IT3789 Cyber Security Attack & Defence

L2 – Attacks & Defenses

NANYANG POLYTECHNIC

WITH KNOWLEDGE COMES RESPONSIBILITY

Attacks & Defenses

Overview

Types of Attack

Phases of an Attack

Countermeasures

Goal of Penetration Testers

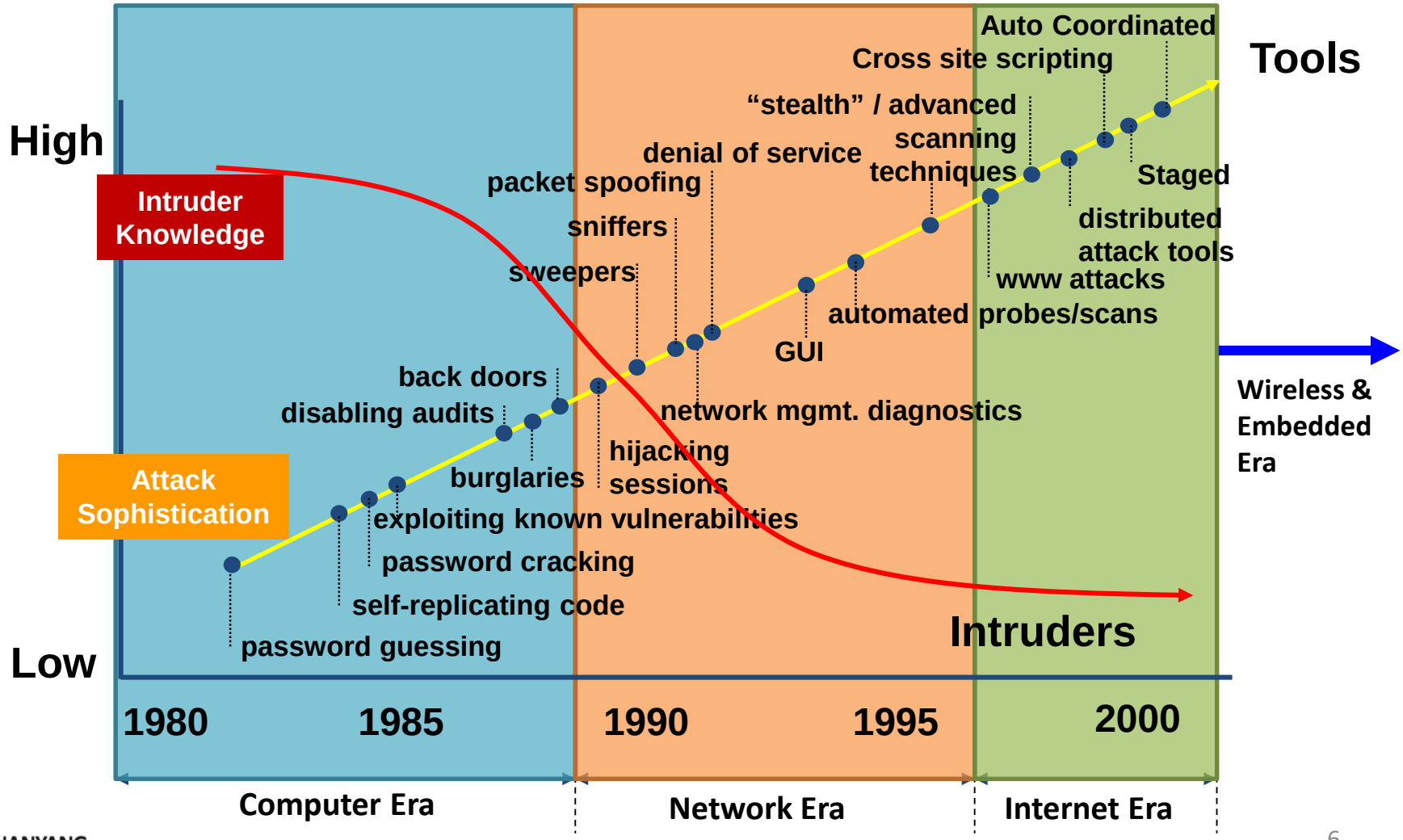
- Understand how to perform an attack in order to find out how vulnerable targeted systems are.
- ULTIMATE AIM: Protect systems from hackers.

NOT TO GAIN UNAUTHORIZED ACCESS TO MACHINES!

Motivation of Hacking

- Recognition
  - When a new vulnerability is discovered, the person who discovers it would report about it in the mailing list (e.g. Bugtraq).
- Admiration
  - Some hackers learn to hack because they admire a hacker.
- Curiosity
  - Many hackers cite curiosity as the primary motivation to hack, as they spend lots of time to hack, and give details of the findings.
- Power and gain
  - Some hackers exploit their skills for illegal wire transfers, or selling stolen secrets to unfriendly governments.
- Revenge
  - A person might feel wronged, and seek revenge by getting professionals to hack, e.g. steal a password to an email account.

