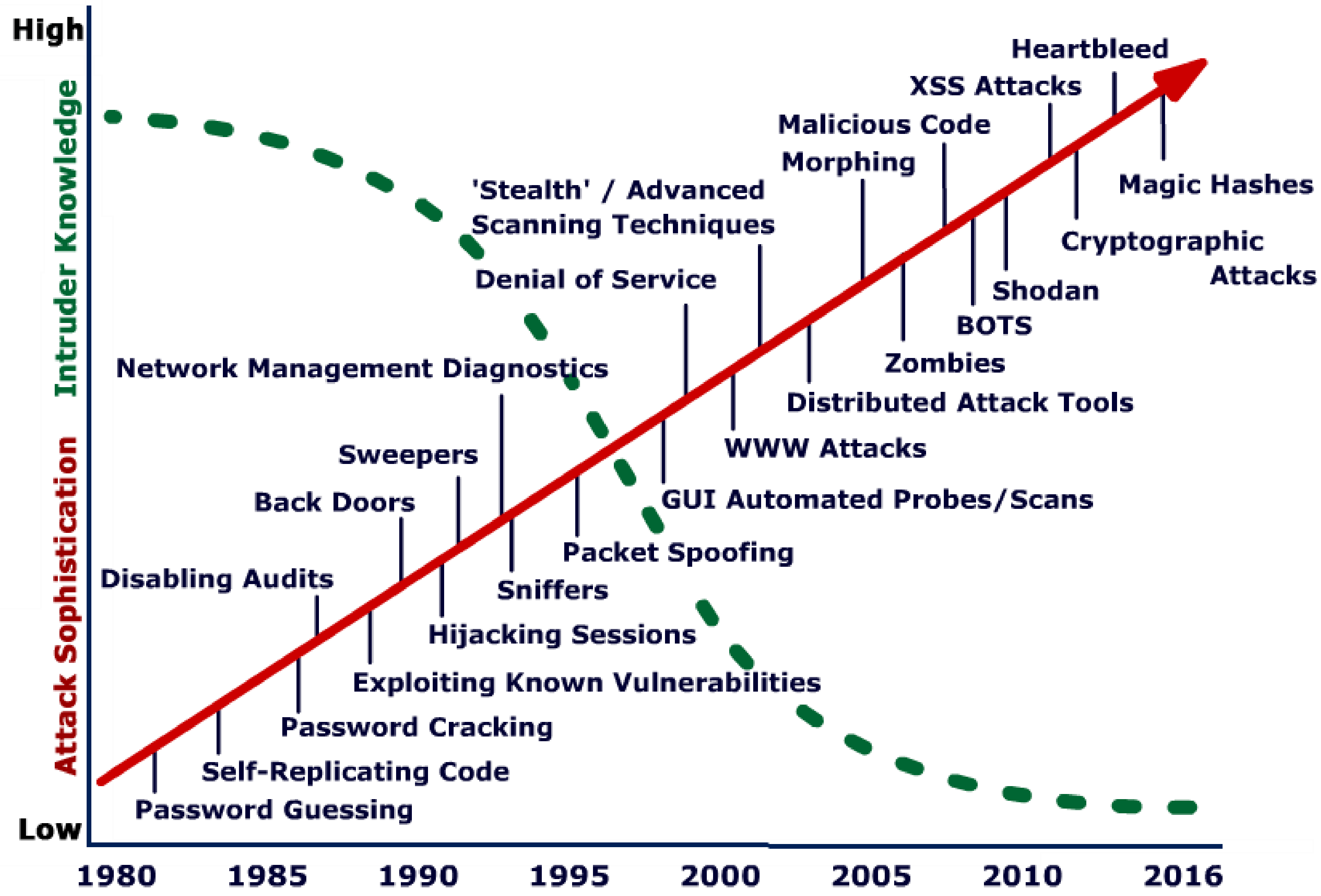
CYBER SECURITY FUNDAMENTALS

By – Apurv Singh Gautam

WHAT TO EXPECT??

