Introduction to Penetration Testing

Introduction to Computer Security

Naercio Magaia and Imran Khan

Outline

- Attack Surfaces
- Attack Trees
- Penetration Testing
  - What is it?
  - Why use it?
  - Who needs it?
- Approaches
- Methodology

Attack Surfaces

Consist of the reachable and exploitable vulnerabilities in a system

Examples:

- Open ports on outward facing Web and other servers, and code listening on those ports
- Services available on the inside of a firewall
- Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats
- Interfaces, SQL, and Web forms
- An employee with access to sensitive information vulnerable to a social engineering attack

Attack Surface Categories

Network Attack Surface

Vulnerabilities over an enterprise network, wide-area network, or the Internet

Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks

Software Attack Surface

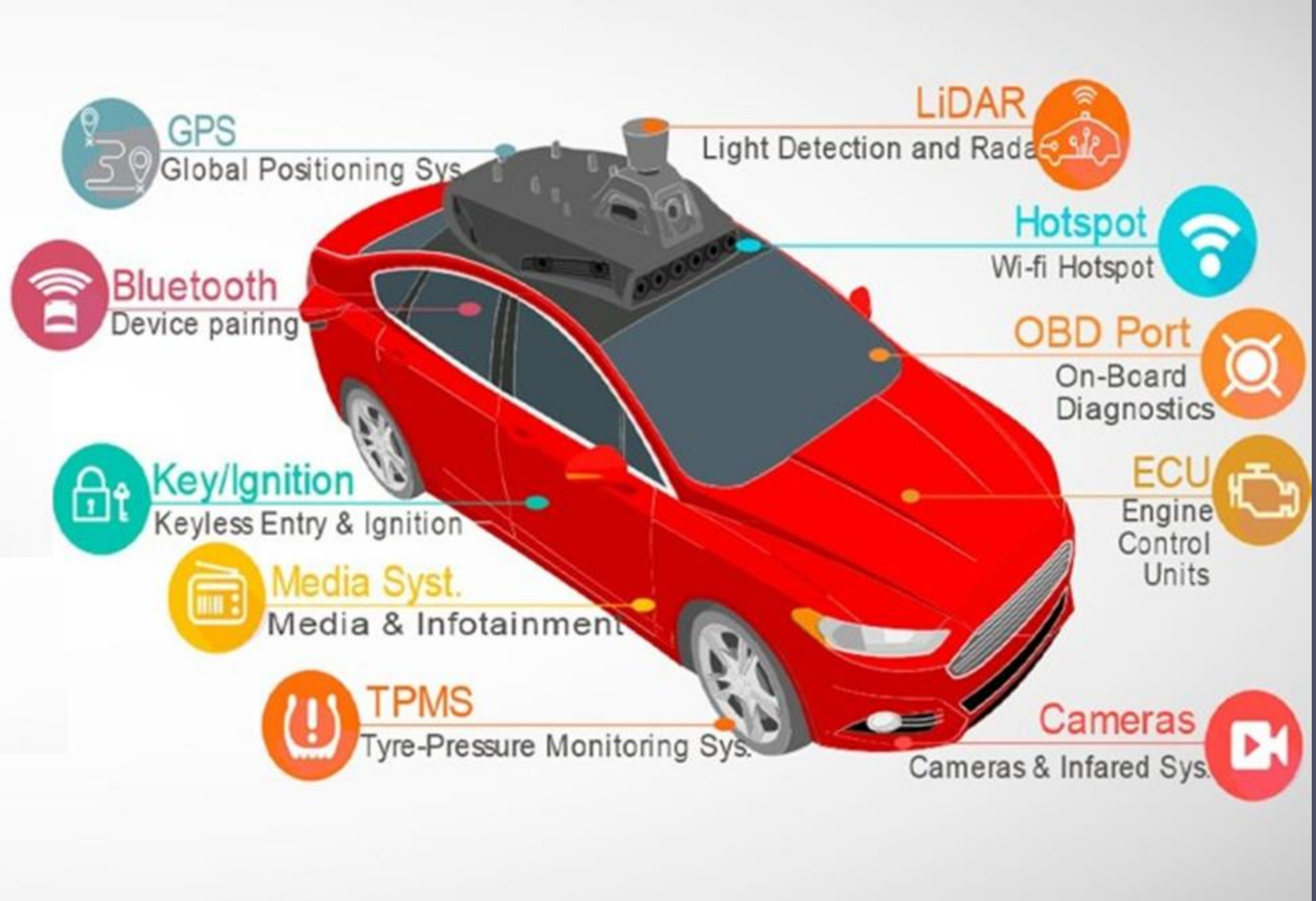
Vulnerabilities in application, utility, or operating system code

