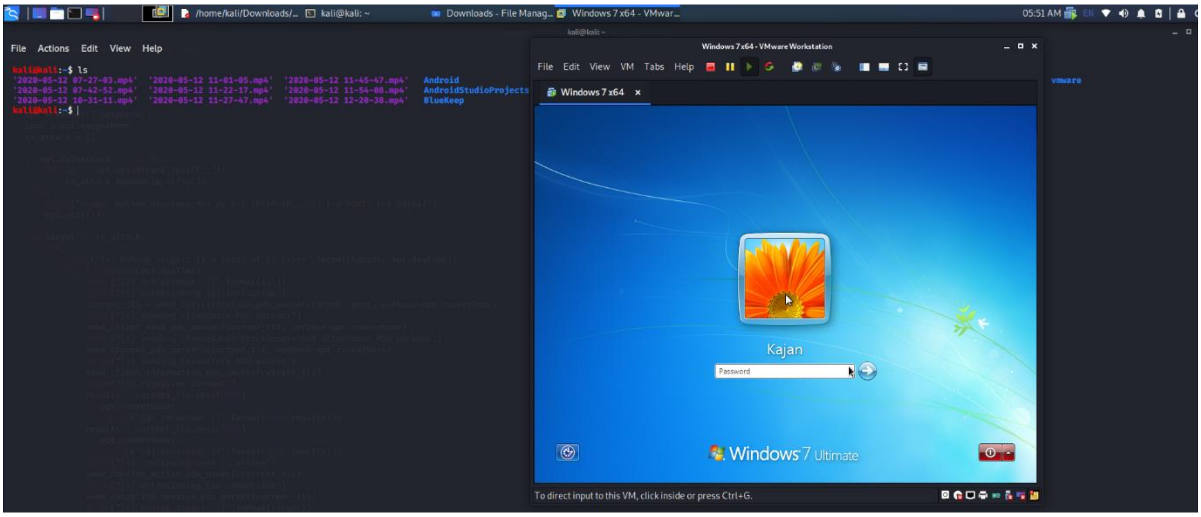
Exploitation Method

Here I Install VM Ware on kali Linux. And I install Windows 7 64 Bit on it. And I remotely exploit codes which I found on exploit DB. There I found Blue Keep Exploit python Codes. Using That Codes we can remotely do a DOS attack on windows Operating system which I mentioned above. But Here I choose

Windows 7x64 bit OS. Here I used You Tube videos and other websites to perform a demo presentation to exploit using Kali 2020. I got some codes from GitHub But its contain lot of errors then I found codes on Exploit DB.

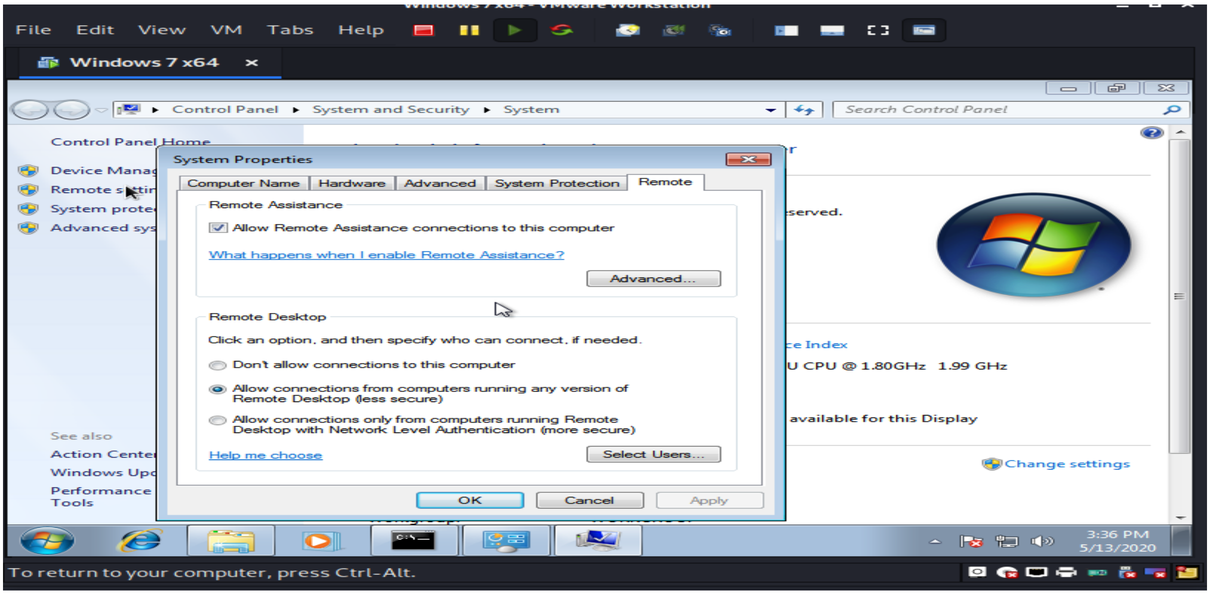
Steps To Do Demo Blue Keep

01 – Start to run Windows 7 on VMware. Log in it and you have to right click >on my computer and go to properties and set as shown in this picture.



```
kali@kali:~$ ls
'2020-05-12 07-27-03.mp4'  '2020-05-12 11-01-05.mp4'  '2020-05-12 11-45-47.mp4'   Android
'2020-05-12 07-42-52.mp4'  '2020-05-12 11-22-17.mp4'  '2020-05-12 11-54-08.mp4'   AndroidStudioProjects
'2020-05-12 10-31-11.mp4'  '2020-05-12 11-27-47.mp4'  '2020-05-12 12-20-38.mp4'   BlueKeep
kali@kali:~$ |
```

/home/kali/Downloads/...
kali@kali: ~
Downloads - File Manag...
Windows 7 x64 - VMwar...
05:51 AM
File
Actions
Edit
View
Help
Windows 7 x64 - VMware Workstation
File Edit View VM Tabs Help
Windows 7 x64
Kajan
Password
Windows 7 Ultimate
To direct input to this VM, click inside or press Ctrl+G.



System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Advanced...

Remote Desktop

Click an option, and then specify who can connect, if needed.