NEED OF SECURITY

- Increasing awareness of technology but not Security
- Continuous Development & Competition in IT
- Increasing number of Cyber Criminals
- Increasing use of Network elements & applications
- Decreasing level of skill set


High
Low
Intruder Knowledge
Attack Sophistication
Heartbleed
XSS Attacks
Malicious Code
Morphing
Magic Hashes
'Stealth' / Advanced
Scanning Techniques
Cryptographic
Attacks
Denial of Service
Shodan
BOTS
Zombies
Network Management Diagnostics
Distributed Attack Tools
Sweepers
WWW Attacks
Back Doors
GUI Automated Probes/Scans
Packet Spoofing
Disabling Audits
Sniffers
Hijacking Sessions
Exploiting Known Vulnerabilities
Password Cracking
Self-Replicating Code
Password Guessing
1980
1985
1990
1995
2000
2005
2010
2016

NEED OF SECURITY

- Any Security breach in the website of any person increases the risk of the public image

- Any Security breach in the website of any company increases the risk of company reputation

- Any Security breach in the government website may increase the risk on project management and government operations

WHAT IS HACKING??

- Hacking is an art of exploring various security breaches

- What people believe: It’s an anti-social activity

  : All the hackers are bad people

- The terms Hacker and Hacking are being misinterpreted and misunderstood with negative sidelines

COMMUNITIES OF HACKERS

- Hackers
- Crackers
- Phreaks
- Script Kiddies

TYPES OF HACKERS

- **White Hat Hacker** - They use their knowledge and skill set for good constructive intents. They find out new security loopholes and their solutions
- **Black Hat Hacker** - They use their knowledge and skill set for illegal activities and destructive intents
- **Grey Hat Hacker –** They use their knowledge and skill set for legal and illegal purpose. They are white hats in public but internally they do some black hat work

NETWORKING FUNDAMENTALS

IP ADDRESS

IP Address is also known as,

- Logical Address, or
- Unique Identity Address

It is used to identify the systems. Whenever any computer connects itself with the internet or with LAN, it gets one IP address, that IP address is always unique in the network. This means, once an IP address is assigned to any system in the network, it cannot be assigned to any other system. The same in the internet, if one IP address has been assigned to one system, it cannot be assigned to anyone else

IP TYPES

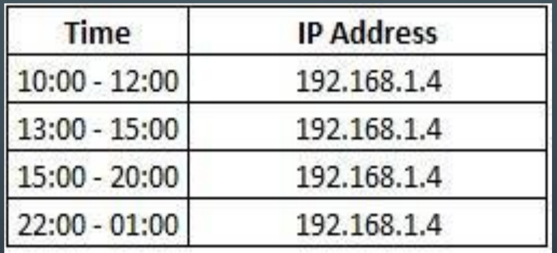
- **Internal IP** - Whenever a computer connects itself with an Internal Network (LAN) , it gets an Internal IP. This IP will be the identity of the particular computer in the network

- **External IP** - Whenever a computer connects itself with the internet , it gets an IP address by ISP. This IP will be the identity of the particular computer over the internet.

IP TYPES

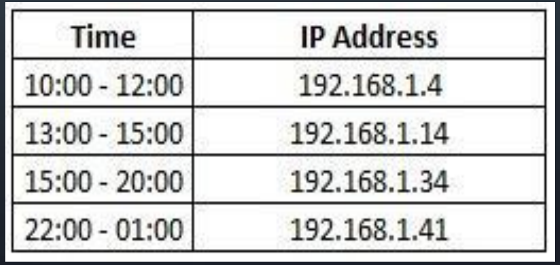
Both the Internal & External IP address can be allocated in two forms.

- **Static IP Address** - Static IP Address remains same in all the sessions.



Time	IP Address
10:00 - 12:00	192.168.1.4
13:00 - 15:00	192.168.1.4
15:00 - 20:00	192.168.1.4
22:00 - 01:00	192.168.1.4

- **Dynamic IP Address** - Dynamic IP Address keeps changing in all the sessions.



Time	IP Address
10:00 - 12:00	192.168.1.4
13:00 - 15:00	192.168.1.14
15:00 - 20:00	192.168.1.34
22:00 - 01:00	192.168.1.41

INTRODUCTION TO TROJANS

VIRUS & WORMS

Virus, *V*ital *I*nformation *R*esource *U*nder *S*eize , is a piece of code which is meant for the malicious purpose. It can replicate itself In the same system or also to the external hard drive. It may harm your system by deleting vital information from your hard drive or by corrupting the operating system files.

