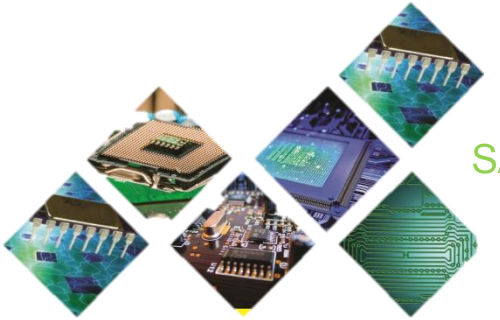


SAFE AND SECURE INTELLIGENT SYSTEMS

ETHICAL HACKING & CYBER SECURITY

17th International Conference on Embedded Systems
31st International Conference on VLSI Design

Quick Intro

- Mr.Anil Raj (B tech(Comp.Sci)/Certified Ethical Hacker/ECSA/LPT/CCNA)
- Former Sr. Info Security Consultant to IBM
- Cyber Security Professional with 9+ years of experience in IT Security Projects, Forensics & IT Security Consulting
- Expertise in Web App Security, VAPT , Network Security , Forensics & Regulatory Compliances
- Winner Of “Talented Personality Of India” Award in field of Cyber Security
- Dynamic Leader and frequent appearance in Media, Newspaper and for Seminars .

Agenda

- Introduction Of Cyber Security And Ethical Hacking
- Element Of Cyber Security
- Overview of Hacking Concept, Types and Phases
- Case Studies
- About Ransomware
- Other Hacking Attacks
- Protection Against Cyber Crime

Did You Ever face…

- Home Page Of Web Browser Changed
- Getting unnecessary Pop-ups while browsing Internet
- Reduction Of Hard Disk Space?
- System Hangs,While task manager show only 10% load?
- Short-cut is created in your pen drive?
- Received prize winning SMS or mail?

Element Of Information Security

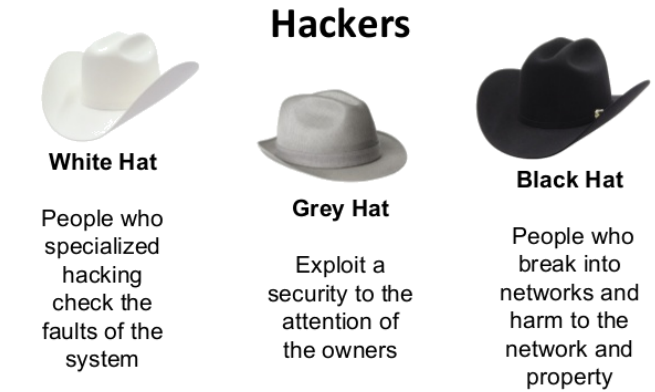
Confidentiality : Assure that the information is accessible only to those authorized to have.

Integrity : The trustworthiness of data and resources in terms of preventing improper and unauthorized changes.