○ Don't allow connections to this computer

● Allow connections from computers running any version of Remote Desktop (less secure)

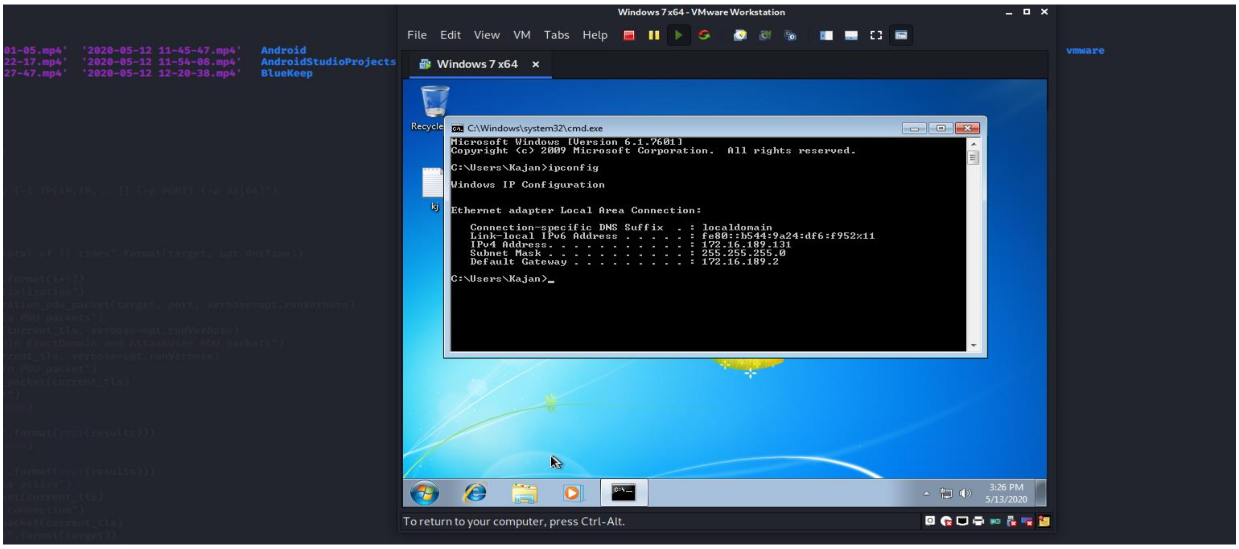
○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Help me choose

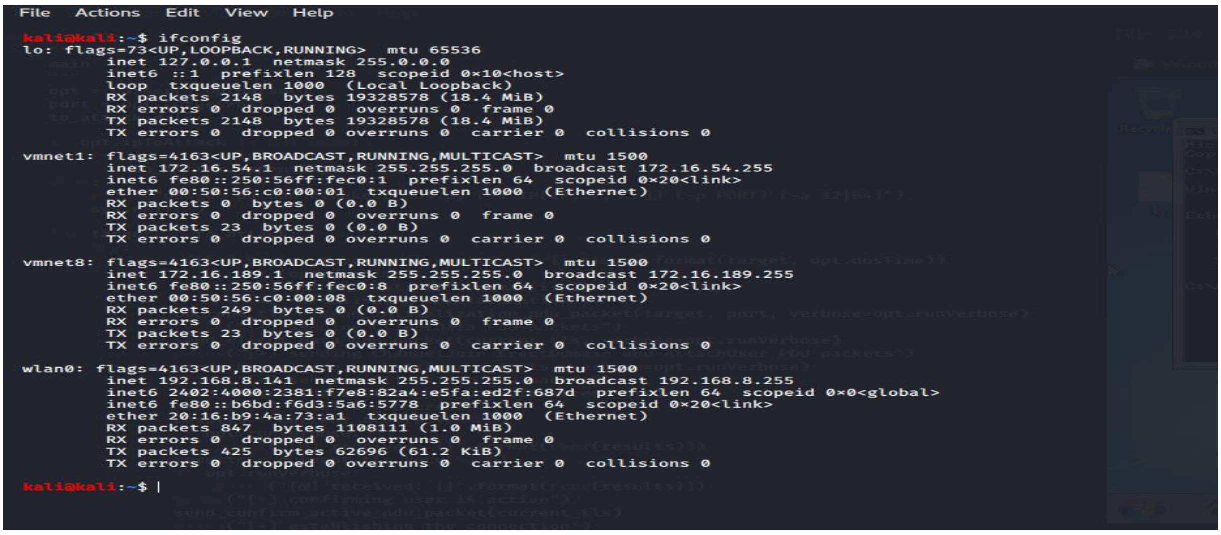
Select Users...

OK Cancel Apply

02 – we need to find both ip address of kali linux and windows 7. In kali using ifconfig command. In windows we need to open cmd then we need to type ipconfig

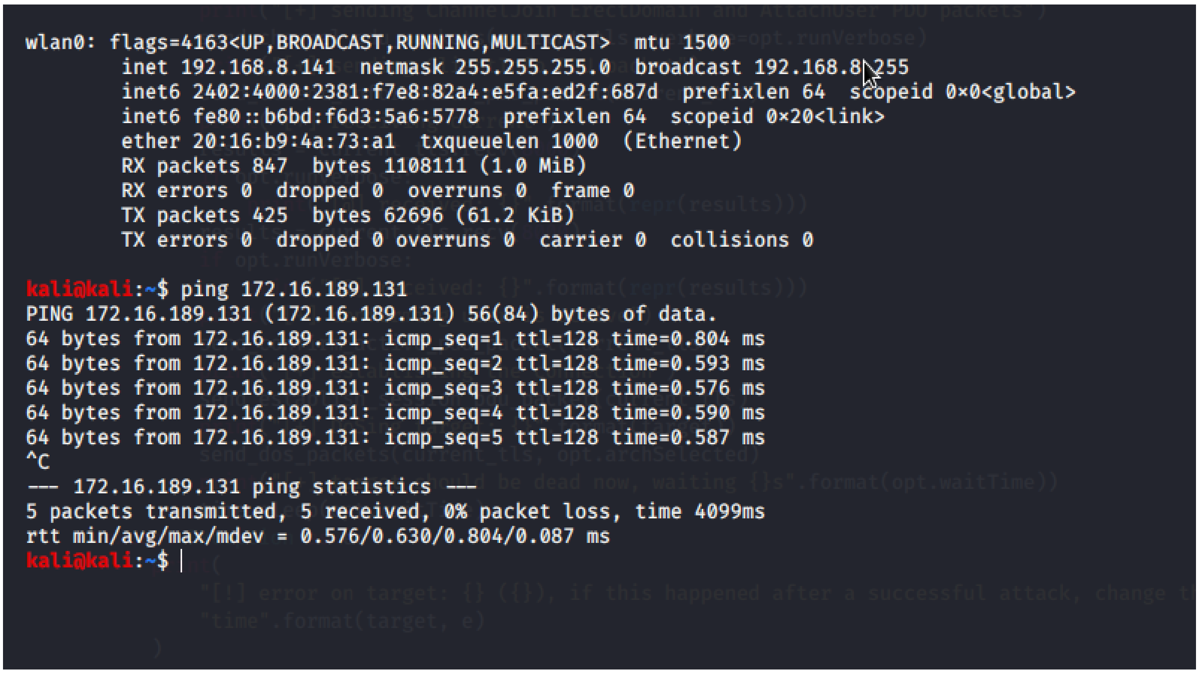

Windows 7 x64 - VMware Workstation
File Edit View VM Tabs Help
Windows 7 x64
Recycle
kj
C:\Windows\system32\cmd.exe
3:26 PM
5/13/2020
To return to your computer, press Ctrl-Alt.

