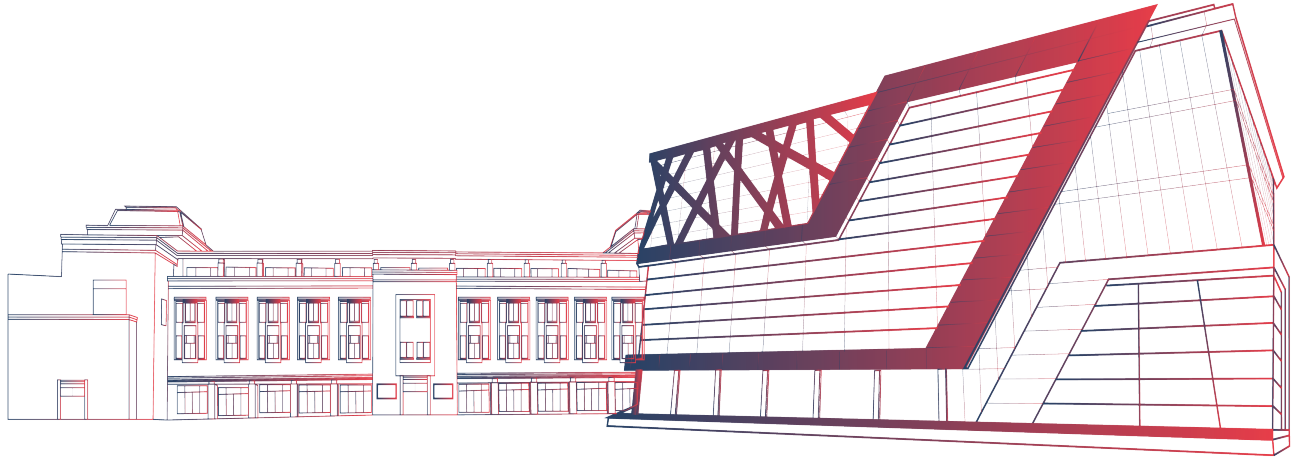
THE NORTHCAP UNIVERSITY

Introduction to VAPT

Vulnerability Assessment & Penetration Testing



30 YEARS OF EXCELLENCE

NAAC Accredited

Vulnerability Assessment and Penetration Testing (VAPT)

THE NORTHCAP UNIVERSITY

V --> Vulnerability :

- The LOOPHOLES ,security misconfigurations which can cause an attacker to get inside a network or website or ways which help an attacker to intrude in the systems.

A --> Assessment :

- Analysing the vulnerability and scanning the vulnerability onto how much it could cause damage to the victim.

P --> Penetration:

- When you get the vulnerability and is accessed, a report is generated and through that further exploitation or intrusion is done this is known as penetration .

T --> Testing:

- When a person is penetrating it requires several procedures or attacks to penetrate this is done through this testing phase.

30 YEARS OF EXCELLENCE

NAAC Accredited

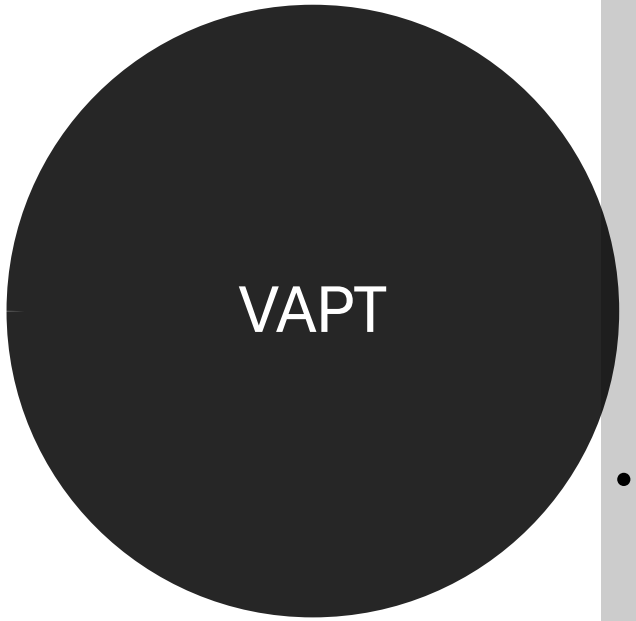
THE NORTHCAP UNIVERSITY

VAPT (Vulnerability Assessment Penetration Testing)

- VAPT Service is the combination of two different Security Services one is **Vulnerability Assessment** (VA) & **Penetration Testing** (PT).
- The tests have different powers and are often shared to achieve a more complete vulnerability analysis.
- Both Services have their own area for securing your network & application.

