# BITS Pilani Presentation

**BITS** Pilani
Pilani Campus

Jagdish Prasad
WILP

# SSZG575: Ethical Hacking
# Session: 01 (Introduction)

# Agenda

- Course description
  - Objective
  - Course content
  - Text books
  - Structure & schedule
  - Evaluation scheme
  - Lecture plan
- Introduction to Ethical Hacking
  - Service & Application
  - Device, System, Person
  - Lifecycle for attack
  - Understand boundaries

# Course objectives

| No | Objective |
|----|-----------|
| CO1 | Introduce students to the techniques and tools for ethical hacking and countermeasures. |
| CO2 | To develop skills of exploit approaches – social engineering, scanning, foot-printing, enumeration, sniffers, buffer overflows. |
| CO3 | Understand service-specific hacking like DNS, Email, Web servers, Proxy; techniques of bypassing security mechanisms and hardening systems and networks for countermeasures of security analysis, monitoring and analysis tools including network traffic and system logs. |
| CO4 | Also learn the security paradigms in cloud computing, mobile platforms and online social networks. |

# Course content

- Introduction to Ethical Hacking
- Basic of Tools & Techniques for Ethical Hacking
- Vulnerabilities and Reverse Engineer Binaries
- Mobile Application Security
- Casing the Establishment
- Wireless Hacking and Hacking Hardware
- Remote Connectivity and VOIP
- Security Issues on Web Server and Database
- Processes and Tools used for Defense
- Recent Hack Reports

# Text books

- Text books

| T1 | Stuart McClure, Joel Scambray, George Kurtz, "Hacking Exposed 7: Network Security Secrets and Solutions, TMGH 2012 |
|---|---|

## Reference books

| R1 | Joseph Muniz, Aamir Lakhani, "Web Penetration Testing with Kali Linux", Shroff 2013 |
|---|---|
| R2 | Nipun Jaiswal, "Mastering Metasploit", Shroff/Packt 2014 |
| R3 | Neil Bergman etc. "Hacking Exposed Mobile: Security Secrets & Solutions", MGH 2013 |

# Text books…

## Other References

| | |
|---|---|
| O1 | https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project |
| O2 | https://www.stateoftheinternet.com/ |
| O3 | http://www.symantec.com/security_response/publications/threatreport.jsp |
| O4 | http://www.kb.cert.org/vuls |
| O5 | http://googleprojectzero.blogspot.in |
| O6 | https://code.google.com/p/google-security-research/issues/list |
| O7 | https://source.android.com/security/index.html and sublinks |

# Learning objectives

| No | Learning Objective |
|---|---|
| CO1 | Understand the components of enterprise and consumer applications and systems that can be exploited for hacking. |
| CO2 | Use tools and techniques to survey the target in the cyber world using foot printing, scanning and enumerating. |
| CO3 | Learn about multiple approaches to find vulnerabilities and exploit them using (a) network based attacks (b) host level compromise across different platforms and (c) deployment/system-component level attacks. |
| CO4 | Understand the weaknesses in wireless communications and execute some of the exploits in controlled environment. |
| L05 | Learn about tools to defend against attacks or minimize the damage. |

# Course structure & schedule

- 16 on-line lectures (2 hours each) + self study

- Schedule
  - Semester start (first lecture)          : 16-Jan-22
  - Last lecture                            : 15-May-22
  - Mid Sem Test                            : 11-13 Mar-22
  - Mid Sem Test Makeup                     : 25-27 Mar-22
  - Comprehensive Exam                      : 20-22 May-22
  - Comprehensive Exam Makeup               : 27-29 May-22

# Evaluation scheme

| No | Name | Type | Duration | Weight | Date & Time |
|----|------|------|----------|--------|-------------|
| EC-1 | Quiz-I | Online | - | 5% | After 4th session |
| | Quiz-II | Online | - | 5% | After 8th session |
| | Assignment / Lab | Offline | - | 10% | After 8th session |
| EC-2 | Mid-Semester Test | Closed Book | 1.5 hours | 30% | 11-13 Mar / 25-27 Mar |
| EC-3 | Comprehensive Exam | Open Book | 2.5 hours | 50% | 20-22 may / 27-29 May |