Particular focus is Web server software

Human Attack Surface

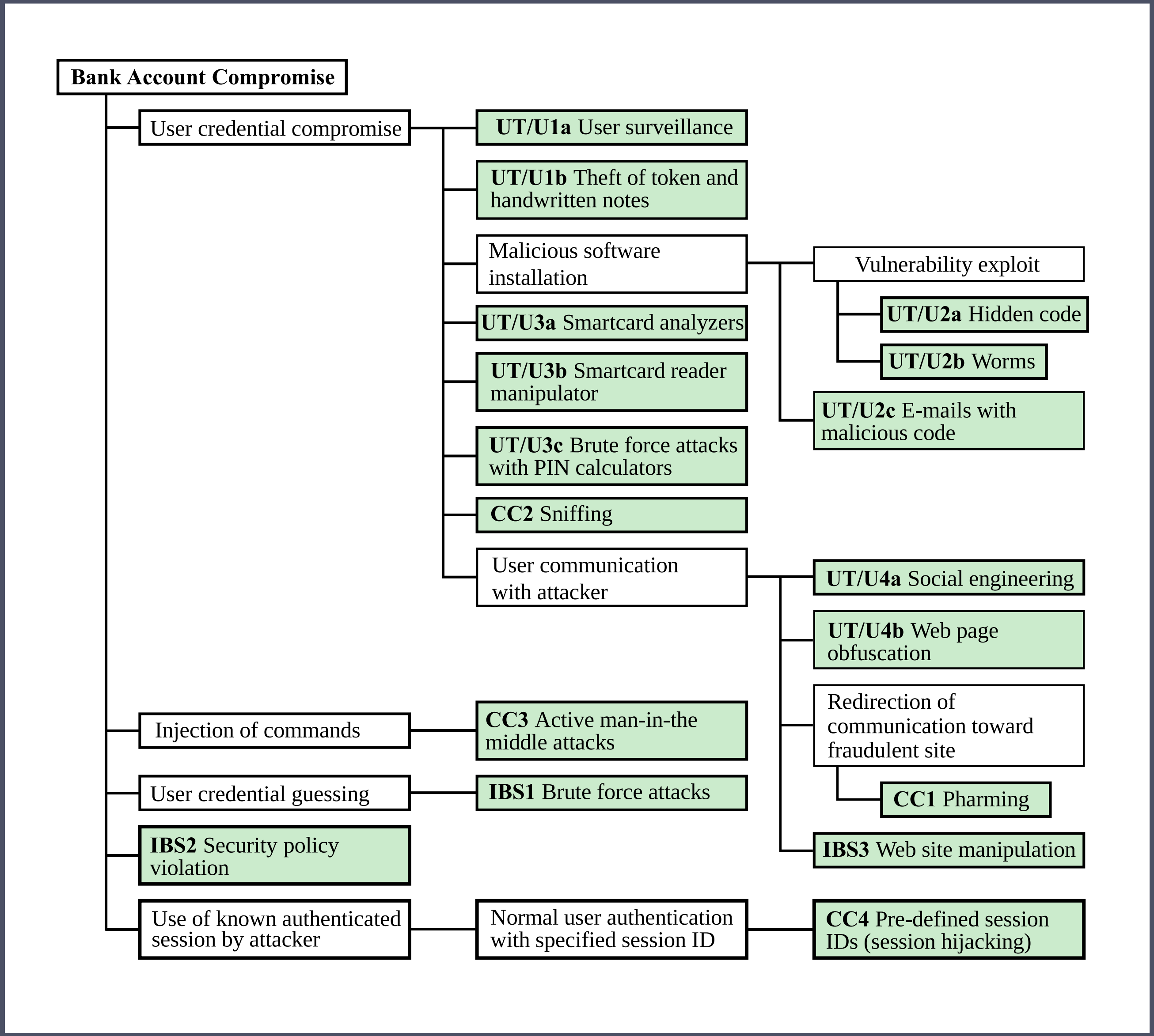
Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

Attack Surfaces in Connected Vehicles



Attack Tree

- Attack trees also provide ways to focus on mode of attack and equipment
  - User terminal and User (UT/U)
  - Communications Channel (CC)
  - Internet Banking Server (IBS)
- Allows for analysis of risk
- Allows for construction of Security Policy
- Starting point for any Penetration Testing