30 YEARS OF EXCELLENCE

NAAC Accredited



• Vulnerability Assessment	• Penetration Test
• **Vulnerability Assessment** Tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to cause damage and those that cannot.	• **Penetration tests** find exploitable flaws and measure the severity of each. Penetration tests attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application.
• Vulnerability scanners alert companies to the pre-existing flaws in their code and where they are located.	• A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system.

- Together, Vulnerability Assessment and Penetration Testing Tools provide a detailed picture of the flaws that exist in an application and the risks associated with those flaws.

VA vs PT

	Vulnerability Scan	Penetration Test
Refining Definitions...	Also known as a "vulnerability assessment," vulnerability scanning involves automated tools that scan for systematic vulnerabilities (loopholes) on a system, network, or application.	Also known as a "pentest" or "ethical hacking," penetration testing is a manual technical test that goes beyond vulnerability scanning. The test identifies vulnerabilities (loopholes) on a system, network, or an application, and subsequently attempts to exploit those vulnerabilities.
Common Methodology...	During a vulnerability scan, scan engines (e.g. Nessus, Nexpose) are used to gather meaningful information. From an attacker perspective, finding a vulnerability is like finding an open-door to a very secure building From a security team perspective, finding a vulnerability provides an opportunity to close that open-door and secure the building.	During a pentest, a mixture of automated tools and manual exploitation techniques are used by the pentester. Automated tools (e.g. Nmap) include basic network discovery, vulnerability scan engines (e.g. Nessus, Nexpose), and exploitation frameworks (e.g. Metasploit). Manual exploitation requires the pentester to gather and interpret the findings from the automated tools to break into a system, a network, or an application. It also involves manual searching for vulnerabilities that automated scanners miss.
Key Differences...	A vulnerability scan is different from a pentest in that it only discovers known vulnerabilities; it does not attempt to exploit a vulnerability but instead only confirms the possible existence of a vulnerability.	During penetration testing, a pentester will attempt to exploit those vulnerabilities to verify its existence. In the real-world, exploiting vulnerabilities by an attacker could be as simple as stealing contents from a database server, traffic sniffing on an internal network, or compromising a web application.

Pro of VA PT

THE NORTHCAP UNIVERSITY

Provides enterprises with a **more comprehensive application evaluation** than any single test alone.

Gives an organization a **more detailed view** of the threats facing its applications, to protect from malicious attacks.

Helps **identify programming errors**

Provides a **methodical approach** to risk management

30 YEARS OF EXCELLENCE

NAAC Accredited

Why are systems vulnerable?

Network misconfiguration

THE NORTHCAP UNIVERSITY

Devices such as **routers, switches and servers**, as well as **firewalls and IPS systems** are either misconfigured

In Some cases, not configured at all, thus running default settings.

- As an example, almost all firewalls have a **default built-in user account with the name,'admin'**.
- Typically, the **password for it is also set to 'admin,'** by default, or something even easier to guess.