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

C:\Users\Kajan>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::b544:9a24:df6:f952%11
   IPv4 Address. . . . . . . . . . . : 172.16.189.131
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.189.2

C:\Users\Kajan>_
```



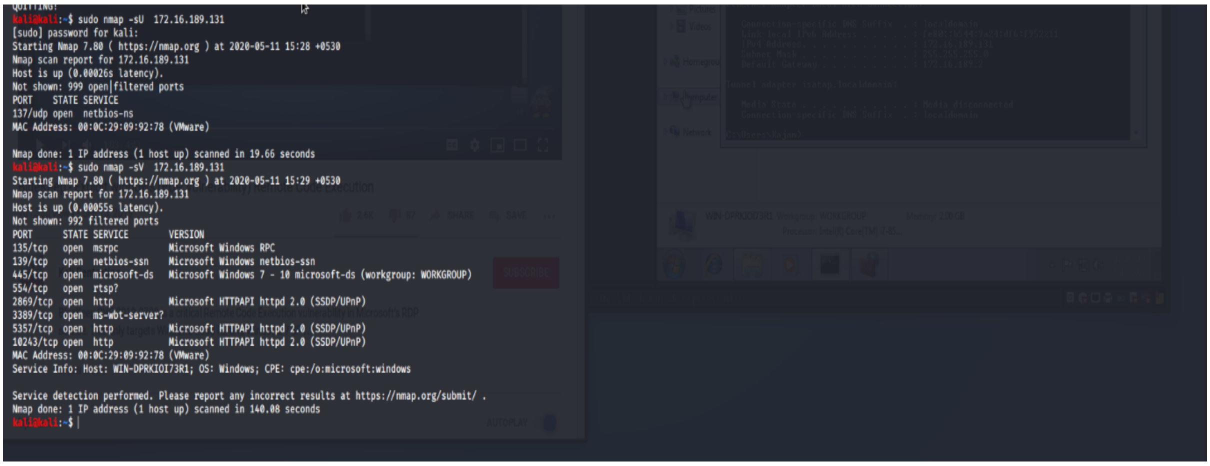
```
kali@kali:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2148  bytes 19328578 (18.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2148  bytes 19328578 (18.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vmnet1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.54.1  netmask 255.255.255.0  broadcast 172.16.54.255
        inet6 fe80::250:56ff:fec0:1  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:c0:00:01  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vmnet8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.189.1  netmask 255.255.255.0  broadcast 172.16.189.255
        inet6 fe80::250:56ff:fec0:8  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:c0:00:08  txqueuelen 1000  (Ethernet)
        RX packets 249  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.8.141  netmask 255.255.255.0  broadcast 192.168.8.255
        inet6 2402:4000:2381:f7e8:82a4:e5fa:ed2f:687d  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::b6bd:f6d3:5a6:5778  prefixlen 64  scopeid 0x20<link>
        ether 20:16:b9:4a:73:a1  txqueuelen 1000  (Ethernet)
        RX packets 847  bytes 1108111 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 425  bytes 62696 (61.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kali@kali:~$ |
```

03 – we need to use ping command in kali terminal and check the connection is fine or not with help of packets send and received fully without lost.

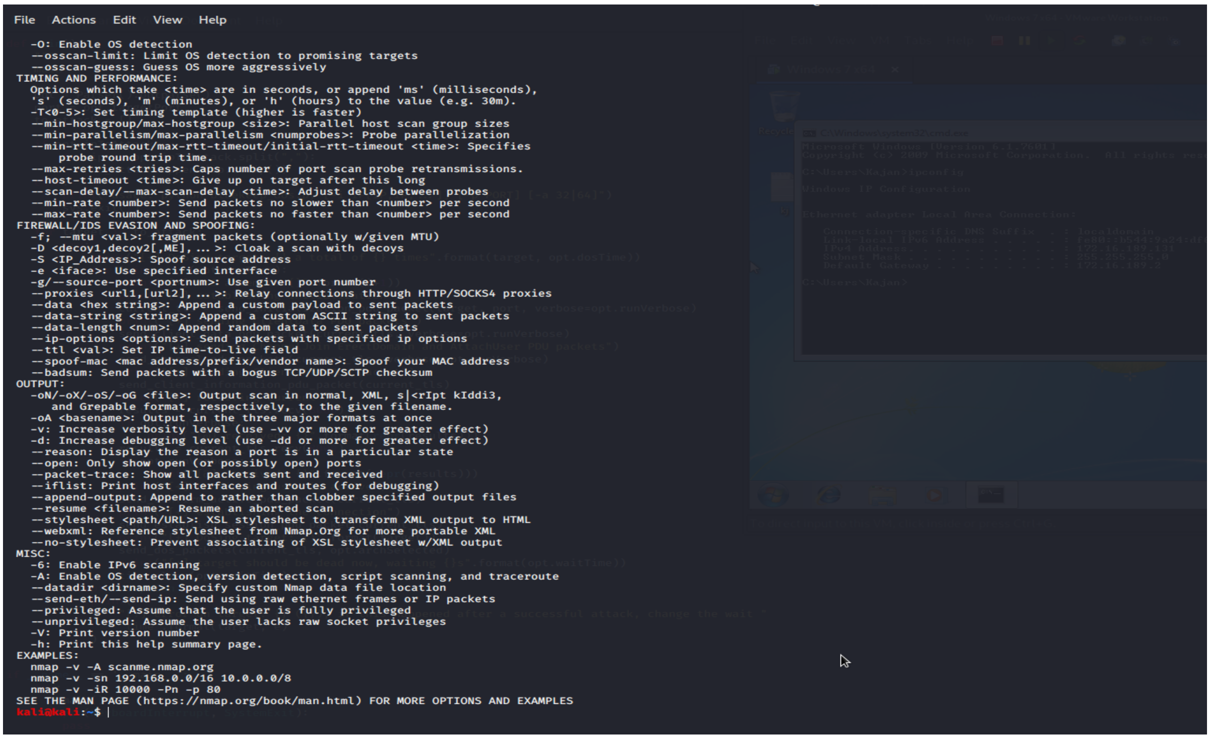