Bank Account Compromise

User credential compromise

UT/U1a User surveillance

UT/U1b Theft of token and handwritten notes

Malicious software installation

Vulnerability exploit

UT/U2a Hidden code

UT/U2b Worms

UT/U2c E-mails with malicious code

UT/U3a Smartcard analyzers

UT/U3b Smartcard reader manipulator

UT/U3c Brute force attacks with PIN calculators

CC2 Sniffing

User communication with attacker

UT/U4a Social engineering

UT/U4b Web page obfuscation

Redirection of communication toward fraudulent site

CC1 Pharming

IBS3 Web site manipulation

Injection of commands

CC3 Active man-in-the middle attacks

User credential guessing

IBS1 Brute force attacks

IBS2 Security policy violation

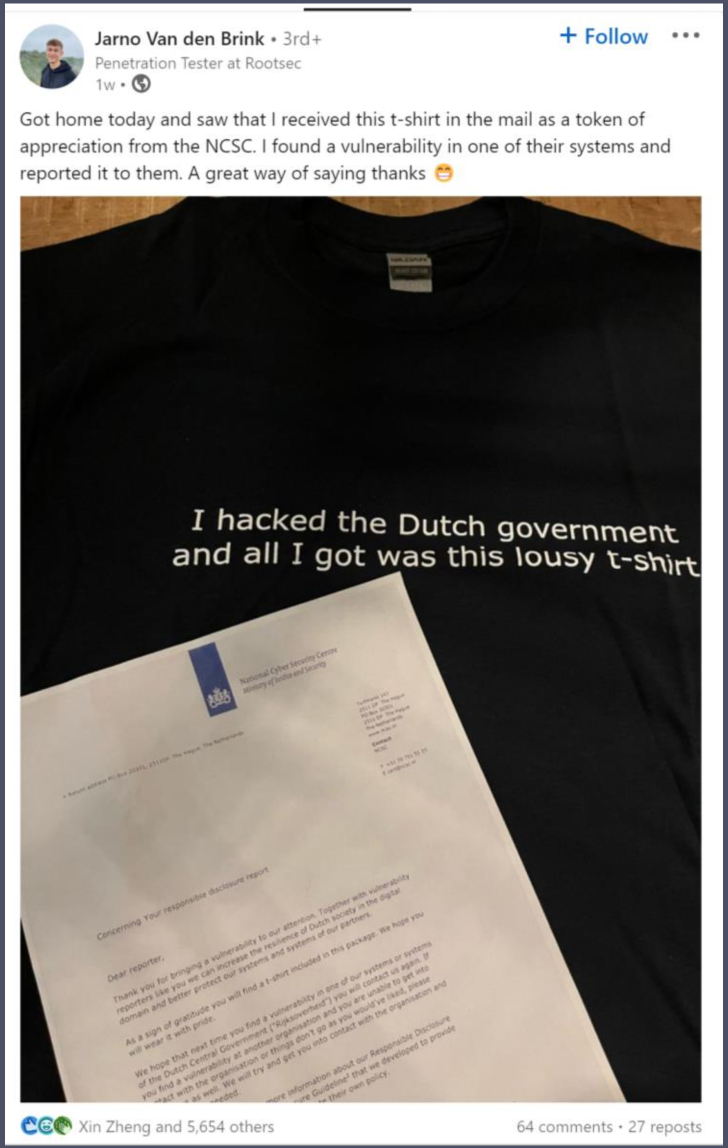
Use of known authenticated session by attacker

Normal user authentication with specified session ID

CC4 Pre-defined session IDs (session hijacking)

What is Penetration Testing?

- Also known as pen testing, pen test, or ethical hacking
- Authorised and legal attempt to expose and exploit vulnerabilities in a target system
  - Computer systems, web applications, networks, IoT, etc.
- Analytical evaluation of the target system's security
- Reporting
  - Catalogue potential threats
  - Determine the feasibility of a cyber-attack
  - Assess the potential impact on a business of a successful cyber-attack



Jarno Van den Brink • 3rd+
Penetration Tester at Rootsec
1w •

+ Follow •••

Got home today and saw that I received this t-shirt in the mail as a token of appreciation from the NCSC. I found a vulnerability in one of their systems and reported it to them. A great way of saying thanks 😁

I hacked the Dutch government
and all I got was this lousy t-shirt
National Cyber Security Centre
Ministry of Justice and Security
Concerning Your responsible disclosure report
Dear reporter,