30 YEARS OF EXCELLENCE

NAAC Accredited

Incorrect programming & practices

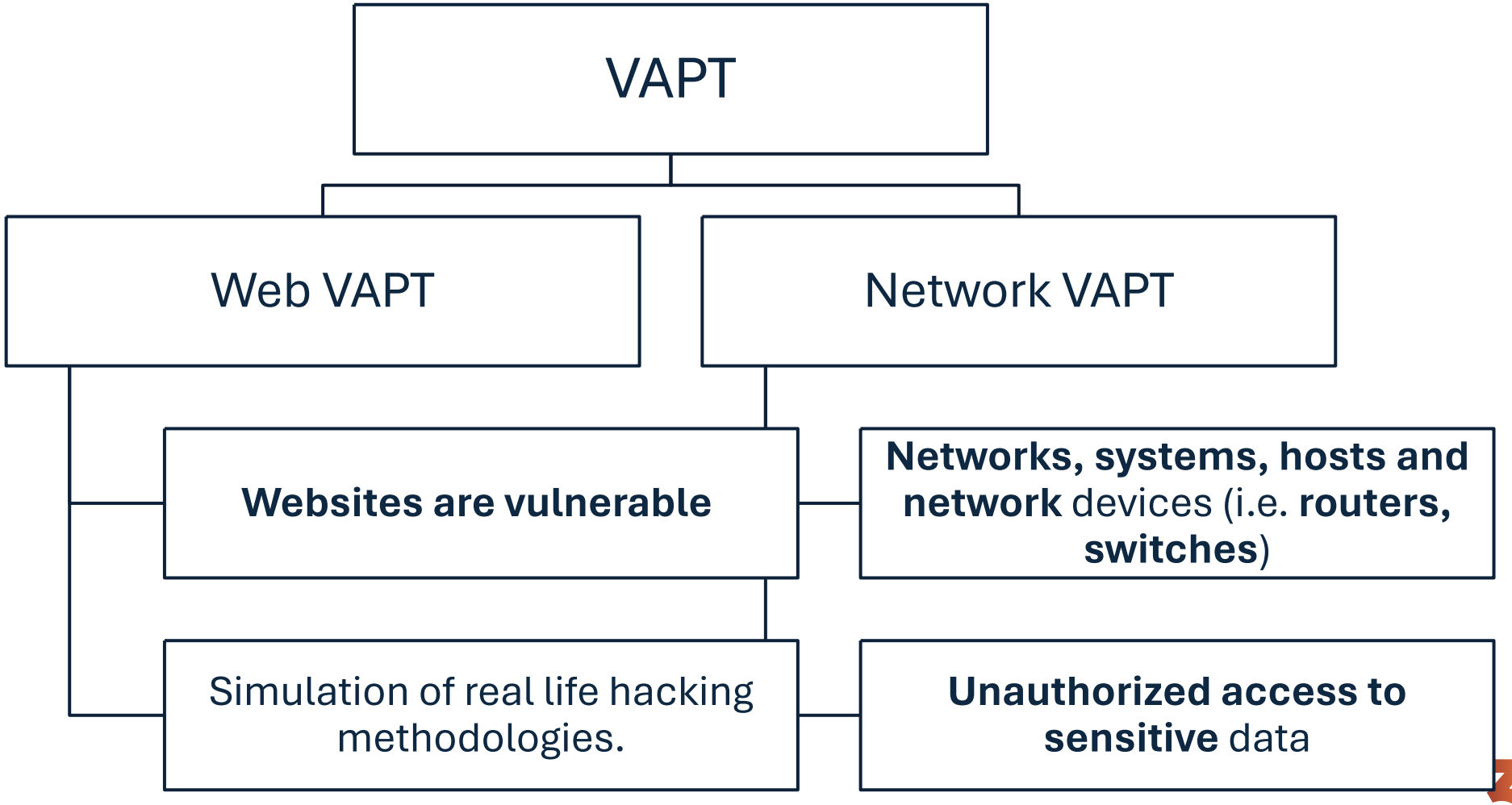
User input taken from a Web application form may be directly sent to a backend database server without parsing it.

- e.g. Can lead to a parameter manipulation attack or SQL injection attack.

E.g. of programming errors would be a Web service accepting requests **without performing adequate authentication**

Human error

VAPT


VAPT
Web VAPT
Network VAPT
Websites are vulnerable
Networks, systems, hosts and network devices (i.e. routers, switches)
Simulation of real life hacking methodologies.
Unauthorized access to sensitive data

Exploit Categories

Web server exploits

Web service exploits

Authentication problems

Configuration problems

Database related problems

Scripting related problems

Case Study

- **Google Search-** BJP website got hacked before elections as VPN credentials were floated online by one minister which were used for hacking website later by attackers

- https://www.saddahaq.com/after-advanis-website-gets-hacked-bjp-blocks-its-website-access-in-pakistan

‘Be Back Soon’: BJP Website Down After Being Allegedly Hacked

The Quint

Published on March 05 2019, 1:16 PM
Last Updated on March 06 2019, 10:27 PM

The official website of the Bharatiya Janata Party (BJP) – http://www.bjp.org/– was taken d

10 organisations monitoring intercepting on internet in India 2019

THE NORTHCAP UNIVERSITY

10 central agencies can now snoop on "any" computer they want

Security agencies can now monitor any information generated, transmitted or received in any computer.