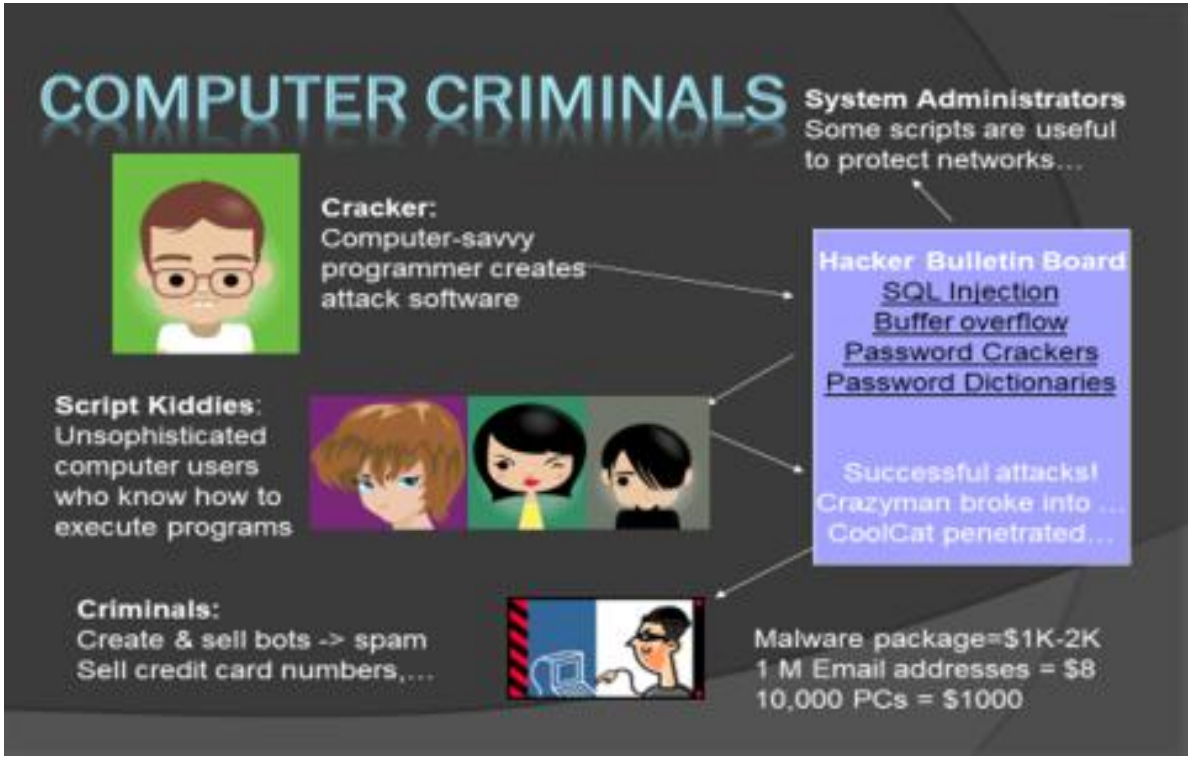
Availability : Resource should be available at the time of requirement

Hacking

- Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to the system resources.

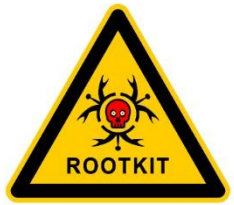


Computer Criminals



Some thing About Malwares

- Virus
- Worms
- Trojan Horse/ Logic Bomb
- Social Engineering
- RootKit
- Botnet/Zombies