# Session schedule

| Day & Date | Timing 10.30 AM - 12. 30 AM |
|---|---|
| Sunday, 16 January, 2022 | CS-1 |
| Sunday, 23 January, 2022 | CS-2 |
| Sunday, 30 January, 2022 | CS-3 |
| Sunday, 6 February, 2022 | CS-4 |
| Sunday, 13 February, 2022 | CS-5 |
| Sunday, 20 February, 2022 | CS-6 |
| Sunday, 27 February, 2022 | CS-7 |
| Sunday, 6 March, 2022 | CS-8 |
| Friday-Sunday 11-13 March, 2022 | Mid-Semester Test (Regular) |
| Sunday, 20 March, 2022 | CS-9 |
| Friday-Sunday 25-27 March, 2022 | Mid-Semester Test (Make-up) |
| Friday, 8th April 2022 | CS-10 (5.50 PM -7.50 PM) |
| Sunday, 10 April, 2022 | CS-11 |
| Sunday, 17 April, 2022 | CS-12 |
| Sunday, 24 April, 2022 | CS-13 |
| Sunday, 1 May, 2022 | CS-14 |
| Sunday, 8 May, 2022 | CS-15 |
| Sunday, 15 May, 2022 | CS-16 |
| Friday-Sunday 20-22 May, 2022 | Compre-Examination (Regular) |
| Friday-Sunday 27-29 May, 2022 | Compre-Examination (Make-up) |

# Lab plan

| Lab # | Topic Covered |
|---|---|
| LO1 | Understanding the lab setup, isolated network, remote shell and related network protocols |
| LO2 | Compilers, assemblers, disassemblers, debuggers, trace tools, environment, sniffers etc. |
| LO3 | Linux password cracking exercises – different encryptions |
| LO4 | Reverse engineering a firmware update |
| L05 | Android tools, app development, and hacking an application to embed our code |
| L06 | Executing OS exploits – Linux |
| L07 | Executing OS exploits – Windows |
| L08 | Understand tools in Kali Linux for survey attempts |
| L09 | Executing protocol exploits – Web Server and Data Bases |
| L10 | Trojans and Camouflage |
| L11 | Wireless Hacking – HackRF One |
| L12 | Tools to mine online social information |
| L13 | Defense – Audit, discover and limit, detect malware, Honeypots, Firewalls, IDS/IPS, Log service |
| L14 | Mock capture the flag exercise |

# Introduction

# Cyber Attacks… Not a Rare News!

- Air India lost 4.5 Mn customer's data in early 2021

- Mumbai power outage in Oct 20 believed to be handiwork of Chinese hackers

- An attack on infrastructure provider Fastly caused major websites to go down in early Jun 21.

- 200% increase in cyber attacks post Covid-19

- Nearly 7,00,000 attacks in 2020 so far in India – IT ministry tells parliament (Sep'20)

- Malware attacks hist computers at NIC's cyber hub (18-Sep-20)

- Cyber attack on NHAI email server (29-Jun-20)