ET Online and Agencies | Updated: Dec 21, 2018, 01.30 PM IST

Agencies

The notification says the subscriber or service provider or any person in charge of the computer resource will have to extend all facilities and technical assistance to the agencies, else they can be fined and even imprisoned for up to seven years.

In a decision with wide ramifications, the government has allowed 10 intelligence and investigating agencies and the Delhi Police to intercept, monitor and decrypt "any information" generated, transmitted, received or stored in "any computer", an action that has come under attack from opposition parties.

The ministry has vested the authority on the agencies under Section 69 of the Information Technology Act, 2000 and Rule 4 of the Information Technology Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

The ten agencies authorized to intercept or request access to user data under the new order are:

- the Intelligence Bureau
- the Narcotics Control Bureau
- the Enforcement Directorate
- the Central Board of Direct Taxes
- the Directorate of Revenue Intelligence
- the Central Bureau of Investigation
- the National Investigation Agency
- the Cabinet Secretariat (R&AW)
- the Commissioner of Delhi Police, and
- the Directorate of Signal Intelligence (for service areas of J and Assam only)

30 YEARS OF EXCELLENCE

NAAC Accredited

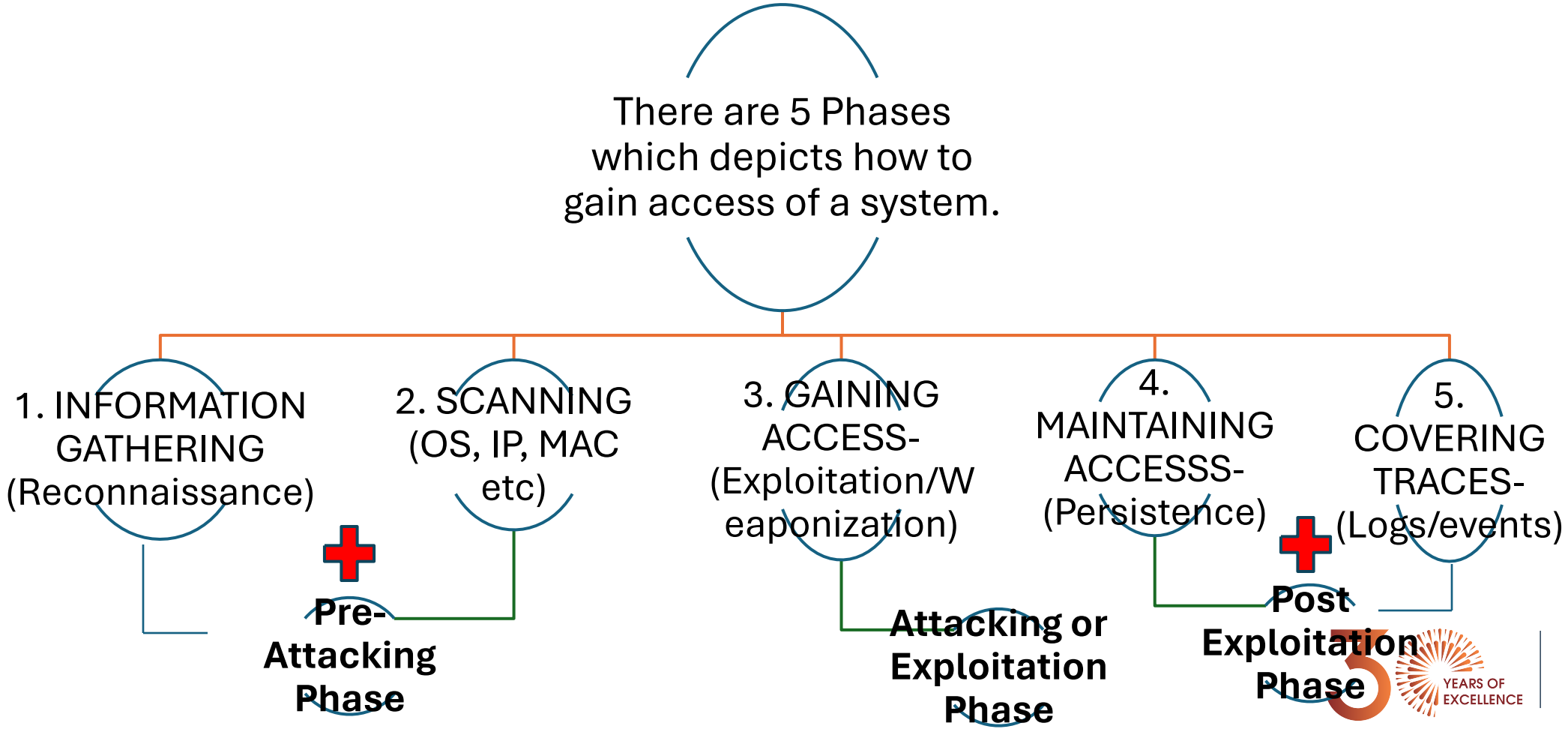
THE NORTHCAP UNIVERSITY

PENETRATION TESTING

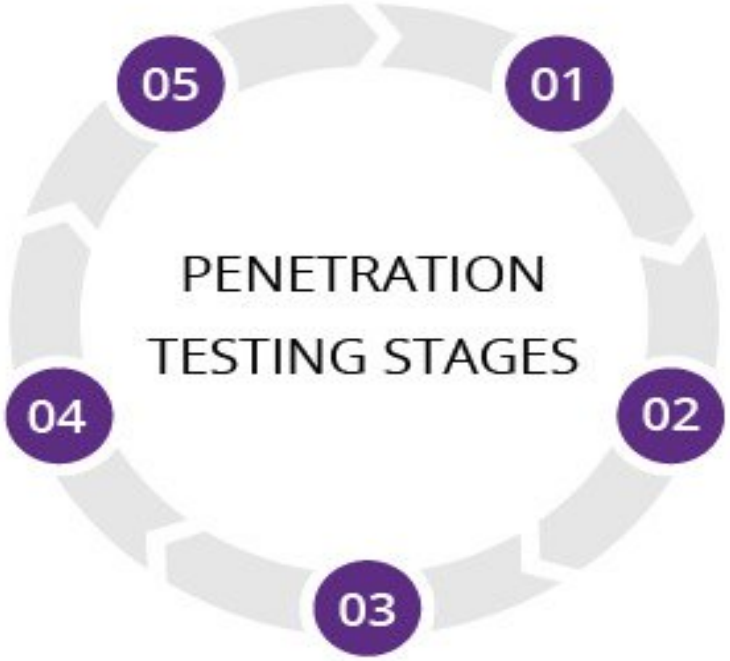
30 YEARS OF EXCELLENCE

NAAC Accredited

5 phases of Penetration Testing



PenTesting



Analysis and WAF configuration

Results are used to configure WAF settings before testing is run again.

Planning and reconnaissance

Test goals are defined and intelligence is gathered.

Maintaining access

APTs are imitated to see if a vulnerability can be used to maintain access.

Scanning

Scanning tools are used to understand how a target responds to intrusions.

Gaining access

Web application attacks are staged to uncover a target's vulnerabilities.