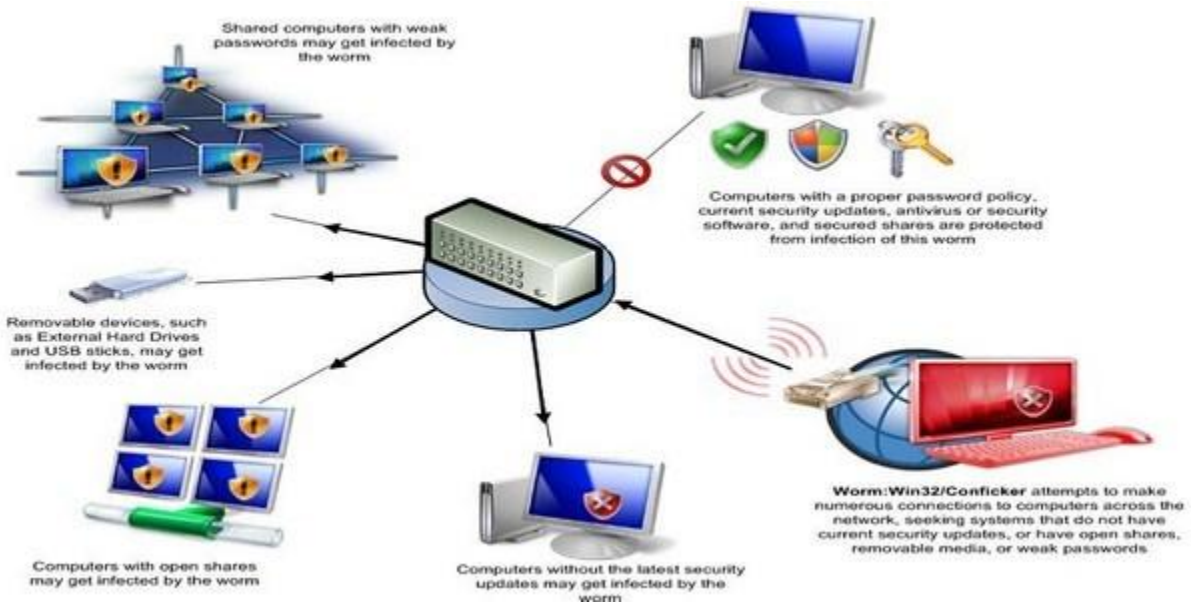


Virus

- A virus attaches itself to a program, file, or disk
- When the program is executed, the virus activates and replicates itself
- In order to recover/prevent virus/attacks:
  - Avoid potentially unreliable websites/emails
  - System Restore
  - Re-install operating system
  - Anti-virus (i.e. Avira, AVG, Norton)

Worm

- Independent program which replicates itself and sends copies from computer to computer across network connections. Upon arrival the worm may be activated to replicate.



LogicBomb/Trojan

- **Logic Bomb:** Malware logic executes upon certain conditions. Program is often used for legitimate reasons.
  - Software which malfunctions if maintenance fee is not paid
  - Employee triggers a database erase when he is fired.

- **Trojan Horse:** Masquerades as beneficial program while quietly destroying data or damaging your system.
  - Download a game: Might be fun but has hidden part that emails your password file without you knowing.

Social Engineering

- Social engineering manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.

Phone Call:
This is John, the System Admin. What is your password?

In Person:
What ethnicity are you? Your mother's maiden name?

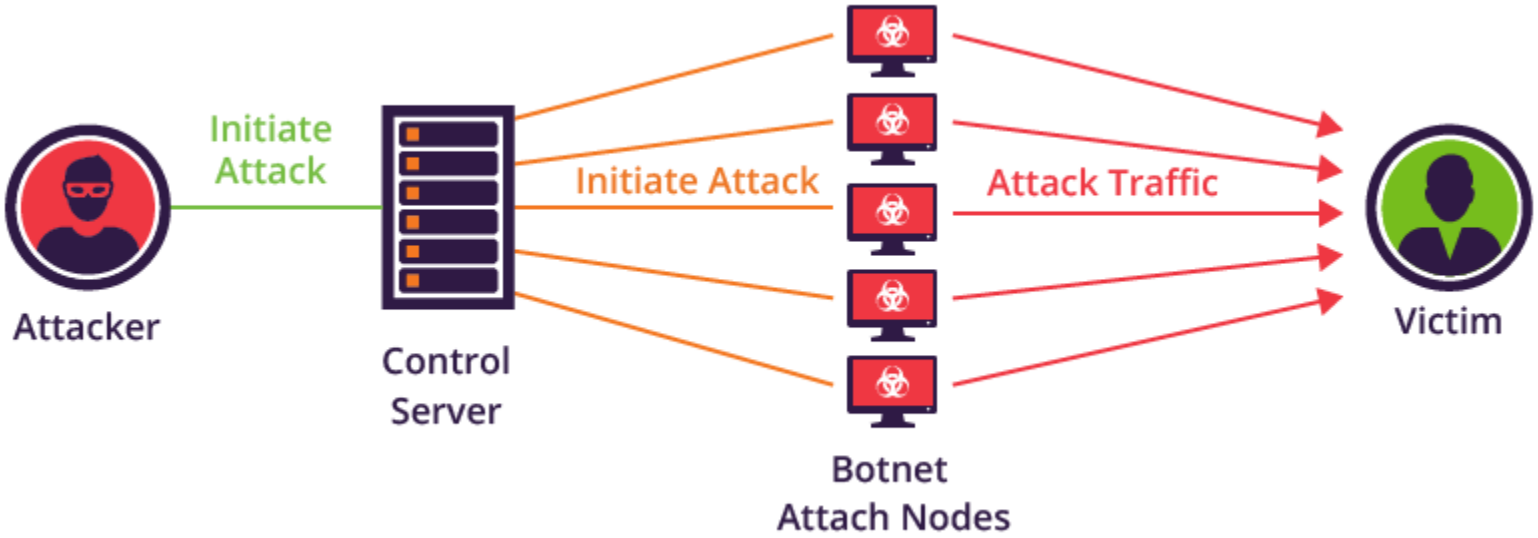
Email:
ABC Bank has noticed a problem with your account…