# News about Hacking

# Global Attack Scenario



**Total WAF Trigger Rule Frequency**

## 120,934,834

Attacks Observed for All Verticals

**Top Country / Area by Attack Frequency**

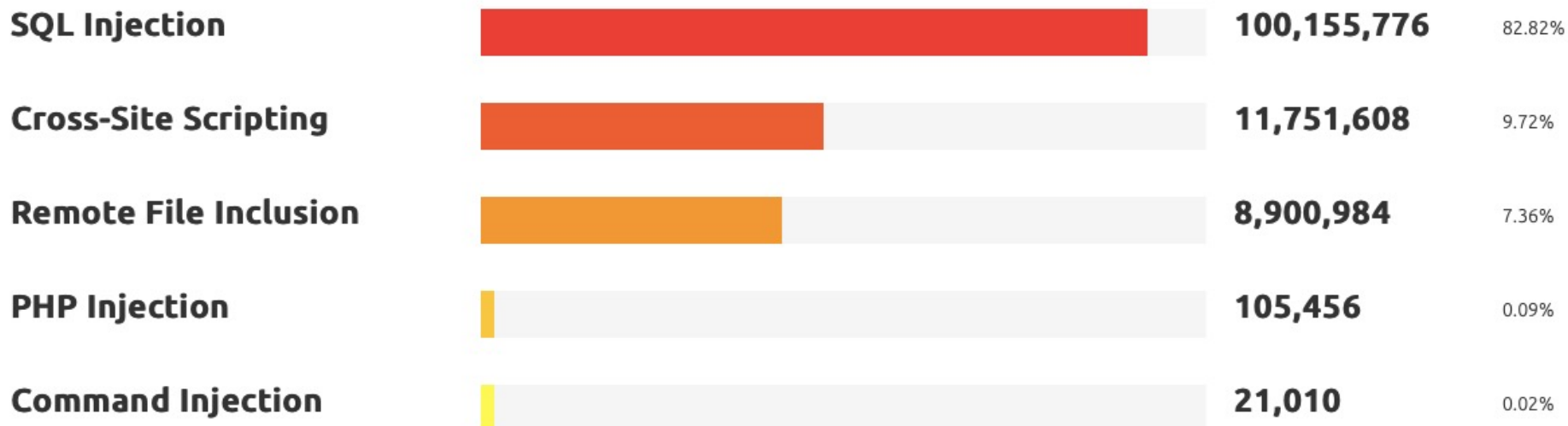🇷🇺 **Russian Federation**

34,101,558 Attacks Sent

**Attack Vector Frequency**

**SQL Injection**

100,155,776 Attacks Observed

**Attack Distribution by Type**

During the reporting period, what was the distribution of the most common web attack types?

| Attack Type | | Count | Percentage |
|---|---|---|---|
| **SQL Injection** | ▬▬▬▬▬▬ | 100,155,776 | 82.82% |
| **Cross-Site Scripting** | ▬▬ | 11,751,608 | 9.72% |
| **Remote File Inclusion** | ▬ | 8,900,984 | 7.36% |
| **PHP Injection** | ▌ | 105,456 | 0.09% |
| **Command Injection** | ▌ | 21,010 | 0.02% |

# Cyber Attacks… Not a Rare News!

# India is one of top 10 most attacked country!!!

# On-going Threat Maps

- Ongoing threats maps - top targeted countries, industries, malware, daily attacks etc.

    http://threatmap.checkpoint.com


    https://cybermap.Kaspersky.com

# Computer Security

- Computer security is protection of items or ASSETS of a computer or computer system

- ASSETS are of following types:
  - **Hardware:** Computers, Devices (disk drives, memory cards, printers etc), Networks
  - **Software:** Operating system, utilities, commercial applications (MS-Office, Oracle apps, SAP etc), individual applications
  - **Data:** Documents, photos, emails, projects, corporate data etc

- ASSETS have a value to an individual
  - Has an owner or user perspective
  - May be monetary or non-monetary
  - Is personal, time dependent & often imprecise

- ASSETS are target for an attack and require security protection

# Vulnerability – Threat - Control Paradigm

- '**Vulnerability**' is a weakness in the system that might be exploited to cause loss or harm

- '**Threat**' is a set of circumstances that has a potential to cause loss or harm to system

- A person who exploits the vulnerability perpetrates an '**Attack**'

- '**Control**' is an action, device, procedure of technique that removes or reduces the vulnerability