```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.8.141  netmask 255.255.255.0  broadcast 192.168.8.255
        inet6 2402:4000:2381:f7e8:82a4:e5fa:ed2f:687d  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::b6bd:f6d3:5a6:5778  prefixlen 64  scopeid 0x20<link>
        ether 20:16:b9:4a:73:a1  txqueuelen 1000  (Ethernet)
        RX packets 847  bytes 1108111 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 425  bytes 62696 (61.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kali@kali:~$ ping 172.16.189.131
PING 172.16.189.131 (172.16.189.131) 56(84) bytes of data.
64 bytes from 172.16.189.131: icmp_seq=1 ttl=128 time=0.804 ms
64 bytes from 172.16.189.131: icmp_seq=2 ttl=128 time=0.593 ms
64 bytes from 172.16.189.131: icmp_seq=3 ttl=128 time=0.576 ms
64 bytes from 172.16.189.131: icmp_seq=4 ttl=128 time=0.590 ms
64 bytes from 172.16.189.131: icmp_seq=5 ttl=128 time=0.587 ms
^C
--- 172.16.189.131 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4099ms
rtt min/avg/max/mdev = 0.576/0.630/0.804/0.087 ms
kali@kali:~$
```

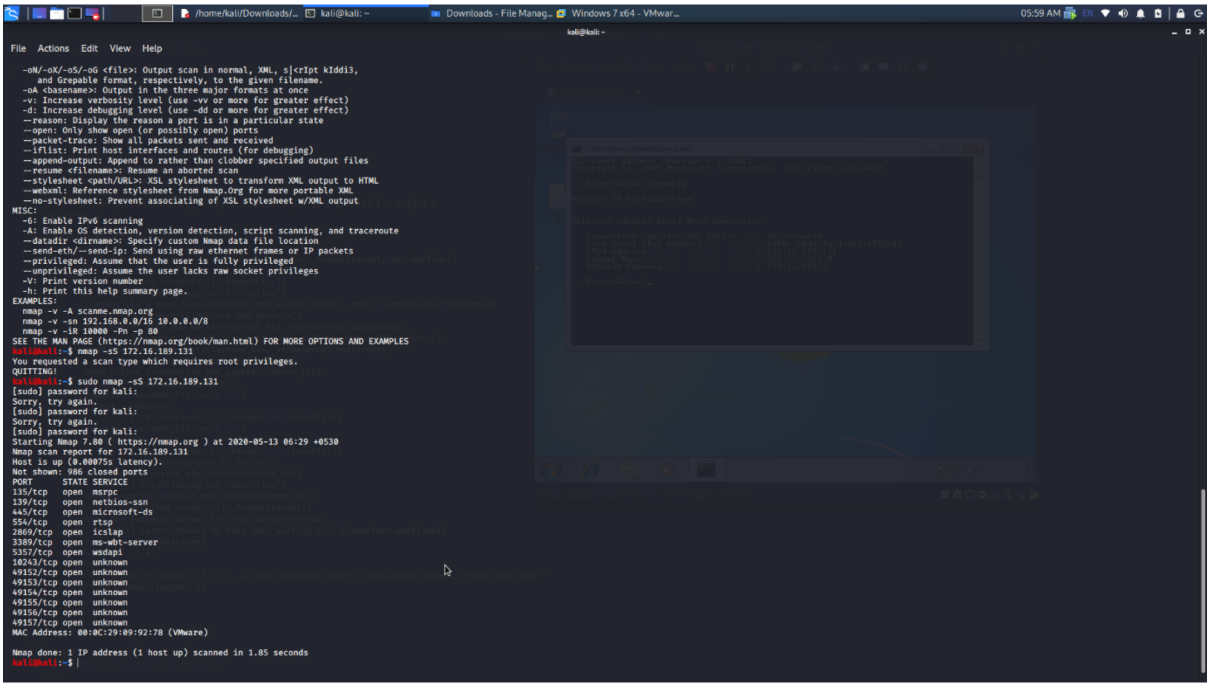
04 – we need to use nmap in kali to check ports are available or not. The port 3389 is used for Blue keep attack.



```
QUITTING!
kali@kali:~$ sudo nmap -sU  172.16.189.131
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-11 15:28 +0530
Nmap scan report for 172.16.189.131
Host is up (0.00026s latency).
Not shown: 999 open|filtered ports
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: 00:0C:29:09:92:78 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 19.66 seconds
kali@kali:~$ sudo nmap -sV  172.16.189.131
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-11 15:29 +0530
Nmap scan report for 172.16.189.131
Host is up (0.00055s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server?
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 00:0C:29:09:92:78 (VMware)
Service Info: Host: WIN-DPRKIOI73R1; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 140.08 seconds
kali@kali:~$
```

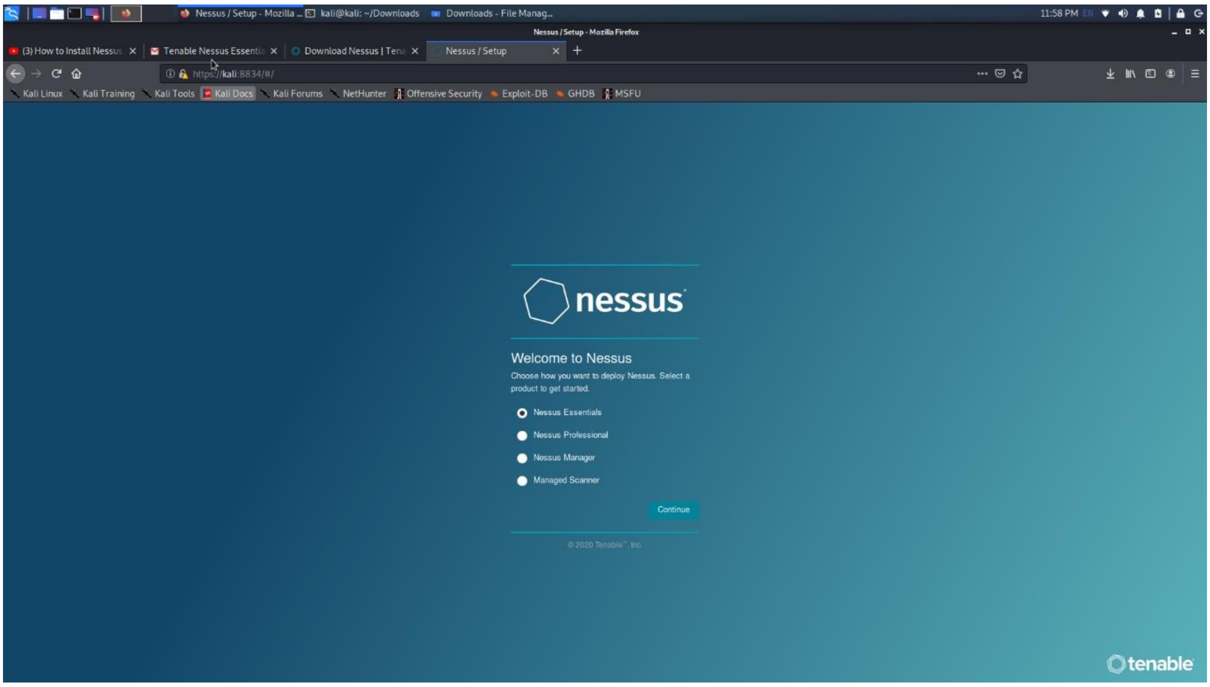