Phishing

- Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Botnet

- A botnet is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack.
- The compromised computers are called zombies



RootKit

- Upon penetrating a computer, a hacker installs a collection of programs, called a rootkit.
  - May enable:
    - Easy access for the hacker (and others)
    - Keystroke logger

Case Studies

- According to KPMG survey, 69% of organization in India, said that ransomware was a significant risk to them while 43% reveles that they had already experienced the same.
- According to CERT 40 incident of ransomware attack were reported, in which 34 incident included Wannacry and Petya ransomware.
- Wannacry attack had been first reported on 12 may 2017 and petya on 27th June 2017.

Case Studies

- However, in the first half of 2017 alone, CERT-IN received 27k report of Cyber security Risk.
- This include a range of threat like Phishing Assault, Website Intrusions and defacement or damages to data in addition to ransomware attack.
- Analyst have stated that India is among the top 7 countries for Ransomware circulation as cyber attack have increased this year globally.

Ransomware…WannaCry

- In one of biggest Cyber Attack in history in May 2017.
- In India the top 5 cities impacted by Ransomware attack where Kolkata followed by Delhi,Bhubneshwar, Pune and Mumbai.
- Almost 60 % of Wannacry attack attempts on Industry while the rest were on individual customers.

WannaCry

- Wannacry infected computers running on older version of Microsoft OS Like XP. Impact Of attack the Ransomware locked user's device and prevent them accessing their Data & Software until a certain ransom was paid to criminals.

Affected Area

- Police department in Aandhra Pradesh were disabled.
- West Bengal State Electricity distribution company limited were attacked.
- A govt. hospital in Odisha was targeted.
- In Gujrat over 120 odd computers connected with GSWAN(Gujrat state wide area network) were affected.
- Maharashtra police department was also partially hit.

Petya

India was on top 10 listing of nation to be hit by petya

Petya…

- Experts pointed out that petya was not really a ransomware like wannacry but it was rather a wiper.
- The aim of this malware was to delete all data, including data on the first sector of disk, where the information about the OS usually stored.
- The idea of this attack was to cause massive destruction of data not to make financial gain.

Affected Area

- JNPT and local manufacturing units of global Companies.

Some Famous Data Breaches In India

- **BSNL Malware attack**

The State Run telco's broadband network in Karnatka Circle was greatly affected by Malware Attack. The Virus rapidly affected 60k modems with default "Admin-admin" Username/Password combination. Following the BSNL had issued an advisory to it's broadband customer to change their default Username and Password.

Zomato Case

- Indian Restro search and discovery service provider Zomato in May 2017 reported that the company's database was breached in that 7.7 millions personal details was revealed.

Reliance Jio

- Jio was also victim of data breach. Interestingly, a website called magikapk.com went live after the attack and anyone could search for persnol details of Jio customer on the website. This website was later taken down after it went virul.

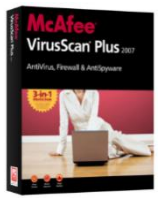
Know the Hacking Weapons…

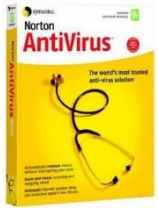
- Metasploit
- Kali LinuX OS
- Nmap
- Nessus
- Brute Force
- Keyloggers

Safe and Secure User Practices

Anti Virus and Anti Spyware

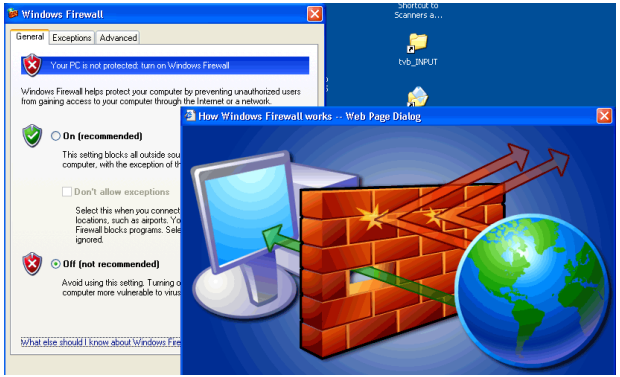
- Anti-virus software detects malware and can destroy it before any damage is done
- Install and maintain anti-virus and anti-spyware software
- Be sure to keep anti-virus software updated