# Example: Vulnerability - Threat - Control
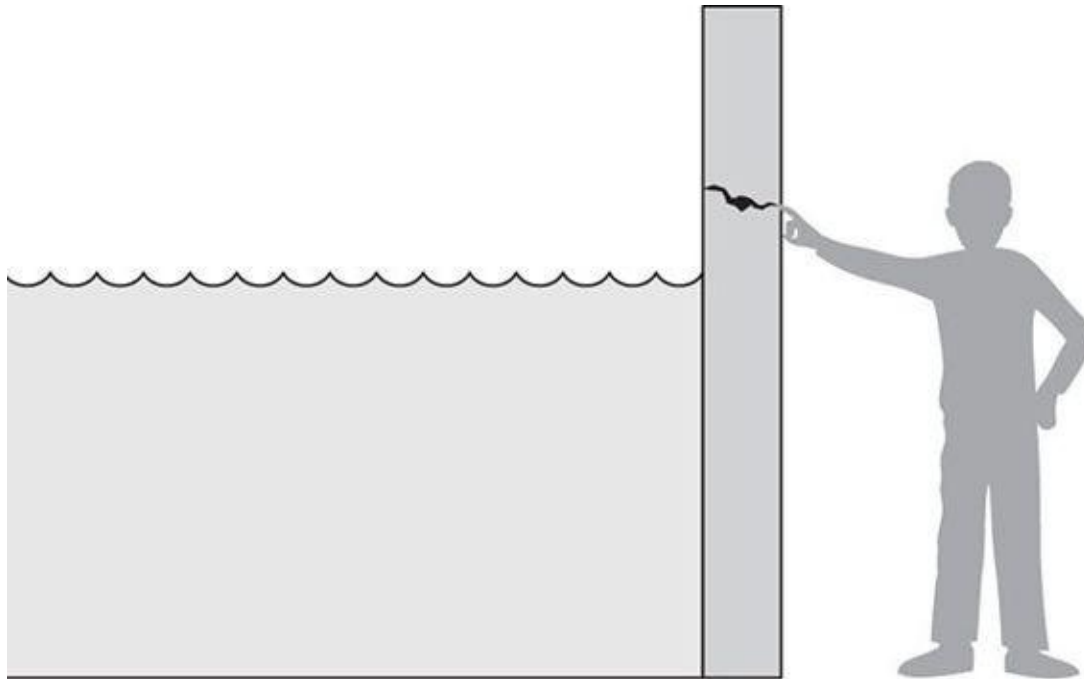


- **Vulnerability:** Crack in the wall
- **Threat:** Rising water level
- **Attack:** Someone pumping more water
- **Control:** Fill the gap, strengthen the wall

# Security Triad - CIA

- **Confidentiality:** Ability of a system to ensure that an asset is viewed by only authorized parties
- **Integrity:** Ability of a system to ensure that an asset is modified by only authorized parties
- **Availability:** Ability of a system to ensure that an asset can be used by any authorized parties
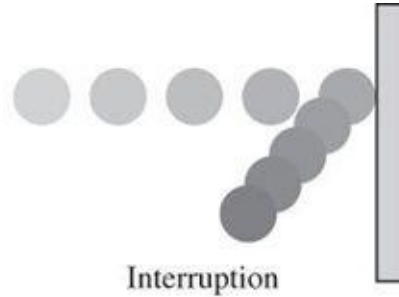
## Additional two properties:

- **Authentication:** Ability of a system to validate the identity of a sender
- **Non-repudiation or Accountability:** Ability of a system to confirm that a sender can not convincingly deny having sent something
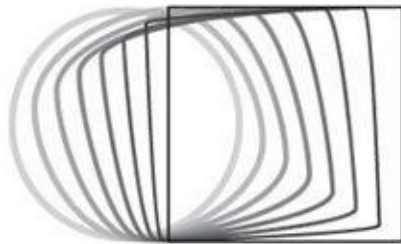
# Acts of Harm
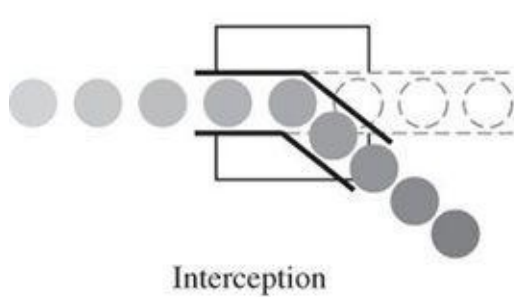
Interception

