Security in Practice

Hacking for fun and profit

Josh Anderson
Penetration Tester at Leviathan Security Group

What drives security in industry?

What all do we need to secure?

Why do we do it?

Motivators

Lowering risk
We want to protect our investment and our earnings if
we get hacked we could lose money and productivity
lawsuits loom ominously overhead, all of the time

Compliance requirement
there are regulatory barriers to entry (PCI/HIPAA/GDPR)

Moral obligation
people trust us with their info, we have to secure it

What jobs does this create?

Blue team - defense

- Software developers
- Network/firewall team
- Disaster recovery / incident response
- Security guards

Red team - offense

- Angry nation states
- Angry hacker groups
- Angry kid from CoD lobby
- People like me!

PenTesting

Types of Pentests

Network

Focus on protocol attacks and known vulnerabilities in old software.
These are my most common projects.

External Network

Literally anybody in the world can see this

Testing public facing web-apps and vpn endpoints

Encryption is very important

Brute force protections are very important

Internal Network

Like attacking a company from the inside

Target remote access methods: ssh, rdp, telnet

Man in the middle attacks

LOTS of Windows

Ultimate goal is Domain Admin
‘

Wireless Network

Are they using strong protocols? WPA2/WPA3?

Spoofing attacks

MitM attacks

Rogue access points

Improperly configured WiFi is equivalent to shouting your secrets in the parking lot

Web and Mobile Application

Larger focus on logic problems and custom code

Webapps

Cross site scripting

Injection attacks

Authorization/authentication issues

Client side access controls

See OWASP Top 10

Mobile Applications

Almost every web app issue

File storage

App permissions

Encryption at rest and in transit

Reverse engineering and tampering

Hardware

Chip level attacks

soldering/direct component bypass

Read directly from the bus/memory

Tamper evident seal bypass

Car hacking

IoT Devices

Social Engineering

Fancy words for just lying your pants off

Phishing

Emails, targeted and non

Social media

Phone calls from “IT”

Easy way to get a foothold

Physical security

“Full red team experience”

Picking locks

RFID badge cloning/brute forcing

Tailgating

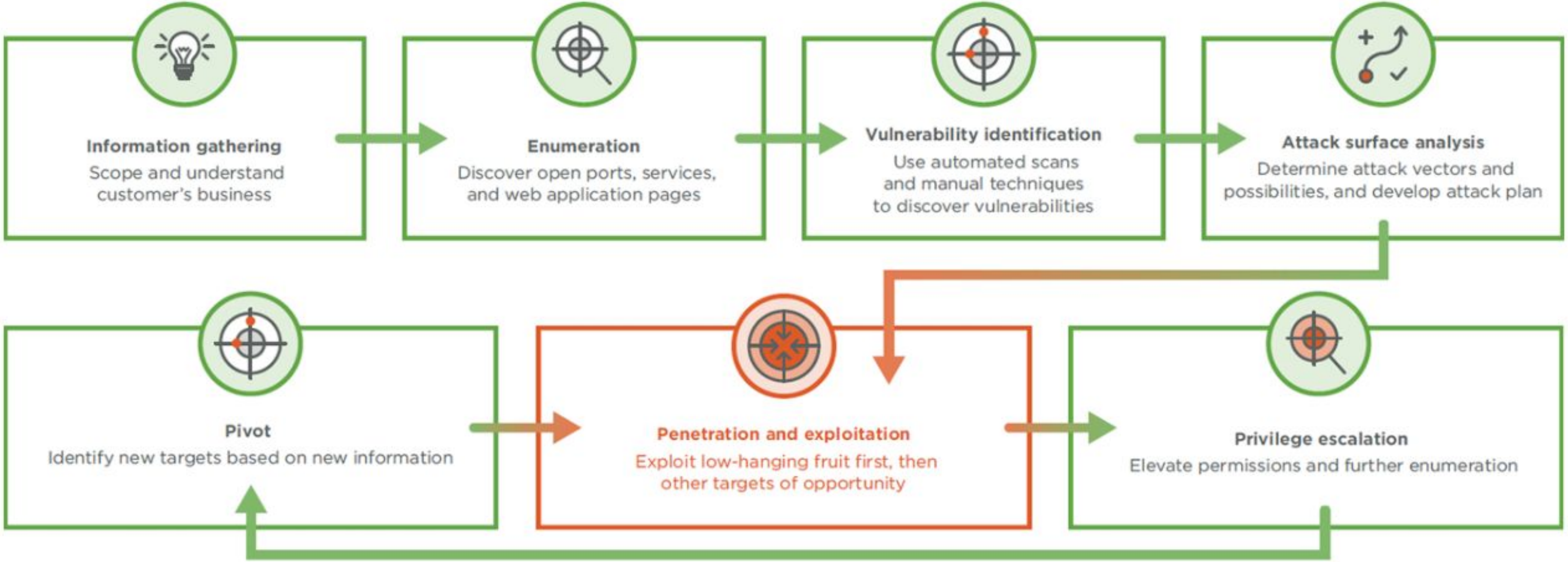
Dressing up as a janitor and just running around with an arm full of plungers while crying