Xin Zheng and 5,654 others · 64 comments • 27 reposts

Types of Hackers

- White hat hacker
  - A computer security expert, who specializes in penetration testing and in other testing methodologies, which **ensures the security** of an organization's information systems
- Malicious hacker (i.e., black hat hacker)
  - Someone who **explores methods for breaching defences and exploiting weaknesses** in a computer system or network
- <u>Permission, motivation and intent:</u>
  - Permission should be obtained before conducting any test, and agree the scope of the test between pen tester and company being audited
  - Stay legal (Computer Misuse Act 1990)
  - Intent to make the computer systems more secure

Pen Testing vs Vulnerability Assessment

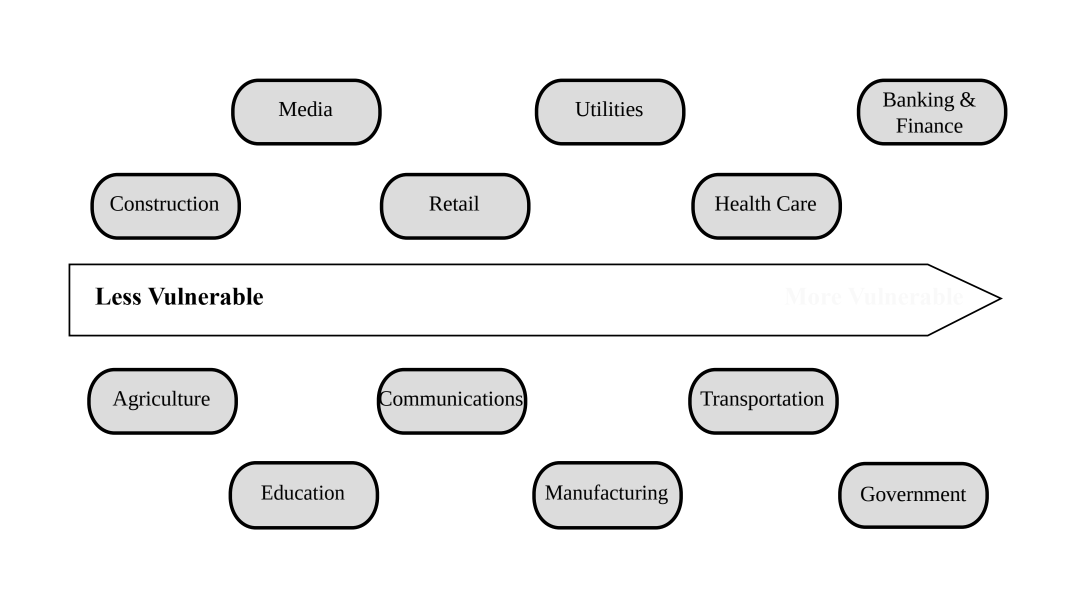
- Vulnerability Assessment (VA) and Attack Trees focuses on discovering potential weaknesses
- Vulnerabilities are not actively exploited in VA
- Pen testing goes beyond VA
  - It actively exploits vulnerabilities

Why Pen Testing?

- To make computer systems, network systems and web applications more secure
- It aims to **find and mitigate security weaknesses** in a system before an attacker exploits them
- **Rationale**: Pen testing **provides a level of assurance** that any malicious user will not be able to penetrate the system
- According to National Institute of Standards and Technology (NIST), it:
  - enhances the organisation's understanding of the system
  - uncovers weaknesses (or deficiencies) in it
  - indicates the level of effort required on the part of adversaries to breaches the system safeguards
- Pen testing should be carried out on any computer system
  - before (and after) it is deployed, in particular Internet facing systems, software version updates

Who needs Pen Testing?

- Large organisations may be required by legislation, in the future, to employ a cyber/digital security specialist
- Cost effective for Small & Medium-sized Enterprises?
- How to pen test?
  - Pen Testing Methodology
  - Analysis is carried out **from the point of view of an attacker**
  - Simulated attempt to exploit vulnerabilities in the target
  - Ethical Hackers use the same tools, techniques and payloads as a Malicious Hacker



Pen Testing Approaches

- Pen tests can be conducted in several ways:
  - No standardised guidelines for pen test execution
- Prior knowledge vary in the amount of detail given to the tester

Blackbox testing	Whitebox testing	Grey box testing
✓ Blind testing ✓ No prior knowledge of target system ✓ Must find and expose the weaknesses ✓ Simulates outside attacker ✓ Labour-intensive ✓ Requires expertise to minimise risks	✓ Insider test ✓ Complete knowledge of the infrastructure ✓ Often conducted as a fully automated process ✓ Simulated insider attack e.g., Unhappy employee e.g., After information leak	✓ Variations between black box and white box ✓ Partial disclosure