Interruption

Modification

Fabrication

**Interception:** Confidentiality lost

**Interruption:** Availability lost

**Modification:** Integrity lost

**Fabrication:** Integrity lost

# Security Threats
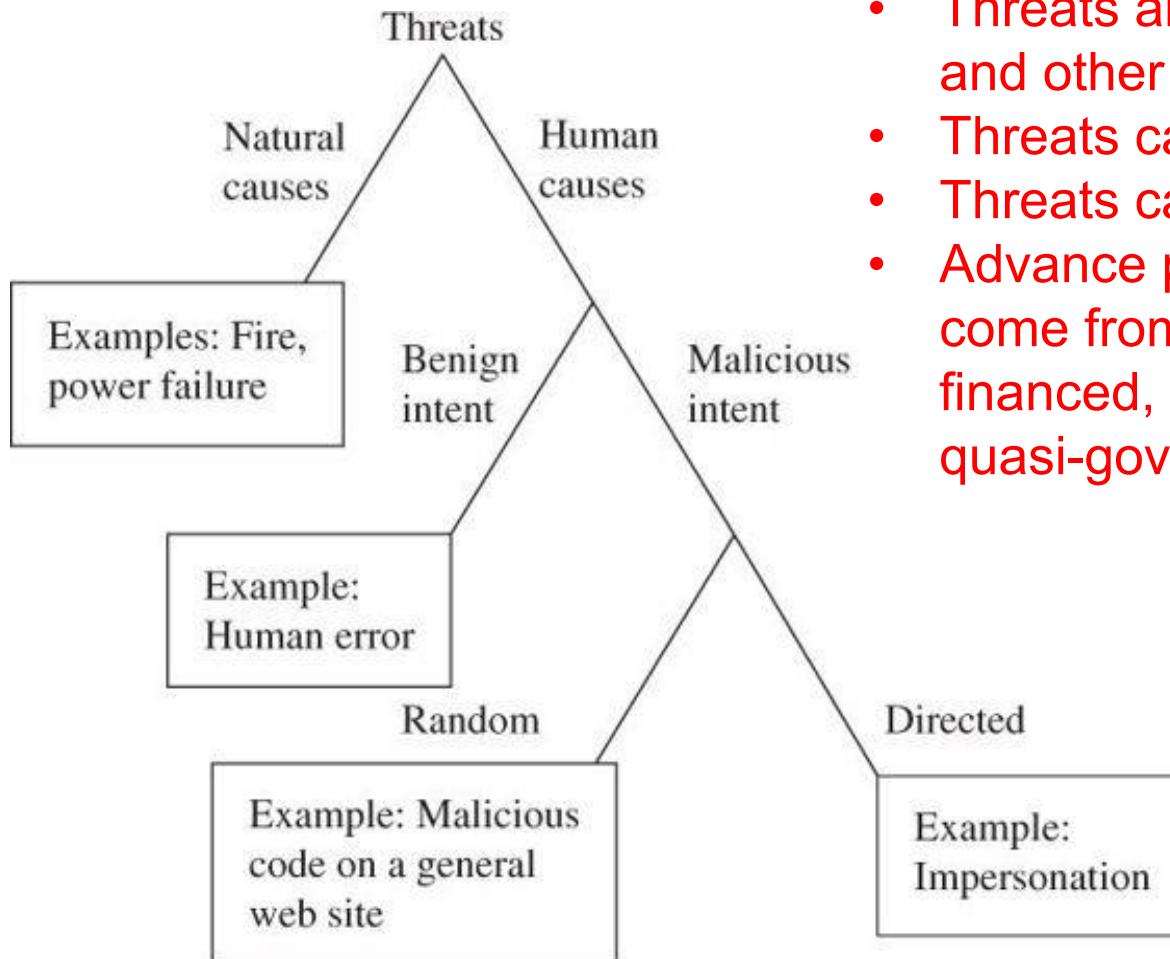
- Threats are caused both by human and other sources
- Threats can be malicious or not
- Threats can be random or targeted
- Advance persistent threat attacks come from organized, well financed, patient and often govt or quasi-govt affiliated groups

# Security Threats

# Who are the Attackers?

- Individual
- **Hackers**
- Terrorist
- Criminal for hire
- Loosely connected group
- Organized crime member
  - cyber crime is lucrative
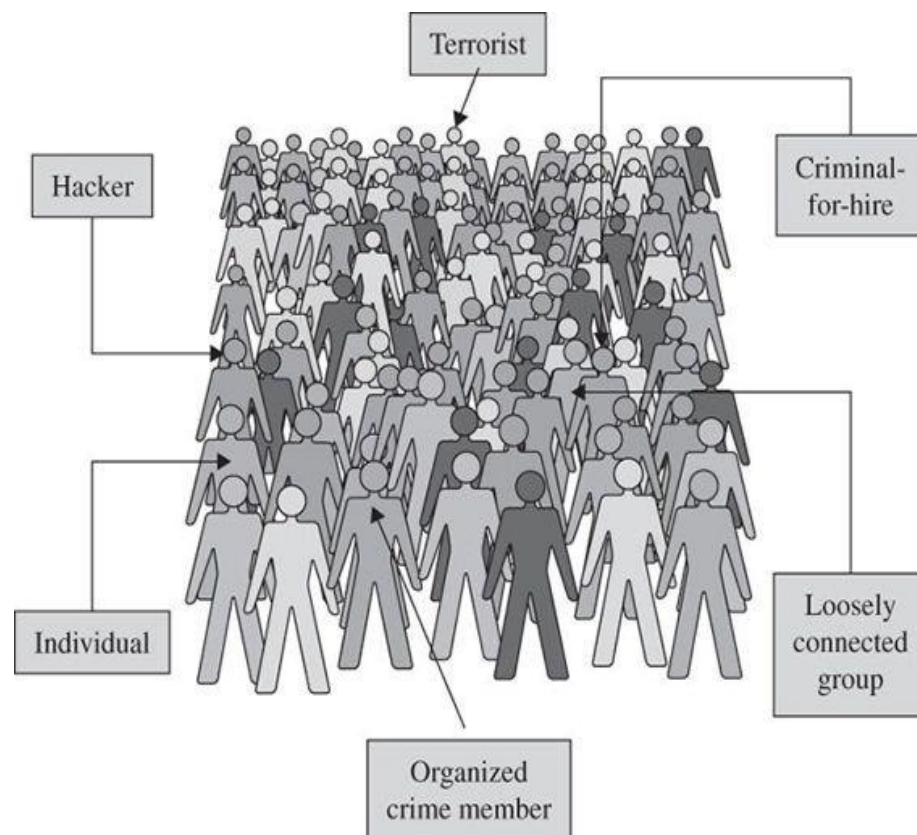
# Hacking

- Act committed toward breaking into a computer and/or network

- Hacking is any technical effort to manipulate the normal behavior of network connections and connected systems

- A hacker is any person engaged in hacking

- Purpose
  - Financial
  - Power
  - Publicity
  - Revenge
  - Adventure
  - Desire to access forbidden information
  - Destructive mindset

# History of Hacking

- The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems.