Attack Sophistication vs Intruder Technical Knowledge



Source : Carnegie Mellon University

Exploiting Weaknesses

- Most hacking tools exploit vulnerabilities in one of the following 4 areas.
  - Operating Systems
    - Install OS with default settings resulting in potential vulnerabilities that are not patched.
  - Applications
    - Most application development is feature-driven with a given deadline.
    - Not tested thoroughly for vulnerabilities.
  - Shrink-Wrap code
    - Off-the-shelf programs come with extra features.
    - Sometimes, these features are exploitable.
    - e.g. Attacker can execute programs through a macro in Microsoft Word.
  - Misconfigurations
    - Many vulnerabilities occur as a result of misconfigurations by system administrators.
    - e.g. App server configurations allows stack traces to be returned to users.

Attacks & Defenses

Overview

Types of Attack

Phases of an Attack

Countermeasures

Types of Attack

- Active attacks
  - Manipulates the target system.
  - Violates confidentiality, integrity and availability and authentication.
  - e.g. Altering configuration to start service.
- Passive attacks
  - Does not modify anything on target system.
  - Focus on getting information.
  - Usually violates confidentiality.
  - e.g. Sniffing packets.

Types of Attack

- Inside attacks
  - Originate from within the organization.
  - Insider trying to gain access to restricted resources.
- Outside attacks
  - Originate from Internet or remote access connection (i.e. outside the organization).

Attacks & Defenses

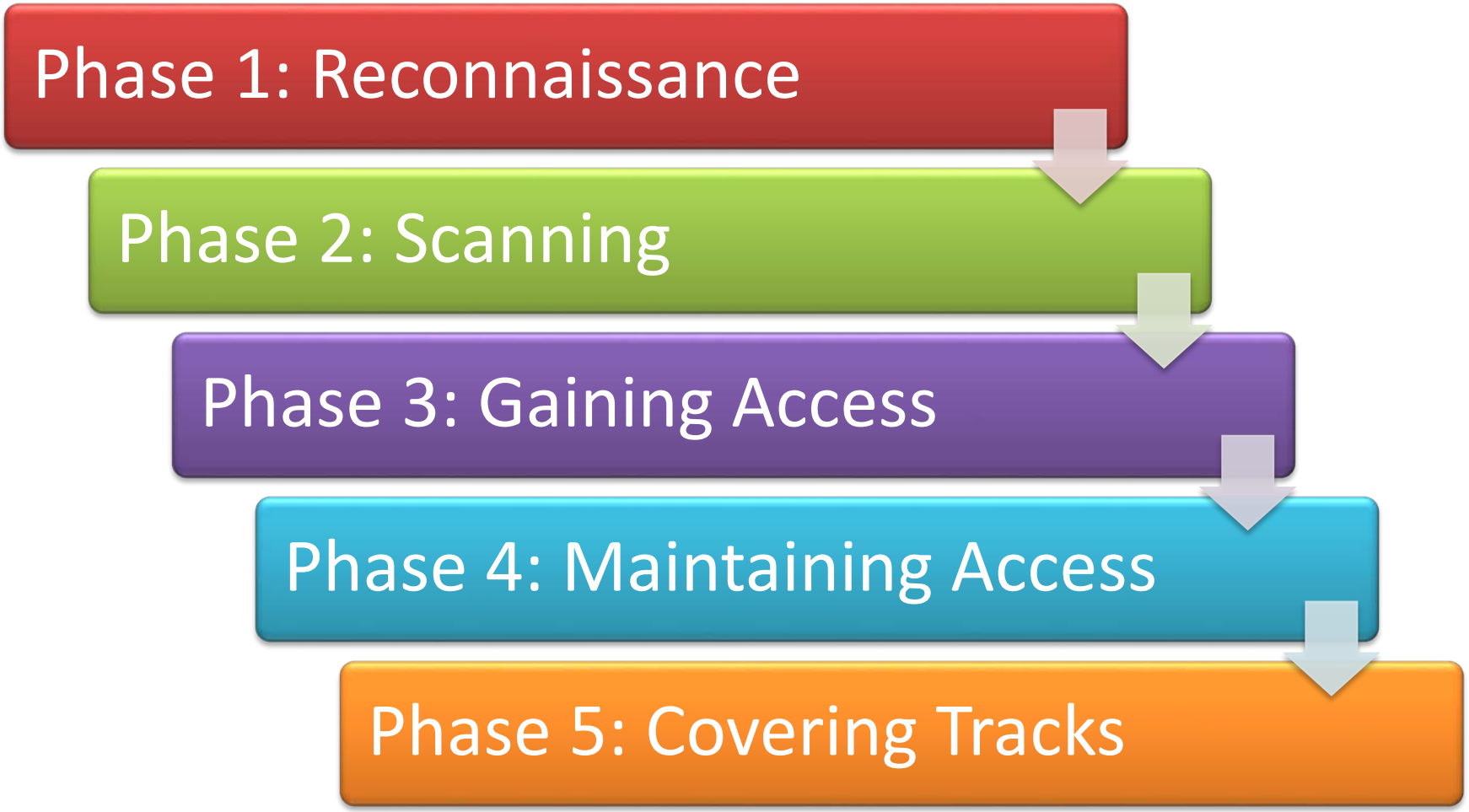
Overview

Types of Attack

Phases of an Attack

Countermeasures

Phases of an Attack



Phase 1 : Reconnaissance

- Gather information from public sources to learn about the target.
  - People
  - Naming conventions
  - Technical Infrastructure
- Information gathered in this phase will be helpful in the other phases.
- Most important stage of an attack.

