
DEV/SECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK SIX / LESSON TWO

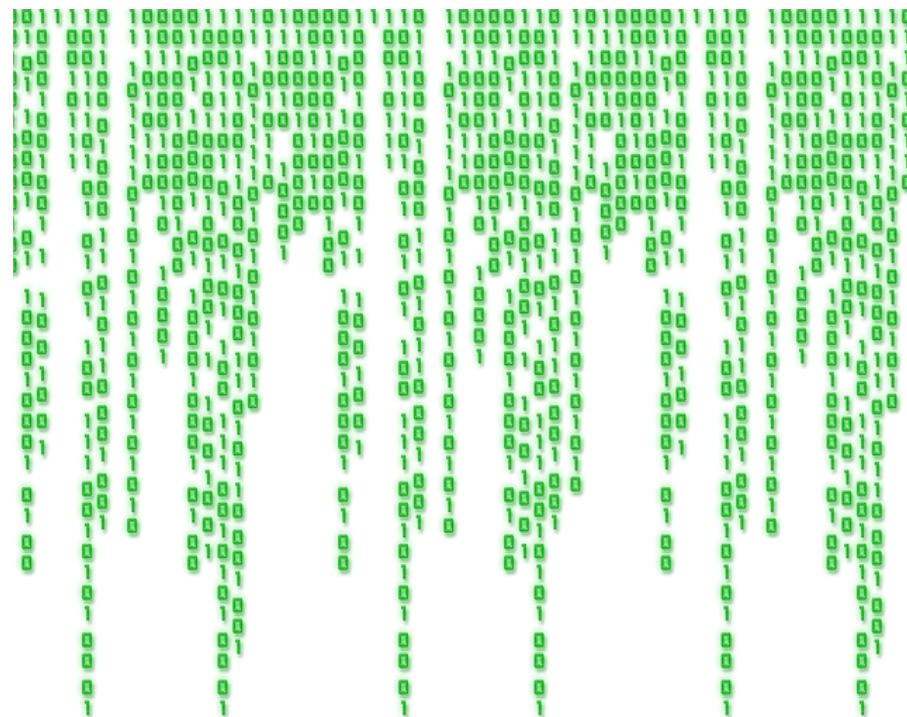
Agenda

- Network Attack
- Nmap
- Enumeration
- Metasploit
- Jenkins
- JBoss
- Lateral Movement
- Lab 2



Network Attack

- Enumerating systems
- Enumerating listening services
- Known vulnerabilities
- Unknown vulnerabilities (0 –Day)
- Misconfigurations
- Bad default installations (HUE, Jenkins, etc...)



Nmap

- Network Mapper
- Written by Fyodor
- Extensible through Nmap scripting engine (NSE) using Lua
- Many many command line args
- RTFM @ <https://svn.nmap.org/nmap/docs/nmap.usage.txt>
- Can test using scanme.nmap.org



Vulnerability Enumeration

- <https://nvd.nist.gov>
- <http://exploit-db.com>
- <https://cve.mitre.org>
- Tools
 - Nessus
 - Qualys
 - Nexpose
 - Nmap

**EXPLOIT
DATABASE**

<http://exploit-db.com>, 2016)



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

MITRE

Metasploit

- Offensive Security Framework
 - Exploit Development
 - Exploit Delivery
- Modular
 - Exploit Modules
 - Auxiliary Modules
 - Scanner Modules
 - Multiple Payloads
 - Meterpreter
 - Shell
- Post Exploitation Modules
 - Gather Data
 - Steal and Crack Password Hashes



```
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...-
IIIIII dTb.dTb
  II 4' v 'B
  II 6. .P
  II 'T;. ;P'
  II 'T; ;P'
IIIIII 'YvP'
I love shells --egypt
```

Jenkins

- Continuous Integration
- Continuous Deployment
- Master/Slave Architecture
- Distributed code execution platform
- Insecure by DEFAULT



JBoss

- Java Application Server
- Older versions are insecure by default
- JMX Console can be used to deploy arbitrary applications
- Many remote code execution vulnerabilities



Lateral Movement/Pivoting

- Establish Foothold
- Gather loot
 - .bash_history
 - .ssh
 - .aws
 - /etc/shadow
- Begin Network Enumeration
 - Scan (loud)
 - ARP (quiet)
- Persistence



Questions?

Lab 2 – Exploiting Jenkins

- <https://github.com/devsecops/bootcamp/blob/master/Week-6/labs/LAB-2.md>