- MIT engineers in the 1950s and 1960s first popularized the term and concept of hacking.

- The so-called "hacks" perpetrated by these hackers were intended to be harmless technical experiments and fun learning activities.

- Later others began applying the term to less honorable pursuits.
  - For example, hackers in US experimented with methods to modify telephones for making free long-distance calls over the phone network illegally.

- As computer networking and the Internet exploded in popularity, data networks became by far the most common target of hacking.

# Hacker Types…

- **White Hat:** White hats are ethical hackers.
    - They use their knowledge and skill to thwart the black hats and secure the integrity of computer systems or networks.
    - They use hacking to identify vulnerabilities and inform the owners of systems so that the vulnerabilities can be plugged-in.
    - If a black hat decides to target you, it's a great thing to have a white hat around.

- **Black Hat:** These are the bad guys. A black hat is a cracker and usage hacking with malicious intent
    - Black hats may also share information about the "break in" with other black hat crackers so they can exploit the same vulnerabilities before the victim becomes aware and takes appropriate measures.

# Hacker Types…

- **Gray Hat –** A gray hat is a bit of both a white hat and a black hat.
    - Their main objective is not to do damage to a system or network, but to expose flaws in system security.
    - The black hat part of the mix is that they may very well use illegal means to gain access to the targeted system or network, but not for the purpose of damaging or destroying data:
    - They want to expose the security weaknesses of a particular system and then notify the "victim" of their success.
    - Often this is done with the intent of then selling their services to help correct the security failure so black hats can not gain entry and/or access for more devious and harmful purposes.

# Vulnerabilities Exploited by Hackers

- Systems with inadequate border protection

- Systems with weak authentication credentials

- Systems with out of date patching

- Remote Access Servers (RASs) with weak access controls.

- Applications with known vulnerabilities

- Open source applications with no protection

- Poorly protected data and websites

- Mis-configured or default configured systems

# Examples of Hacking

- One of the biggest examples is Stuxnet - a virus attack on the Nuclear program of Iran, which is suspected to be carried out jointly by USA and Israel.

- Some of the other victims of hacking are organizations such as:
  - Adobe hack: 2013
  - Yahoo Hack: 2013
  - eBay hack: 2014
  - Sony hack: 2014
  - Mariott hack: 2018
  - Dubsmash hack: 2019
  - ….

# What is Ethical Hacking?

- Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data.

- Ethical hack involves duplicating strategies and actions of malicious attackers.

  – Helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

- Ethical hackers ("white hats") are security experts that perform these assessments.

  – The proactive work they do helps to improve an organization's security posture.

  – With prior approval from the organization or owner of the IT asset, the mission of ethical hacking is opposite from malicious hacking.

# Key Concepts of Ethical Hacking

- Ethical Hacking follows four key protocol concepts:
  - **Stay legal**. Obtain proper approval before accessing and performing a security assessment.
  - **Define the scope**. Determine the scope of the assessment so that the ethical hacker's work remains legal and within the organization's approved boundaries.
  - **Report vulnerabilities**. Notify the organization of all vulnerabilities discovered during the assessment. Provide remediation advice for resolving these vulnerabilities.
  - **Respect data sensitivity**. Depending on the data sensitivity, ethical hackers may have to agree to a non-disclosure agreement, in addition to other terms and conditions required by the assessed organization.

# Ethical Hackers v/s Malicious Hackers

- Ethical hackers:
  - Use their knowledge to secure and improve the technology of organizations.
  - They provide an essential service to these organizations by looking for vulnerabilities that can lead to a security breach.
  - An ethical hacker reports the identified vulnerabilities to the organization. Additionally, they provide remediation advice.
  - With the organization's consent, the ethical hacker performs a re-test to ensure the vulnerabilities are fully resolved.