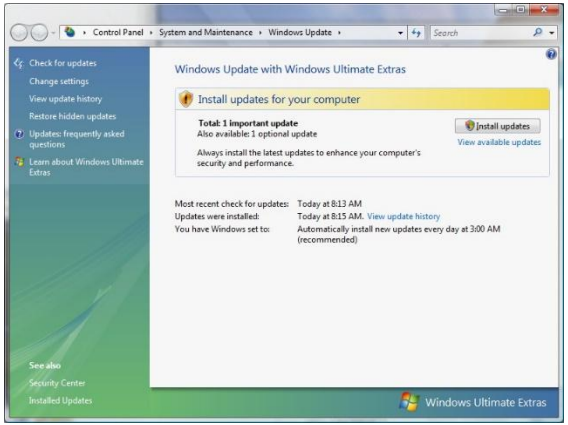
Firewall

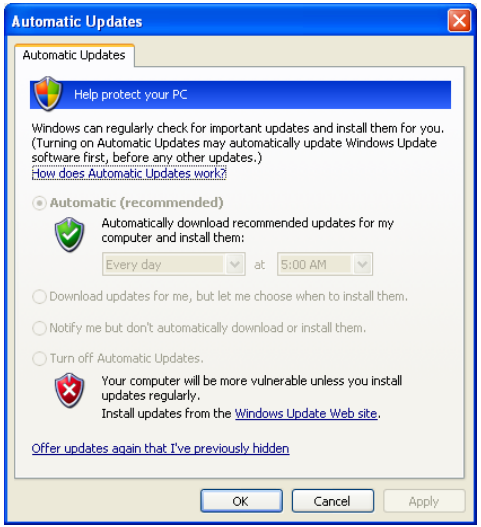
- A firewall acts as a wall between your computer/private network and the internet. Hackers may use the internet to find, use, and install applications on your computer. A firewall prevents hacker connections from entering your computer.
- Filters packets that enter or leave your computer



Protect Your Operating System

- Microsoft regularly issues patches or updates to solve security problems in their software. If these are not applied, it leaves your computer vulnerable to hackers.
- The Windows Update feature built into Windows can be set up to automatically download and install updates.





Creating a Good Password

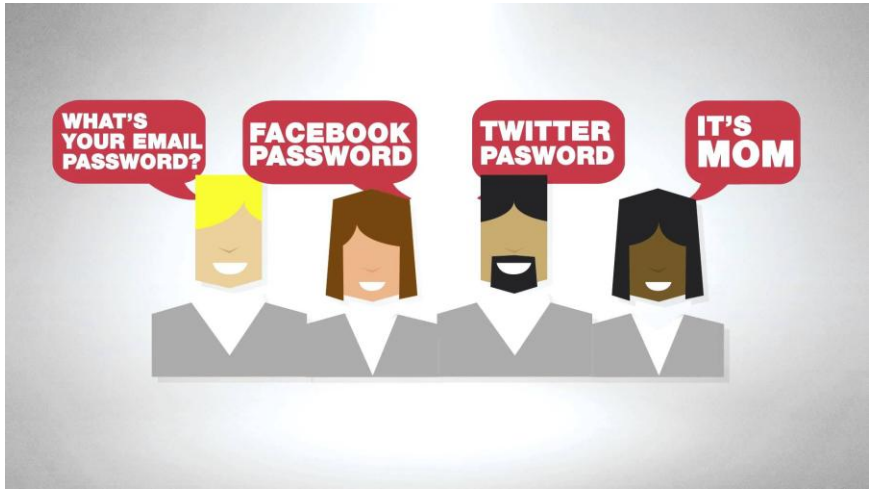
Combine 2 unrelated words	Mail+Phone=m@!lf0n3
Abbreviate a phrase	My favourite color is blue= mfciblue
Music Lyric	Happy Birthday to you Happy Birthday to you Happy Birthday to Dear John Happy Birthday to you hb2uhb2uhb2ujhb2u