Constraints and Risks

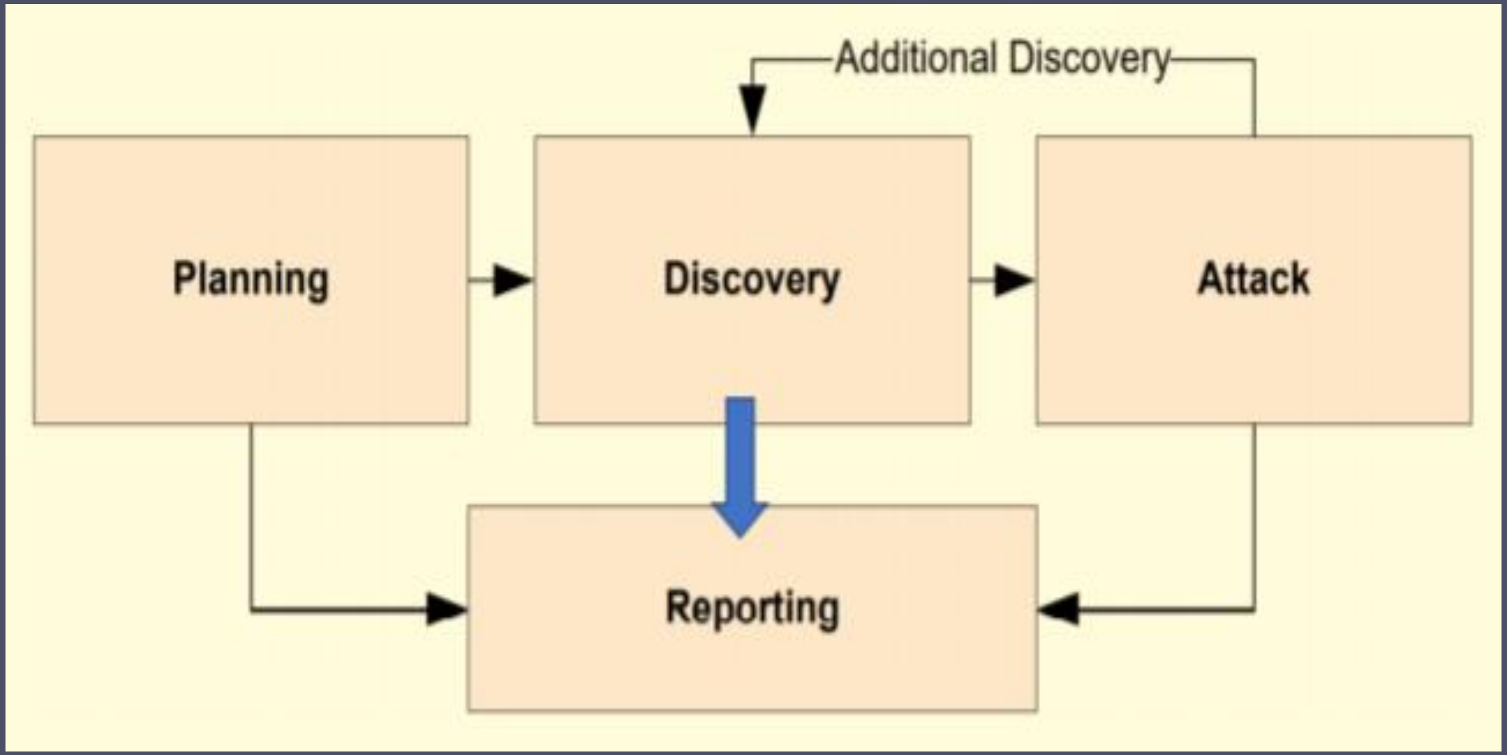
Constraints	Risks
✓ Ethical hackers are (frequently) constrained by time ✓ Malicious hackers are constrained by stealth ✓ Pen tester tend to be noisy - Not concerned about triggering IDS and firewalls - Not realistic attack simulation	✓ Testing may slow the response time ✓ Systems may be damaged in the course of a penetration testing ✓ Risks can be mitigated by experienced pen testers

Pen Testing Methodology

- National Institute of Standards and Technology (NIST)
  - o https://www.nist.gov/
- Penetration Testing Execution Standard (PTES)
  - o http://www.pentest-standard.org/index.php/Main_Page
- Payment Card Industry Security Standards Council
  - https://www.pcisecuritystandards.org/
- Open Web Application Security Project (OWASP)
  - o https://owasp.org/ - Web applications only

NIST Methodology

- NIST Special Publication 800-115
  - Technical Guide to Information Security Testing and Assessment
    - NIST four-stage penetration testing methodology