- Malicious hackers:
  - Intend to gain unauthorized access to a resource (the more sensitive the better) for financial gain or personal recognition.
  - Deface websites or crash backend servers for fun, reputation damage, or to cause financial loss.
  - The methods used and vulnerabilities found remain unreported.
  - They aren't concerned with improving the organizations security posture.

# Skills for Ethical Hacking

- Overall require a wide range of computer skills.
- All ethical hackers should have:
  - Expertise in scripting languages.
  - Proficiency in operating systems.
  - A thorough knowledge of networking.
  - A solid foundation in the principles of information security.
  - specialize to be subject matter experts (SME) on a particular area within the ethical hacking domain

# What Problems does Hacking Identify?

- Ethical hacking aims to mimic an attacker and looks for attack vectors against the target.

- Once the ethical hacker gathers enough information, they use it to look for vulnerabilities against the asset.

- As next step, ethical hackers use exploits against the vulnerabilities to demonstrate how a malicious attacker could exploit it.

- Some of the common vulnerabilities discovered by ethical hackers include:
  - Injection attacks
  - Broken authentication
  - Security misconfigurations
  - Use of components with known vulnerabilities
  - Sensitive data exposure

- After the testing, ethical hackers prepare a detailed report. This includes steps to compromise the identified vulnerabilities and steps to patch/mitigate the same.

# Key Limitations of Ethical Hacking

- **Limited scope:**
  - Ethical hackers cannot progress beyond a defined scope to make an attack successful.
  - However, it's not unreasonable to discuss out of scope attack potential with the organization.

- **Resource constraints:**
  - Time constraints - limited.
  - Computing power and budget constraints.

- **Restricted methods:**
  - Some organizations ask experts to avoid test cases that lead the servers to crash (i.e. Denial of Service - DDoS attacks).

# Cyber Attack Lifecycle (Kill Chain)

| Cyber Attack Lifecycle | Recon | | Deliver | | Control | | Maintain |
|---|---|---|---|---|---|---|---|
| | Weaponize | | | Exploit | | Execute | |
| Defense Action | Proactive Detection Mitigation | | | | Incidence Response and Mission Assurance | | |
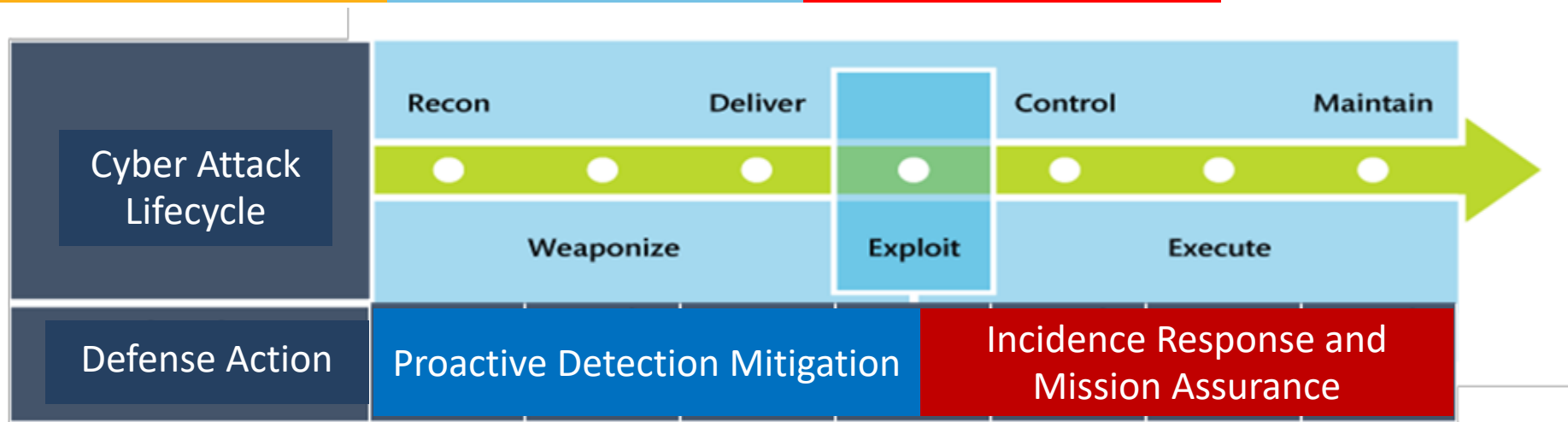
The cyber attack lifecycle, first articulated by Lockheed Martin as the "kill chain," depicts the phases of a cyber attack:

- **Recon**—the adversary develops a target;
- **Weaponize**—the attack is put in a form to be executed on the victim's computer/network;
- **Deliver**—the means by which the vulnerability is weaponized;
- **Exploit**—the initial attack on target is executed;
- **Control**—mechanisms are employed to manage the initial victims;
- **Execute**—leveraging numerous techniques, the adversary executes the plan;
- **Maintain**—long-term access is achieved.

