DEVSECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK SIX / LESSON ONE

Copyright © DevSecOps Foundation 2015-2016

Week 6 Offensive Security

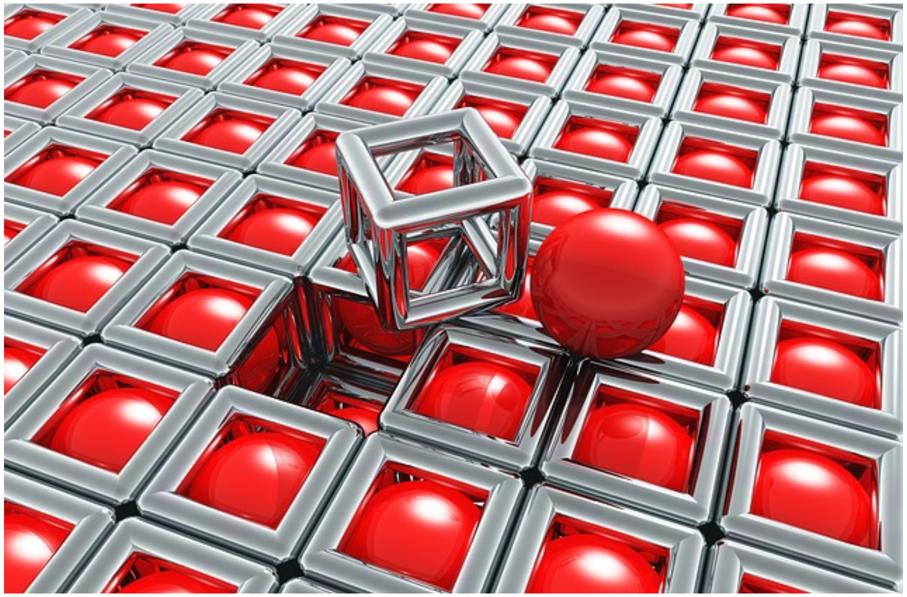
Agenda

- Thinking Outside the box
- Web Application Vulnerability Chaining
- Lab 1 Web App Vuln Chaining
- Lateral Movement
  - Metasploit Intro
- AWS Account Takeover (ATO)
  - ATO Lab

Copyright © DevSecOps Foundation 2015-2016

Thinking Like an Attacker

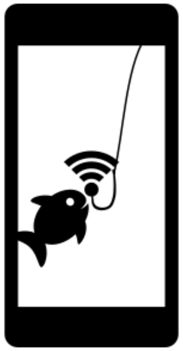
- Attacking the weak link (Humans)
- Redefine the perimeter
- High value target $$$
- Most value for least effort
- Persistence
- Obfuscation

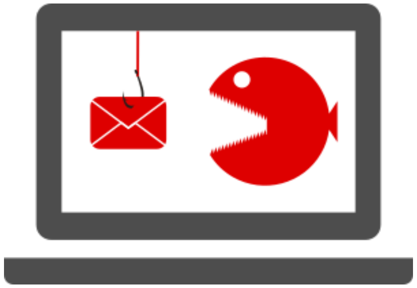


Copyright © DevSecOps Foundation 2015-2016

Attack Vectors

- Phishing
- Network
- Malware
- Application
- Web Application
- Mobile
- Wireless MITM

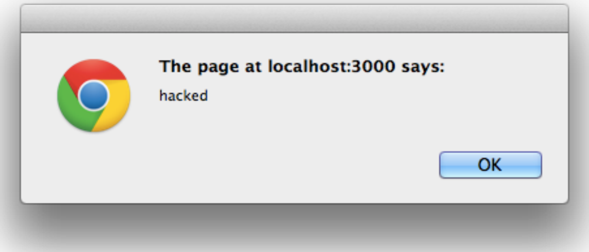




Copyright © DevSecOps Foundation 2015-2016

Web Application Exploit Chaining

- Sometimes one vuln is not good enough
- Chaining exploits together improves both the likelihood of occurrence and the impact of successful exploitation
- This is called "vulnerability weaponization"
- You have to be able to "think outside the box" and be a little sadistic



The page at localhost:3000 says:

hacked

http://example.com/redirect.php?url=http://evil.attacker.com

Copyright © DevSecOps Foundation 2015-2016

Exploit Chaining Example #1

Unvalidated redirect + 0-day browser plugin exploit

==

Malware drop on victim’s PC

+

OS priv escalation exploit

==

Hostile PC takeover and/or foothold into internal network

- If attack is targeted, the goal will be the latter (foothold)
- If attack is non-targeted, the goal will be the former (ransomware)

Copyright © DevSecOps Foundation 2015-2016

Exploit Chaining Example #2

Persistent XSS vuln on commonly frequented site

+

CSRF vulnerability in victim's broadband router's "mgmt web app"

==

Router take-over and/or foothold into internal network

- If attack is targeted, goal will be the latter (foothold)
- If attack is non-targeted, goal will be the former (use router for DDOS)

Copyright © DevSecOps Foundation 2015-2016

Exploit Chaining Example #3

Unvalidated Redirect

+

XSS (exploiting Broken Session Mgmt and/or Sensitive Data Exposure vulns)

+

more Broken Session Mgmt

==

Successful Account Hijack bypassing MFA protection

Copyright © DevSecOps Foundation 2015-2016

Questions?

Copyright © DevSecOps Foundation 2015-2016

Lab 1 Chaining Web Exploits

Copyright © DevSecOps Foundation 2015-2016

Copyright © DevSecOps Foundation 2015-2016