```
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
kali@kali:~$ |
```



```
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
kali@kali:~$ nmap -sS 172.16.189.131
You requested a scan type which requires root privileges.
QUITTING!
kali@kali:~$ sudo nmap -sS 172.16.189.131
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-13 06:29 +0530
Nmap scan report for 172.16.189.131
Host is up (0.00075s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:09:92:78 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds
kali@kali:~$ |
```

05 -After we confirm ports are available, we need to check the vulnerable are available for our ip address of windows with the help of nessus tool. If you don’t have you need to install it with the help of youtube.



https://kali:8834/#/

Welcome to Nessus

Choose how you want to deploy Nessus. Select a product to get started.

● Nessus Essentials

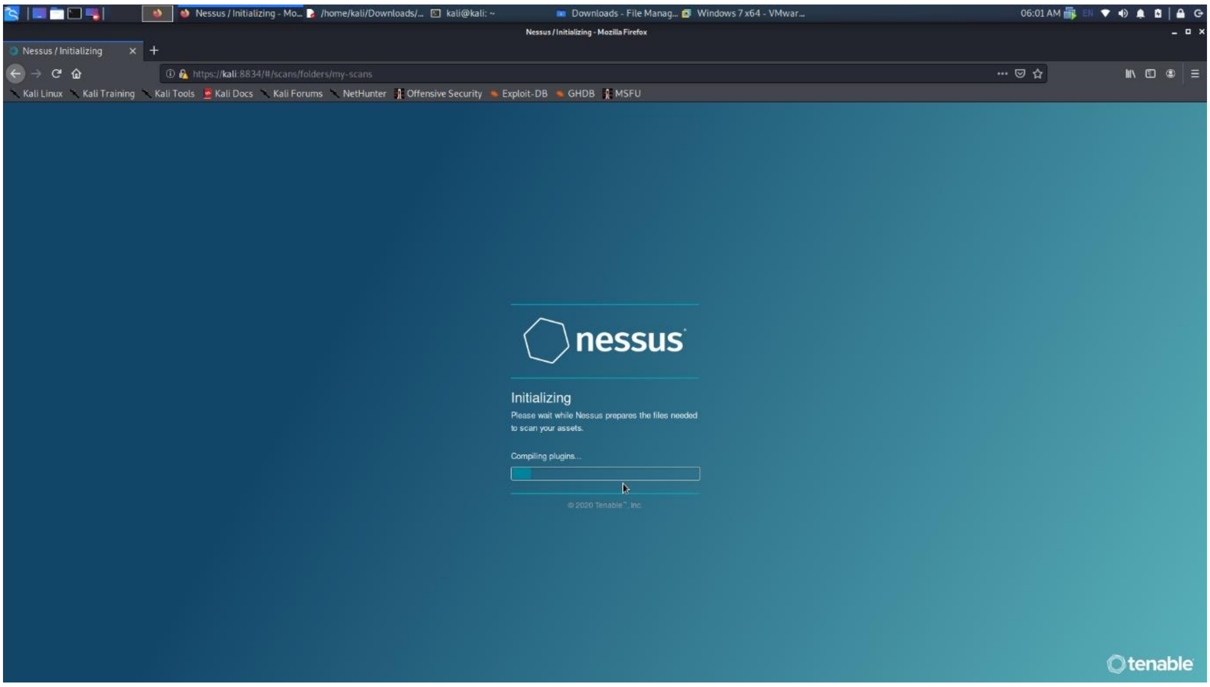
○ Nessus Professional

○ Nessus Manager

○ Managed Scanner

Continue

© 2020 Tenable™, Inc.



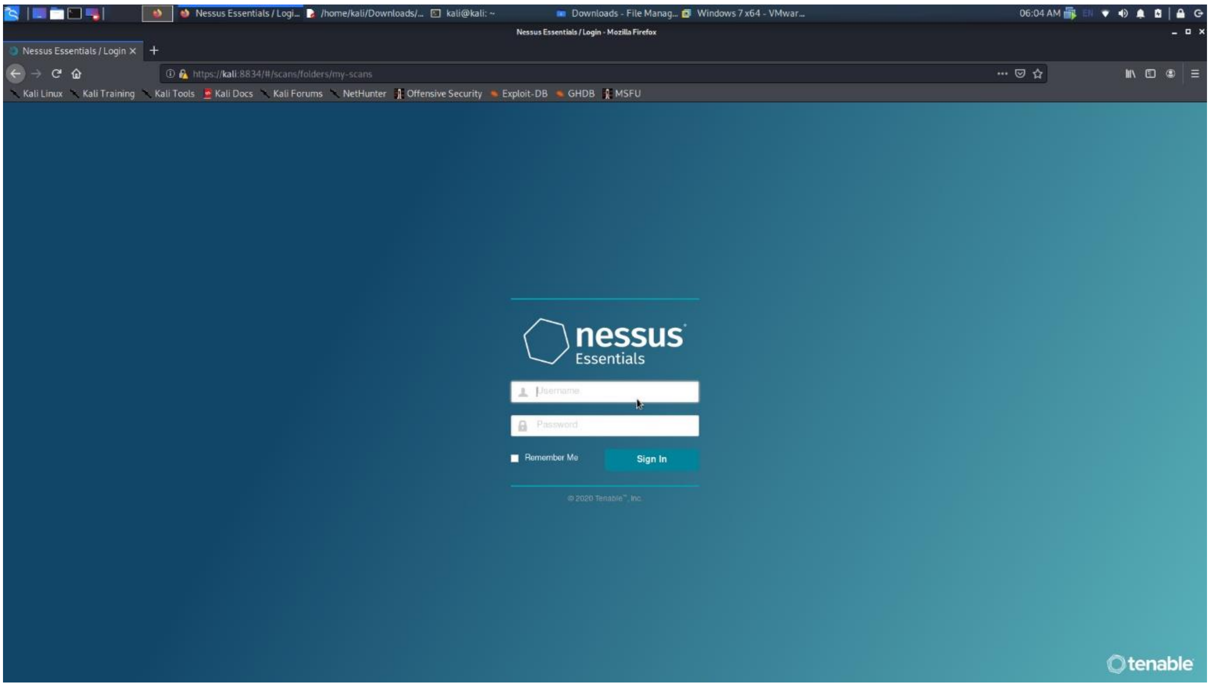
https://kali:8834/#/scans/folders/my-scans

Initializing

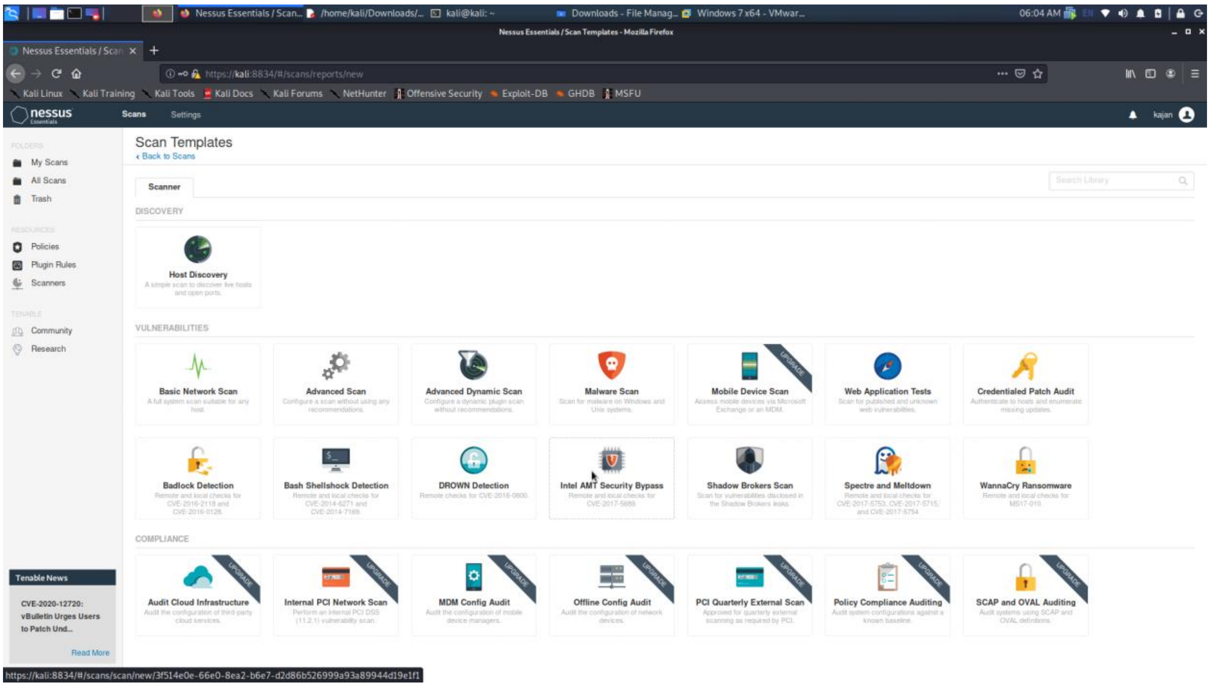
Please wait while Nessus prepares the files needed to scan your assets.

Compiling plugins...

© 2020 Tenable™, Inc.



06- sacn your ip address as shown in this picture and see All kind of vulnerable under critical normal categories.



Scan Templates

‹ Back to Scans

Scanner

DISCOVERY

- Host Discovery: A simple scan to discover live hosts and open ports.

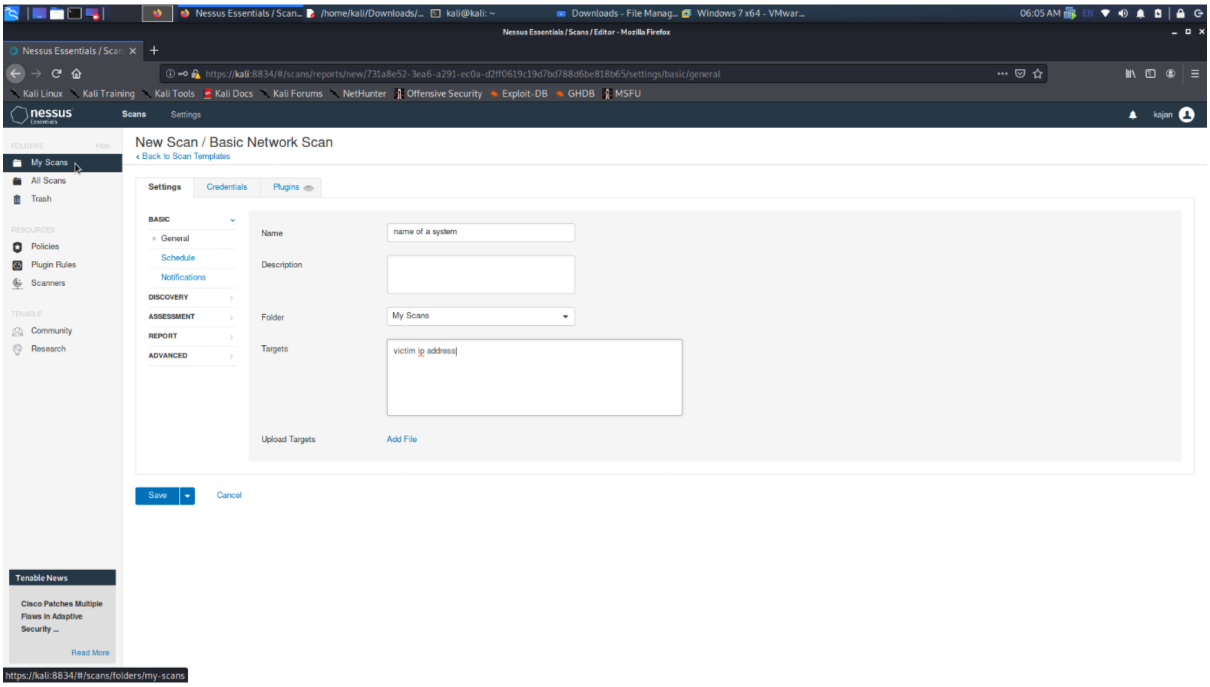
VULNERABILITIES

- Basic Network Scan: A full system scan suitable for any host.
- Advanced Scan: Configure a scan without using any recommendations.
- Advanced Dynamic Scan: Configure a dynamic plugin scan without recommendations.
- Malware Scan: Scan for malware on Windows and Unix systems.
- Mobile Device Scan (UPGRADE): Assess mobile devices via Microsoft Exchange or an MDM.
- Web Application Tests: Scan for published and unknown web vulnerabilities.
- Credentialed Patch Audit: Authenticate to hosts and enumerate missing updates.