# Cyber Attack Lifecycle

| Stage | Description |
|---|---|
| Reconnaissance | • Harvest email addresses, company information, etc. |
| Weaponization | • Couple exploit with backdoor into deliverable payload |
| Delivery | • Deliver weaponized bundle to the victim via email, web, usb, etc. |
| Exploitation | • Exploit vulnerability to execute code on victim system |
| Installation | • Install malware on the asset |
| Command & Control | • Command channel for remote manipulation of victim |
| Actions on Objectives | • With "Hands on Keyboard" access, intruders accomplish their original goal |

Source: Lockheed Martin Cyber Kill Chain

ercot

# What is OWASP?

- Open Web Application Security Project (OWASP) is a non-profit foundation that works to improve the security of software.

- OWASP programs include:
  - Community-led open source software projects
  - Over 275 local chapters worldwide
  - Tens of thousands of members
  - Industry-leading educational and training conferences

- OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted.

- OWASP projects, tools, documents, forums, and chapters are free and open to anyone interested in improving application security.

- OWASP Foundation was launched on December 1st, 2001 and incorporated as a United States non-profit charity on April 21, 2004.

# What is OWASP Top 10?

- OWASP Top 10 is an online document on OWASP's website that provides ranking of and remediation guidance for the top 10 most critical web application security risks.

- The risks are ranked and based on the frequency of discovered security defects, the severity of the vulnerabilities, and the magnitude of their potential impacts.

- This is to enable them to incorporate the report's findings and recommendations into their security practices, thereby minimizing the presence of these known risks in their applications

# OWASP Top 10

- **Injection:** Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query.

- **Broken Authentication:** Incorrect implementation of authentication and session management functions, allowing attackers to compromise passwords, keys, or session tokens etc.

- **Sensitive Data Exposure:** Inadequate protection of sensitive data, such as financial, healthcare, and PII, by web applications and APIs.

- **XML External Entities (XXE):** Older or poorly configured XML processors evaluate external entity references within XML documents.

- **Broken Access Control:** Poor enforcement of restrictions on what authenticated users are allowed to do.

- **Security Misconfiguration:** A result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information.

# OWASP Top 10…

- **Cross-Site Scripting XSS:** XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript.

- **Insecure Deserialization:** Insecure deserialization often leads to remote code execution.

- **Using Components with Known Vulnerabilities:** Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application.

- **Insufficient Logging & Monitoring:** Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data.

# It Takes Time to Become a Hacker

- This class alone won't make you a hacker, or an expert
  - It might make you a script kiddie
- It usually takes years of study and experience to earn respect in the hacker community
- It's a hobby, a lifestyle, and an attitude
  - A drive to figure out how things work

# What You Can Do Legally?

- Laws involving technology change as rapidly as technology itself

- Find what is legal for you locally

    - Laws change from place to place

- Be aware of what is allowed and what is not allowed

- Governments are getting more serious about punishment for cybercrimes

# What You Cannot Do Legally?

- Accessing a computer without permission is illegal

- Other illegal actions

  - Installing worms or viruses

  - Denial of Service attacks

  - Denying users access to network resources

- Be careful your actions do not prevent customers from doing their jobs

# Get It in Writing

- Using a contract is just good business

- Contracts may be useful in court

- Internet can also be a useful resource

- Have an attorney read over your contract before sending or signing it

# Tools we will use

| S.No. | Toool Name | Use |
|-------|------------|-----|
| 1 | Wireshark | Network analyser |
| 2 | Burpsuite | Analyse and exploit vulnerabilities |
| 3 | ZAP (Zed Attack Proxy) | Analyse and exploit vulnerabilities |
| 4 | Metasploit | Framework of security tools |
| 5 | Maltego | Eveny analyser |
| 6 | Hydra | Password cracker |
| 7 | Aircrack | WEP & WPA password cracker |
| 8 | John the Ripper | Password cracker |
| 9 | SQLMap | SQL injection tool |
| 10 | Nmap | Network analyser, port scanner |

# Useful Sites

- OWASP

  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- Symantec

  http://www.symantec.com/security_response/publications/threatreport.jsp

- Akmai

  https://www.stateoftheinternet.com/

- Hacker news

  https://thehackernews.com

# Thank You