Worms are the virus that replicates itself by resending itself as an e-mail attachment or as part of a network message. Worms does not alter files but resides in active memory and duplicates itself. Worm use parts of an operating system that are automatic and usually invisible to the user

TROJANS

Trojans are piece of code which is meant for the remote administration purpose. It may or may not harm your computer but the hacker can administrate your computer remotely. A hacker may see the webcam, can get the logs of all the key strokes and can also delete any file & folders from your system. Trojans are one of the most dangerous and widely used by hackers to get into the systems

TYPES OF TROJANS

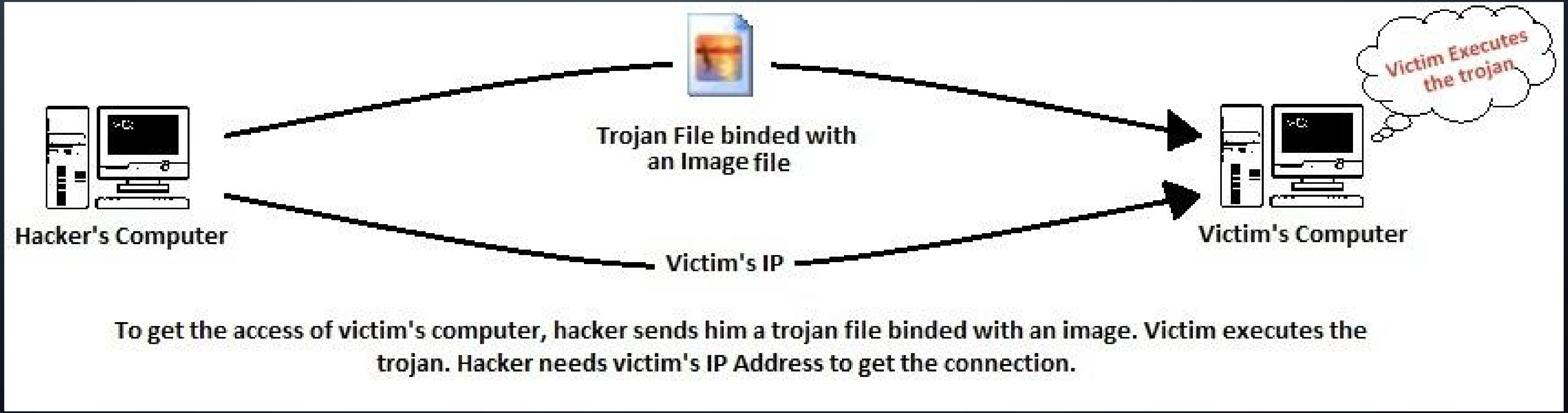
- Direct Connection Trojan

- Reverse Connection Trojan

DIRECT CONNECTION TROJAN

In the direct connection Trojan, Victim's IP Address plays essential role. Hacker sends Trojan to victim, victim unknowingly executes it. To get the remote connection of victim's computer, hacker needs to have IP Address of victim. Hacker uses different methods to get the IP address of victims such as,