The Planning phase

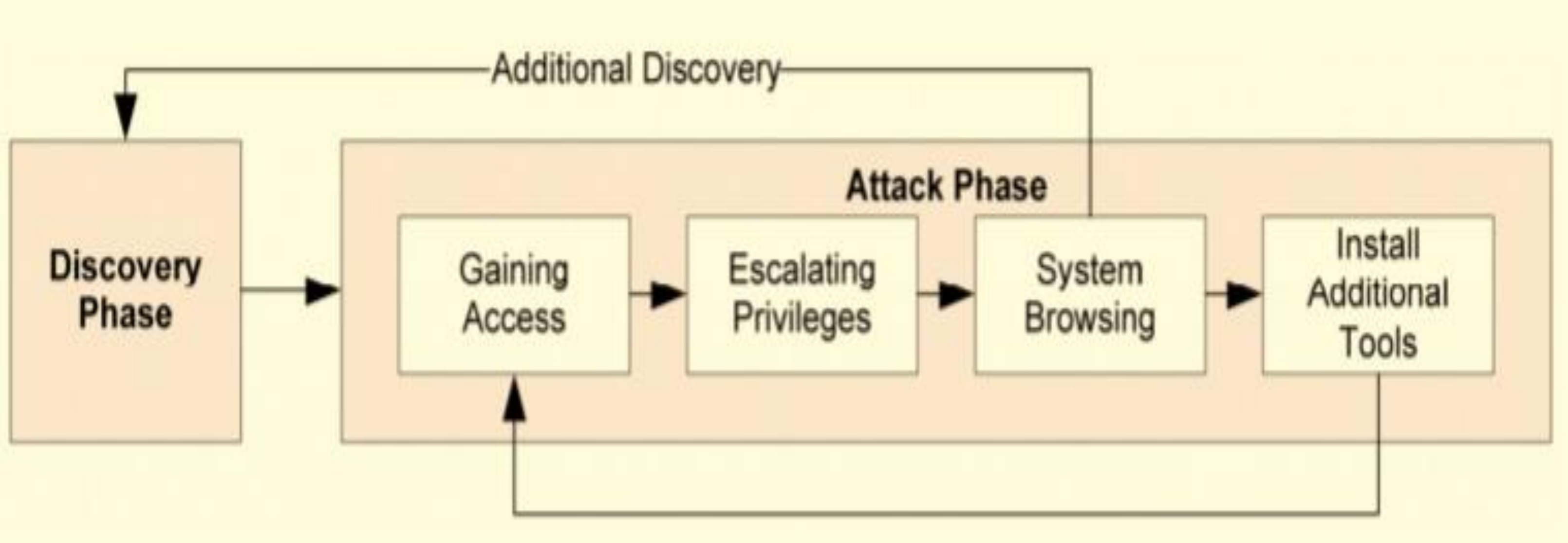
- The scope of a project defines what is to be tested, i.e., the Rules of Engagement
- Neglecting proper pre-engagement activities
  - **Unsatisfied customers & Legal issues**
- Pen testing requires a lot of trust
  - It **is essentially hacking a system**
- Important to understand what the customer expects from the pen test
  - Not uncommon for a client to be unaware of exactly **what it is they need to be tested**
  - Also, possible the client not to know how to communicate **what they are expecting from the test**
- Important to establish communication channels between all parties involved

Rules of Engagement

- Pen tester and company being audited **must mutually agree** on
  - Terms, Conditions, Rules, Requirements and Scope that secure the interests of both parties
  - Detailed information about the resources to be included in the test
- List any system or attack that the client **does not want to be included** in the test
  - For example: DNS servers, Mail servers, Firewalls, Public-facing websites, and Internal systems storing sensitive data…
- Management approval finalised
- Formally documented in a **legal contract signed** by all the parties
- Legal authorisation required before initiating any pen testing assignment
- Confidentiality or Non-Disclosure Agreement signed
  - Findings should be confidential, and shared only with the client
- **No actual test occurs in this phase**