Types of Penetration Testing

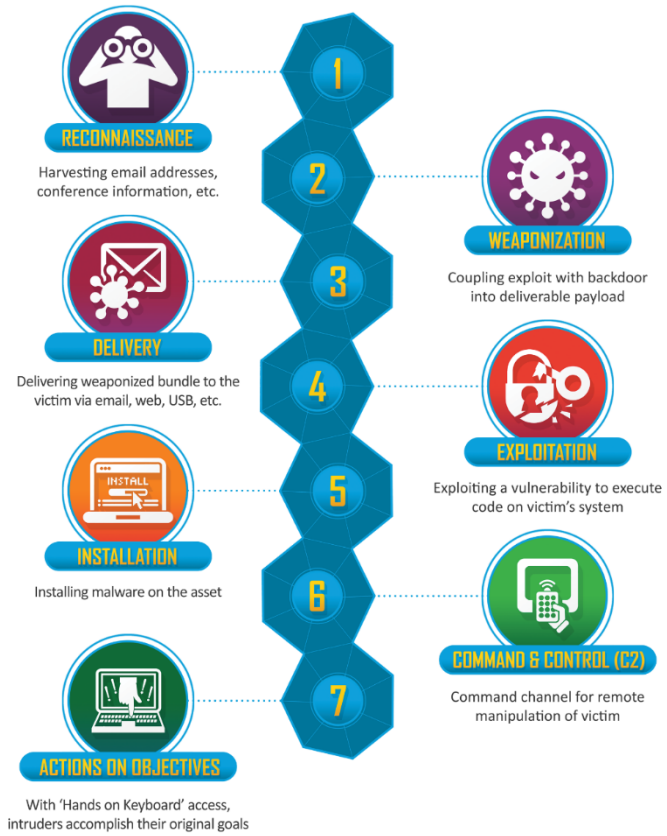
The types of penetration testing **can vary depending on the technology**.

Here are some of the **common types of pen testing:**

- **Network Testing**
- **Mobile Application Testing**
- **Web Application Testing**
- **Cloud Testing**
- **Social Engineering Testing**

Even though each area of penetration testing **have differing tool sets**,

They **share a common methodology**



THE

THE CYBER KILL CHAIN®

ed Martin, **the Cyber Kill Chain®** framework is part of the **Intelligence Driven Defense®** model for identification and p
what the adversaries must complete in order to achieve their objective.

Cyber Kill Chain® enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, tec

Advanced

oordinated, Purposeful

P: Persistent

Month after Month, Year after Year

Person(s) with

https://www.youtube.com/watch?v=zhClg4cLemc&feature=emb_logo

30 YEARS OF EXCELLENCE

NAAC Accredited

Cyber Kill Chain

- Lockheed Martin derived the kill chain framework from a military model – originally established to identify, prepare to attack, engage, and destroy the target. Since its inception, the kill chain has evolved to better anticipate and recognize insider threats, social engineering, advanced ransomware and innovative attacks.

How the Cyber Kill Chain Works

- There are several core stages in the cyber kill chain. They range from reconnaissance (often the first stage in a malware attack) to lateral movement (moving laterally throughout the network to get access to more data) to data exfiltration (getting the data out). All of your common attack vectors – whether phishing or brute force or the latest strain of malware – trigger activity on the cyber kill chain.

Stages of Kill Chain

- **Reconnaissance**
  The observation stage: attackers typically assess the situation from the outside-in, in order to identify both targets and tactics for the attack.
- **Intrusion**
  Based on what the attackers discovered in the reconnaissance phase, they're able to get into your systems: often leveraging malware or security vulnerabilities.
- **Exploitation**
  The act of exploiting vulnerabilities, and delivering malicious code onto the system, in order to get a better foothold.
- **Privilege Escalation**
  Attackers often need more privileges on a system to get access to more data and permissions: for this, they need to escalate their privileges often to an Admin.
- **Lateral Movement**
  Once they're in the system, attackers can move laterally to other systems and accounts in order to gain more leverage: whether that's higher permissions, more data, or greater access to systems.
- **Obfuscation / Anti-forensics**
  In order to successfully pull off a cyberattack, attackers need to cover their tracks, and in this stage they often lay false trails, compromise data, and clear logs to confuse and/or slow down any forensics team.
- **Denial of Service**
  Disruption of normal access for users and systems, in order to stop the attack from being monitored, tracked, or blocked
- **Exfiltration**
  The extraction stage: getting data out of the compromised system.

Case Study

- Attacker took .3 roubles from per user/month. Total users were 14.7 million
- Total sum per day was 0.3x14.7 millions
- Total salary per month =50 millions
- Bank got to know after 1.6 years
- Bank thought s/w glitch, then matched accounts on paper, it took time.
- Attacker arrested after 3-4months later bank employed attacker and offered job of CISO highest position (22LPA)
- Chief information security officer

NIST (National Institute of Standards and Technology)

- *NIST implements practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the U.S. to adopt cybersecurity capabilities.*

(https://www.nist.gov/topics/cybersecurity)

1805 profiles for jobs