- Badlock Detection: Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
- Bash Shellshock Detection: Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
- DROWN Detection: Remote checks for CVE-2016-0800.
- Intel AMT Security Bypass: Remote and local checks for CVE-2017-5689.
- Shadow Brokers Scan: Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
- Spectre and Meltdown: Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.
- WannaCry Ransomware: Remote and local checks for MS17-010.

COMPLIANCE

- Audit Cloud Infrastructure (UPGRADE): Audit the configuration of third-party cloud services.
- Internal PCI Network Scan (UPGRADE): Perform an internal PCI DSS (11.2.1) vulnerability scan.
- MDM Config Audit (UPGRADE): Audit the configuration of mobile device managers.
- Offline Config Audit (UPGRADE): Audit the configuration of network devices.
- PCI Quarterly External Scan (UPGRADE): Approved for quarterly external scanning as required by PCI.
- Policy Compliance Auditing (UPGRADE): Audit system configurations against a known baseline.
- SCAP and OVAL Auditing (UPGRADE): Audit systems using SCAP and OVAL definitions.

https://kali:8834/#/scans/scan/new/3f514e0e-66e0-8ea2-b6e7-d2d86b526999a93a89944d19e1f1


Nessus Essentials / Scans / Editor - Mozilla Firefox
https://kali:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general
nessus Essentials
Scans
Settings
kajan
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
Cisco Patches Multiple Flaws in Adaptive Security ...
Read More

New Scan / Basic Network Scan

‹ Back to Scan Templates

Settings | Credentials | Plugins

BASIC
- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: name of a system

Description:

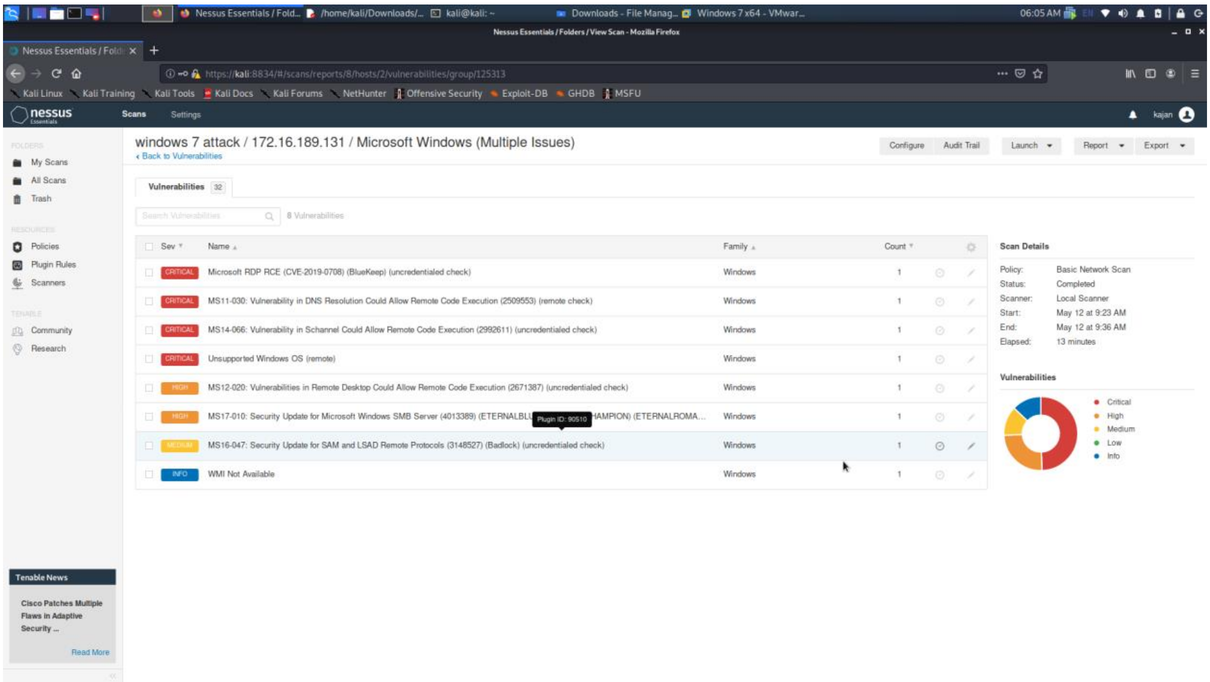
Folder: My Scans

Targets: victim ip address

Upload Targets: Add File

Save | Cancel

https://kali:8834/#/scans/folders/my-scans



windows 7 attack / 172.16.189.131 / Microsoft Windows (Multiple Issues)

‹ Back to Vulnerabilities

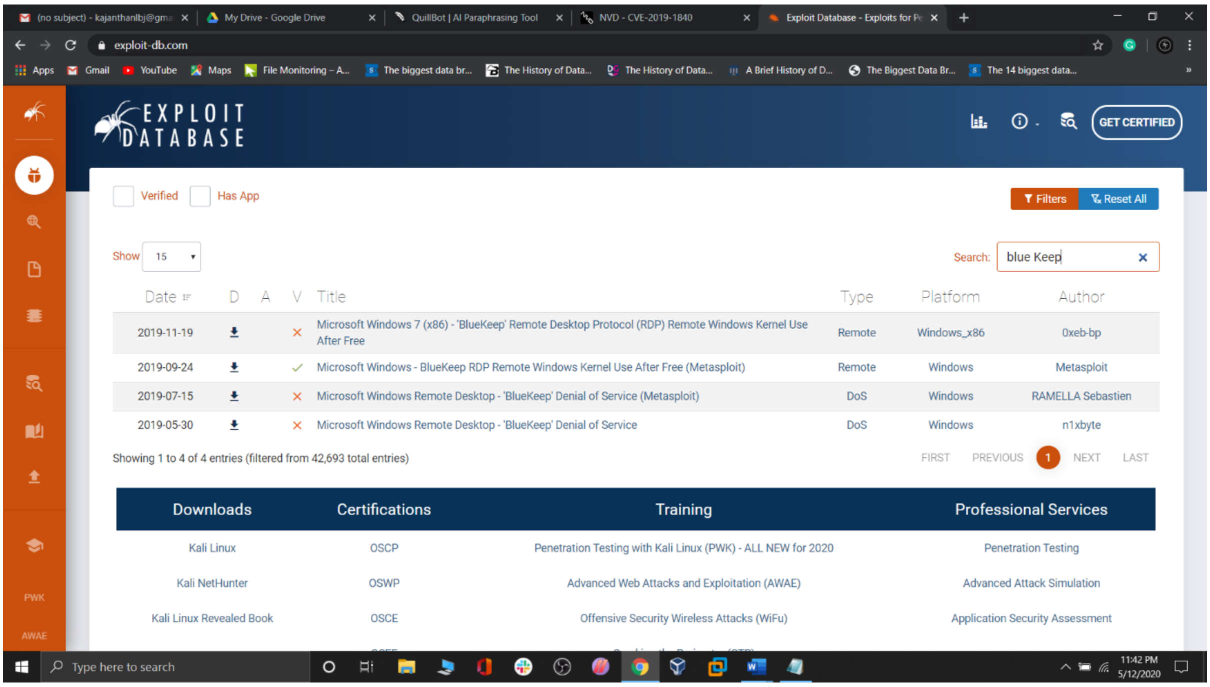
Sev	Name	Family	Count
CRITICAL	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	Windows	1
CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)	Windows	1
CRITICAL	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	Windows	1
CRITICAL	Unsupported Windows OS (remote)	Windows	1
HIGH	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	Windows	1
HIGH	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLU HAMPION) (ETERNALROMA...	Windows	1
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	Windows	1
INFO	WMI Not Available	Windows	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	May 12 at 9:23 AM
End:	May 12 at 9:36 AM
Elapsed:	13 minutes

Vulnerabilities

07- After we found Blue Keep vulnerable to our windows 7 ip address we need to download Exploit codes in Exploit DB or in GitHub and download it and ready to exploit.



☐ Verified ☐ Has App

Show 15

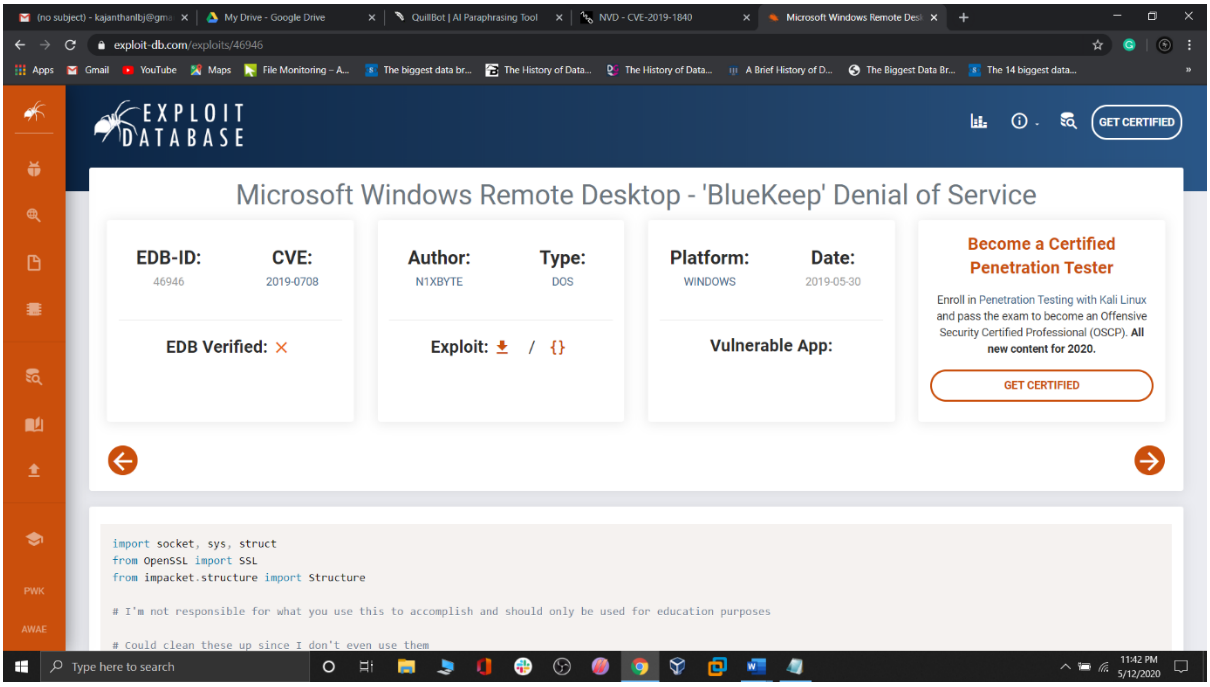
Search: blue Keep

Date	D	A	V	Title	Type	Platform	Author
2019-11-19	⬇		✗	Microsoft Windows 7 (x86) - 'BlueKeep' Remote Desktop Protocol (RDP) Remote Windows Kernel Use After Free	Remote	Windows_x86	0xeb-bp
2019-09-24	⬇		✓	Microsoft Windows - BlueKeep RDP Remote Windows Kernel Use After Free (Metasploit)	Remote	Windows	Metasploit
2019-07-15	⬇		✗	Microsoft Windows Remote Desktop - 'BlueKeep' Denial of Service (Metasploit)	DoS	Windows	RAMELLA Sebastien
2019-05-30	⬇		✗	Microsoft Windows Remote Desktop - 'BlueKeep' Denial of Service	DoS	Windows	n1xbyte

Showing 1 to 4 of 4 entries (filtered from 42,693 total entries)

FIRST PREVIOUS 1 NEXT LAST

Downloads	Certifications	Training	Professional Services
Kali Linux	OSCP	Penetration Testing with Kali Linux (PWK) - ALL NEW for 2020	Penetration Testing
Kali NetHunter	OSWP	Advanced Web Attacks and Exploitation (AWAE)	Advanced Attack Simulation
Kali Linux Revealed Book	OSCE	Offensive Security Wireless Attacks (WiFu)	Application Security Assessment



Microsoft Windows Remote Desktop - 'BlueKeep' Denial of Service

EDB-ID: 46946 CVE: 2019-0708

EDB Verified: ✗

Author: N1XBYTE Type: DOS

Exploit: ⬇ / {}

Platform: WINDOWS Date: 2019-05-30

Vulnerable App:

Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.

GET CERTIFIED