More information = Higher successful rate

Phase 1 : Reconnaissance

- Information obtained in this phase.
  - Domain name
  - Contacts at the target organization
  - DNS Server IP addresses
  - Other target system IP addresses
  - Possibly, technology in use (e.g. operating system version)
  - Possibly, overview of business relationships associated with the target
  - Possibly, very sensitive information (e.g. usernames and passwords)

Passive vs Active Reconnaissance

- Passive Reconnaissance
  - Gather information of a target without connecting to target directly.
  - e.g. Search engine results of target.
- Active Reconnaissance
  - Gather information of a target by probing the network.
    - e.g. DNS interrogation.
  - More risk of detection as compared to passive reconnaissance.

Reconnaissance Tools

- Whois databases
  - Offers information on registrar.
- Search the Fine Web
  - Through target's website, search engine etc.
- Enumeration
  - Gathering and compiling relevant information the target systems from specific services.
- Low-Technology Reconnaissance
  - Social Engineering
  - Physical Break-in
  - Dumpster Diving

Phase 2 : Scanning

- Taking information gathered during reconnaissance and examine target's network.
  - Look for openings and vulnerabilities.
- Often relies on automated tools to look for openings in the armor.
- Irony
  - Attacker only need to find one way in to achieve his goal.
  - IT Security Professional must defend all entry points.

Phase 2 : Scanning

- Information obtained in this phase.
  - Network addresses of hosts, servers, firewalls, routers and other network devices
  - Network topology
  - Operating systems
  - Open ports and services in each of the machines in the network
  - List of potential vulnerabilities in the machines

Scanning Tools

- War Diallers
  - Spots badly secured external connection using THC-Scan, PhoneSweep and TeleSweep etc.
- War Driving
  - Scan for wireless access points.
- Network mappers
  - Ping sweeps, traceroute, Cheops-ng (an automated tool), etc.
- Port Scanners
  - Scanning for open ports at targeted systems.
- Vulnerability Scanners
  - Scan for known vulnerabilities using tools such as Nessus.
    - Misconfigurations
    - Unpatched systems with known vulnerabilities
    - Other weaknesses

Phase 3 : Gaining Access

- A.k.a. owning the system.
- Attacker will try to gain access into system by
  - Breaking in physically.
  - Manipulating poorly written software.
  - Exploiting weak password storage mechanism.
  - Gathering data that is not properly encrypted, such as user IDs and passwords.
  - Exploiting vulnerabilities of network.
  - Exploiting vulnerabilities of operating system.
- Based on information gathered during reconnaissance and scanning phases.

Activities in Gaining Access

- Running scripts for known exploited vulnerabilities
- Stack-based buffer overflow attacks
- Password attacks using password cracking tools
- Protocol-based attacks
  - Through activities such as sniffing, spoofing, denial-of-service attacks, session hijacking
- Web-based attacks
  - Through session tracking
- Privilege escalation

Phase 4 : Maintaining Access

- Need to keep access for future exploitation and attacks.
- Secure exclusive access with backdoors, rootkits and Trojans.
  - Harden system from other hackers and security personnel.
- Owned system is sometimes known as zombie system.
- Owned systems may be used to launch attacks on other machines.

Activities in Maintaining Access

- Planting Trojan horses software
  - Create listening servers in victim system.
- Planting backdoor software
  - Help to bypass security access controls.
- Planting RootKits
  - By overwriting critical system components with customised data or program which will create an ‘legitimate’ access channel.

Phase 5 : Covering Tracks

- Why cover tracks?
  - Avoid detection
  - Continue using owned system
  - Remove evidence of attack
  - Possibly avoid legal actions
- Erase records of intrusion thereby hiding the history of intrusion.
- Hide all backdoors created.

Activities in Covering Tracks

- Alteration of event logs
  - e.g. Remove log files.
- Switching off Intrusion Detection System (IDS) alarms.
- Hidding files and directories
  - Using RootKits.
  - Through OS.
- Using tunneling protocol
  - Create covert channels for future communication.

Attacks & Defenses

Overview

Types of Attack

Phases of an Attack

Countermeasures

Countermeasures

- For Host
  - Close unused port and disable unneeded services.
  - Keep system patches & signature files up-to-date.
  - Harden system by proper system configuration, remove default settings and hardening scripts.
  - Automate regular backup of logs & critical information.
- For Network
  - Deploy Defense-In-Depth tools.
  - Lockdown defense mechanisms & servers by add-ons.
  - Audit regularly by using vulnerability scanners.
- Implement and regularly revise security policies & incident response procedures.
- Create awareness and training.

Attacks & Defenses

Overview

- Goal of penetration Testers
- Motivation of Hacking
- Exploiting Weaknesses

Types of Attack

- Active vs Passive
- Inside vs Outside

Phases of an Attack

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks

Countermeasures