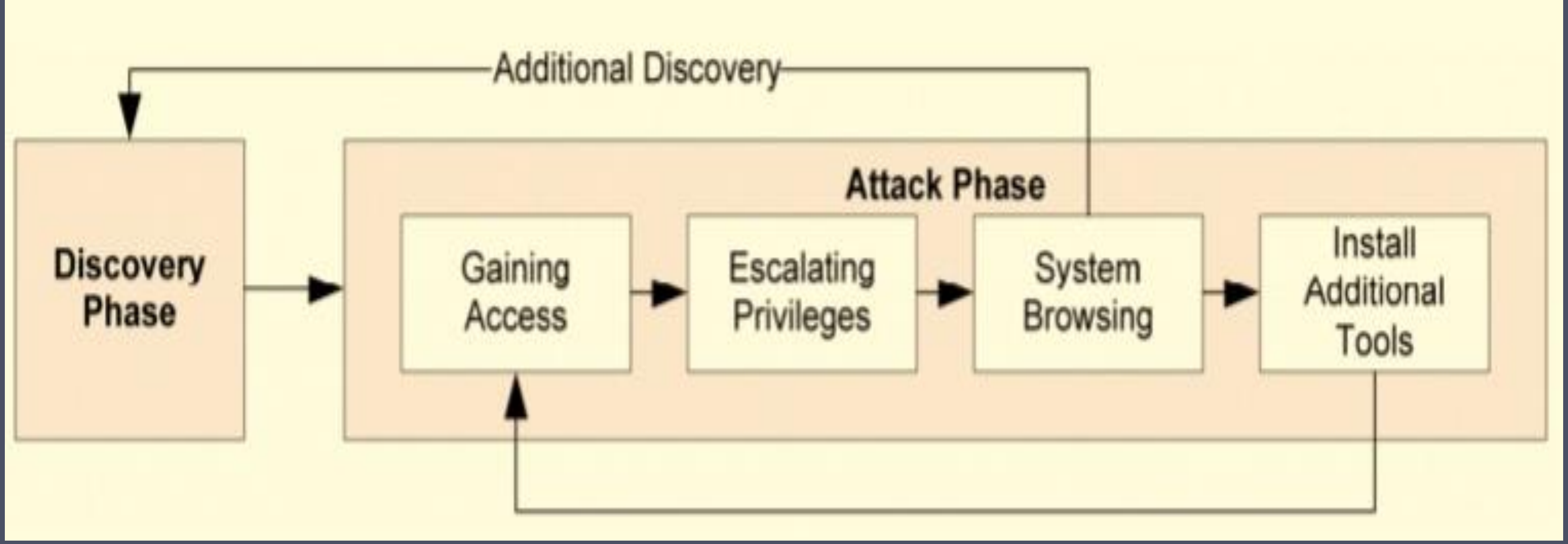
The Discovery Phase

- Discovery phase
  - Reconnaissance / Information Gathering
  - Target Scanning
  - Vulnerability Assessment