```
import socket, sys, struct
from OpenSSL import SSL
from impacket.structure import Structure

# I'm not responsible for what you use this to accomplish and should only be used for education purposes

# Could clean these up since I don't even use them
```

09 – finally By typing python3(name of file).py (ip address of windows) (64 bit or 32 bit)

Pyhton3 46904.py 172.16.189.131 64

You can see Blue Colour codes are running and your windows 7 start to shutting down

Conclusion

If it is still being running older versions of OSs, need to be protect from the Blue Keep malware.If u Haven't patched your system to help guard against this malware, It's time to do something
about it.

CISA urges users and administers to review and incorporate effective mitigation steps as soon as possible, the Microsoft Security Warning and Microsoft Client Guidance for CVE-2019-0708.

1. Patch as soon as possible with the latest Microsoft update. In order to fix this vulnerability, Microsoft released security updates. Microsoft has also released updates on a range of OSs, including Windows Vista, Windows XP and Windows Server 2003, which are no longer officially supported. As ever, before installation, Cybersecurity and Infrastructure Security Agency invites users and administrators to test patches.

2. We can upgrade end-of-life OSs. Consider upgrading to a newer, supported OS like Window 10 any EOL OS that is no longer supported by Microsoft.

3. Disable services not used by OS. Disable services This best practice decreases vulnerability exposure.

4. Enable authentication of the network level in Windows 7 and Windows Server 2008, and Windows Server 2008 R2. It allows a client access to be authenticated and essentially mitigates Blue Keep as it needs an unauthenticated user to exploit the vulnerability.

5.Can be blocked Ports 3389 on enterprise perimeter firewall of the Network Transmission Control Protocol (TCP). Since port 3389 is used for starting an RDP session, it prevents an attacker from running Blue Keep outside the user network, blocking it. This will therefore block valid RDP sessions and can not prevent the initiation of unauthenticated sessions in the network.

6.Monitor incoming RDP connections.