Dropbox that phones home

Keyloggers

Rubber ducky

Components of an attack



Information gathering
Scope and understand customer's business

Enumeration
Discover open ports, services, and web application pages

Vulnerability identification
Use automated scans and manual techniques to discover vulnerabilities

Attack surface analysis
Determine attack vectors and possibilities, and develop attack plan

Pivot
Identify new targets based on new information

Penetration and exploitation
Exploit low-hanging fruit first, then other targets of opportunity

Privilege escalation
Elevate permissions and further enumeration

Img Source: Coalfire https://www.coalfire.com/solutions/threat-and-vulnerability-management/penetration-tests

Differences between an attack and a pentest

We don’t get to stop just because we got inside, we need to find as many holes in the security as possible

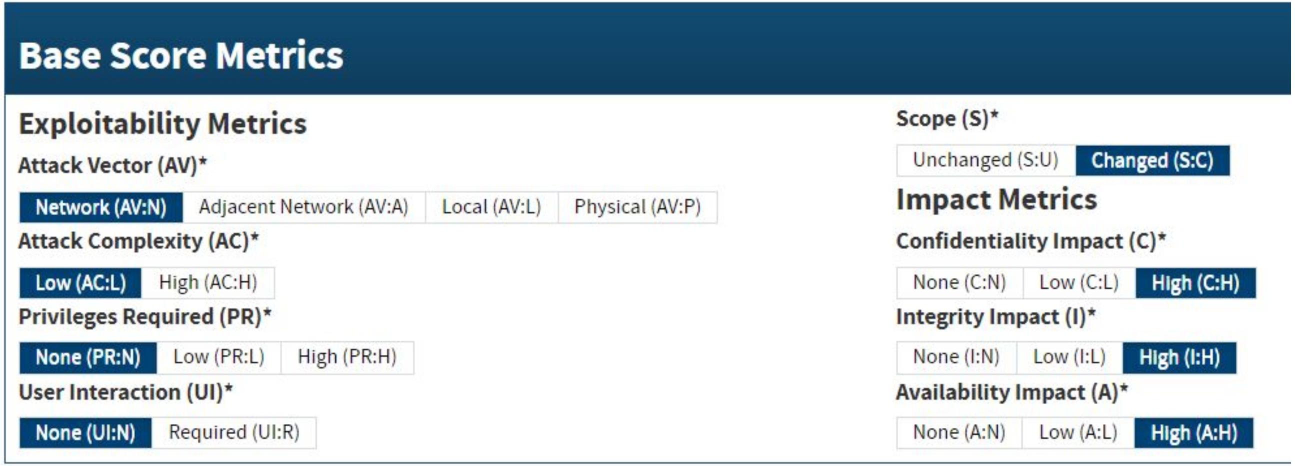
Our goal is to find the line, not just cross it

We don’t always get inside, so sometimes they open the door for us

We need to be real careful what we do with our access and the data we get. Often data exfiltration is not allowed

The last step is ALWAYS reporting. All value comes from what we teach the client, not solely from what we are able to do

CVSS: Example of quantifying risk



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

[✓ Network (AV:N)] Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

[✓ Low (AC:L)] High (AC:H)

Privileges Required (PR)*

[✓ None (PR:N)] Low (PR:L) High (PR:H)

User Interaction (UI)*

[✓ None (UI:N)] Required (UI:R)

Scope (S)*

Unchanged (S:U) [✓ Changed (S:C)]

Impact Metrics

Confidentiality Impact (C)*

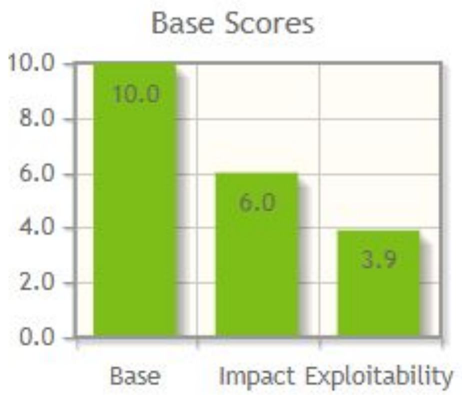
None (C:N) Low (C:L) [✓ High (C:H)]

Integrity Impact (I)*

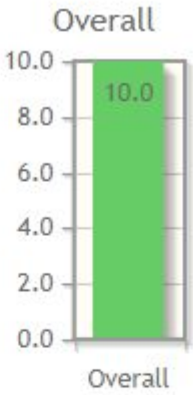
None (I:N) Low (I:L) [✓ High (I:H)]

Availability Impact (A)*

None (A:N) Low (A:L) [✓ High (A:H)]



Base Scores



Overall

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Thanks!

Feel free to email me with questions!

josh.anderson@leviathansecurity.com