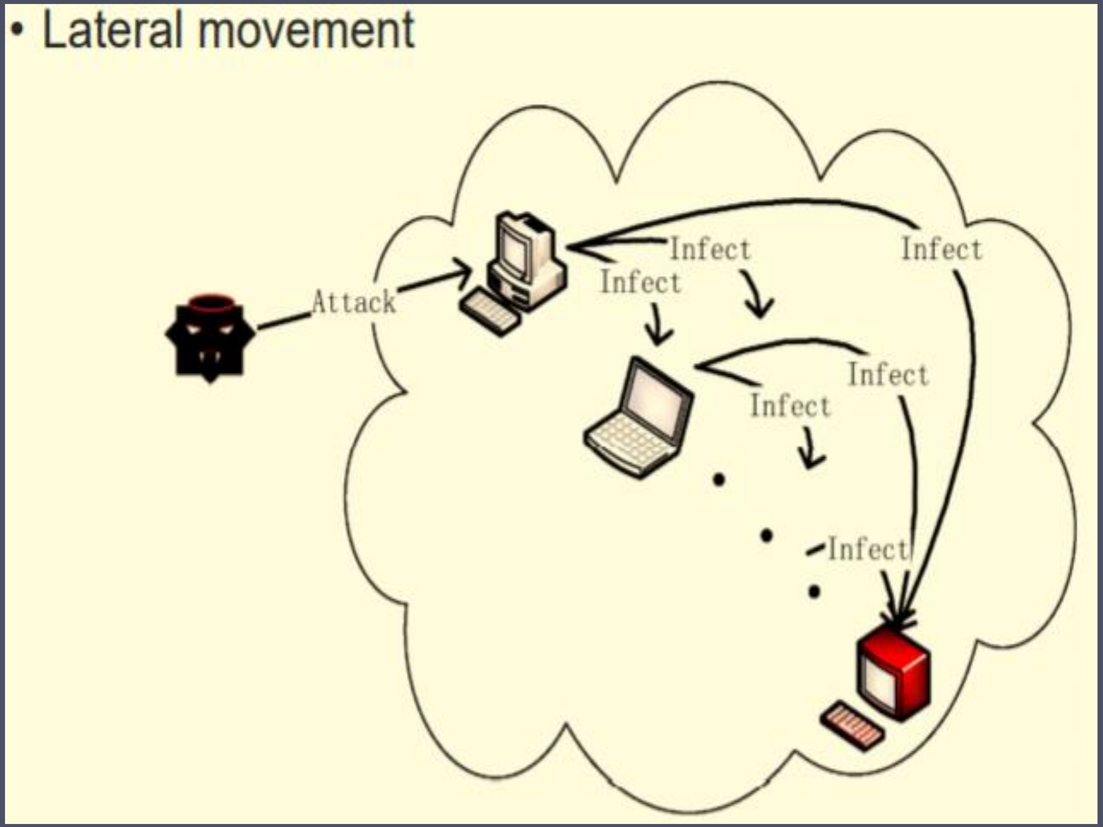


The Attack Phase

- Exploits vulnerabilities discovered to confirm existence
- Active exploitation of the vulnerabilities in the target
- Exploits do not always grant maximum level of access to a system
  - May result in additional discovery about the targeted system
  - May induce a change in the state of the targeted network security



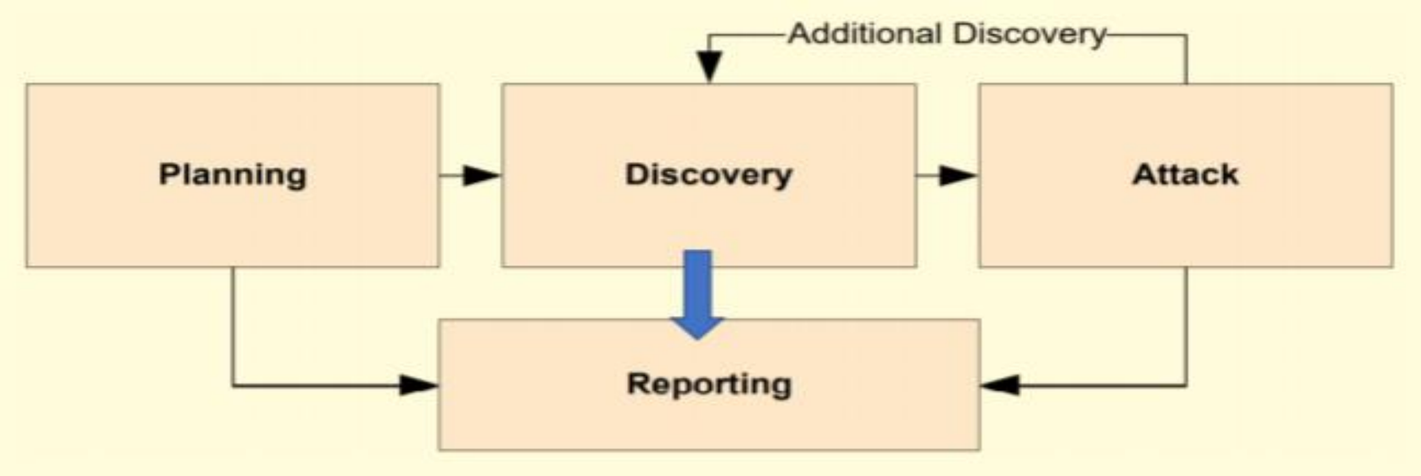
Attack Surface Exploitation



- Some exploits enable pen testers to **escalate privileges** on a system
- Required to gain access to additional resources, i.e., lateral movement
- Installing additional tools to facilitate the testing process
  - To gain access to additional systems or resources on the network
  - To obtain access to information about the network or organisation
- Testing and analysis on multiple systems should be conducted during a penetration test to determine the level of access
- If an attack on a specific vulnerability proves impossible, the tester should attempt to exploit another vulnerability discovered

The Reporting Phase

- Pen testing assignments ends with a final pen testing report
- Reporting simultaneously with the other three phases
  - *Planning phase*: development of pen test plan (i.e., Rules of engagement)
  - *Discovery and attack phases*: written logs are kept and periodic reports to system administrators and management
- Specific **recommendations to address and fix vulnerabilities discovered** during the test



The Reporting phase

- The final pen testing report should include
  - All the **relevant information uncovered** during the pen testing
  - Detailed explanation of **how the test was conducted**
  - Describe **what was done during the test**
  - Executive summary highlighting the most critical issues uncovered
  - Propose mitigations and solutions for the security issues
- Publicly available pen test reports
  - https://github.com/juliocesarfort/public-pentesting-reports

Summary

- Attack Surfaces
- Attack Trees
- Penetration Testing
  - What is it?
  - Why use it?
  - Who needs it?
- Approaches
- Methodology