Password Recommendations

- Never use ‘admin’ or ‘root’ or ‘administrator’ as a login for the admin
- A good password is:
  - **private:** it is used and known by one person only
  - **secret:** it does not appear in clear text in any file or program or on a piece of paper pinned to the terminal
  - **easily remembered:** so there is no need to write it down
  - **at least 8 characters, complex:** a mixture of at least 3 of the following: upper case letters, lower case letters, digits and punctuation
  - **not guessable** by any program in a reasonable time, for instance less than one week.
  - **changed regularly:** a good change policy is every 3 months

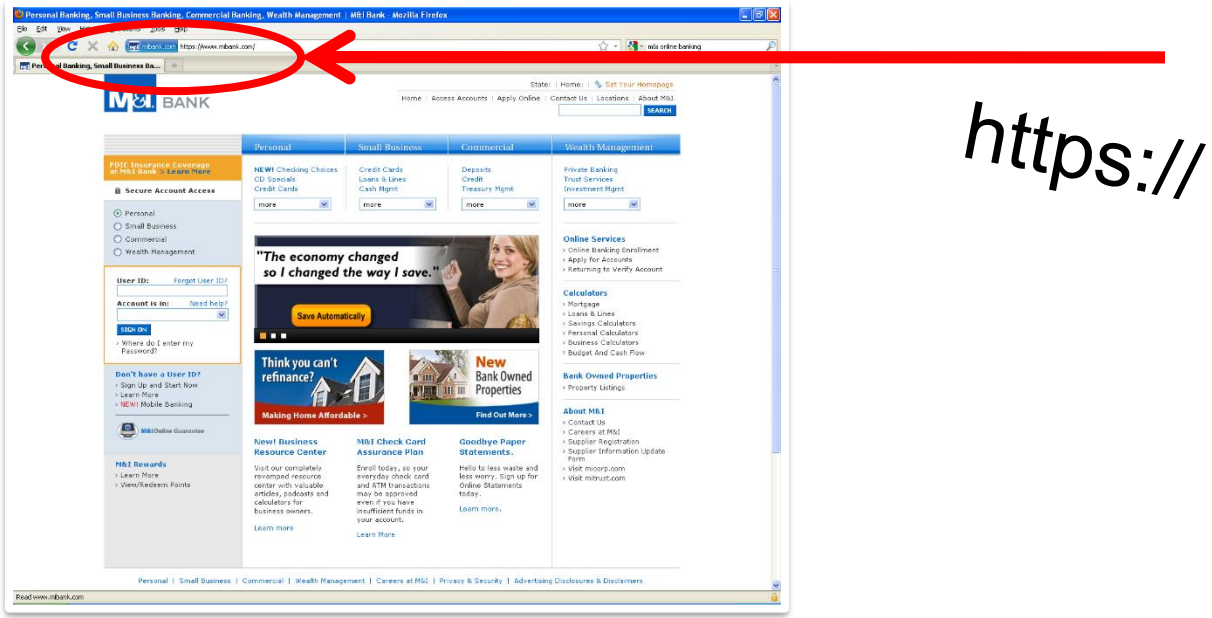
Avoid Social Engineering & Malicious Software

- Do not open email attachments unless you are expecting the email with the attachment and you trust the sender.
- Do not click on links in emails unless you are absolutely sure of their validity.
- Only visit and/or download software from web pages you trust.



Secure Online Activity

- Always use secure browser to do online activities.
- Frequently delete temp files, cookies, history, saved passwords etc.



Back-up Important Information

- No security measure is 100%
- What information is important to you?
- Is your back-up:

Recent??

Off-Site and Secure??

Tested??

Encrypted??

Put This Knowledge To Work

- These are best practices involving Information Security
- Most of these practices are from the NIST.
- Use these practices at home and at work to keep safe and secure

You can reach me for security queries

M- 9657665636
info@cybervaultsec.com