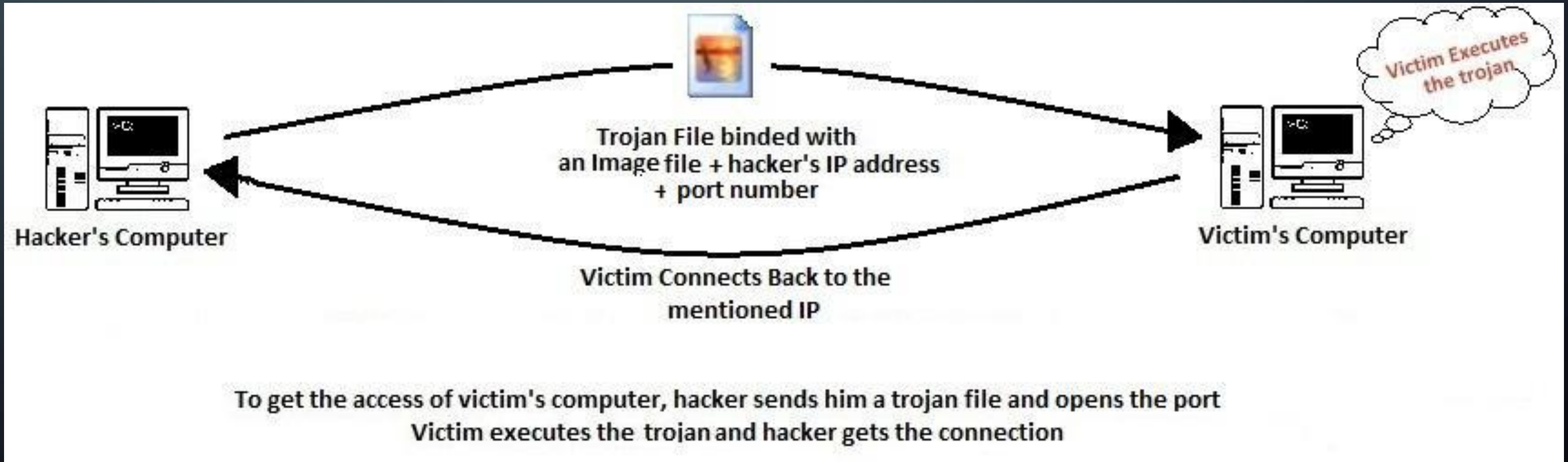
- Email Tracing


Trojan File binded with an Image file
Victim Executes the trojan
Hacker's Computer
Victim's Computer
Victim's IP

To get the access of victim's computer, hacker sends him a trojan file binded with an image. Victim executes the trojan. Hacker needs victim's IP Address to get the connection.

REVERSE CONNECTION TROJAN

Hacker creates the Trojan with his own IP address. In this case, when a victim executes the Trojan, hacker gets the connection. Hacker needs to open one port to get the connection.


Trojan File binded with
an Image file + hacker's IP address
+ port number
Hacker's Computer
Victim's Computer
Victim Executes the trojan
Victim Connects Back to the mentioned IP

To get the access of victim's computer, hacker sends him a trojan file and opens the port
Victim executes the trojan and hacker gets the connection

RAT (REMOTE ADMINISTRATION TOOL)

RAT IS, Remote Administration Tool used to create the Trojans. One can use their own coding to create the Trojans also but RAT may help you to create it easily.

- It is also used to control the victim's computer. After creating and sending the Trojan, hacker needs to open a port on his own system, for this a hacker can use RAT.
- RAT is created by the hackers to help the hackers,
- Also after getting the connection hacker can perform various tasks such as accessing the webcam, file & folder operations, edit the registry and even can edit the command prompt of the victim using RAT.

RAT (REMOTE ADMINISTRATION TOOL)

RATs are available for both the types of Trojans. There are numerous RATs available over the internet such as,

- Cyber Gate
- Dark Comet
- Pro Rat
- Poison Ivy
- Net Bus

Etc, etc, etc, …

INTRODUCTION TO SOCIAL ENGINEERING

“Cause there’s no PATCH for HUMAN STUPIDITY”

WHAT IS SOCIAL ENGINEERING??

In context of Information Security, it is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

CNN Money
HACKER?

TECHNIQUE

- Human Interaction

- Respectable & Known Person or Entity

- Assembling all gathered information together

TYPES OF SOCIAL ENGINEERING

- Quid Pro Quo – Something for something
- Phishing
- Baiting
- Pretexting
- Diversion Theft

WEAKEST LINK??

No matter how strong your:

- Firewalls
- IDS & IPS
- Cryptography
- Anti-Virus Software

- You are the weakest link in computer security. People are more vulnerable than computers.
- “The weakest link in the security chain is the human element: - Kevin Mitnick

WAYS TO PREVENT SOCIAL ENGINEERING

- User Awareness
- Policies
- Third party Test
- Be Smart

WATCH THIS HACKER BREAK INTO MY CELL PHONE ACCOUNT IN 2 MINUTES

CONTACT

- Email – apurvsinghgautam@gmail.com
- Mobie No. - +91 9918045500
- Social Name – Apurv Singh Gautam

  (Google, Facebook, Twitter, LinkedIn, Quora, etc etc)