Penetration Testing

How Offensive Security Improves System Resilience

Presented by: Joseph Doba

josephdoba.com

https://www.linkedin.com/in/joseph-aj-doba/

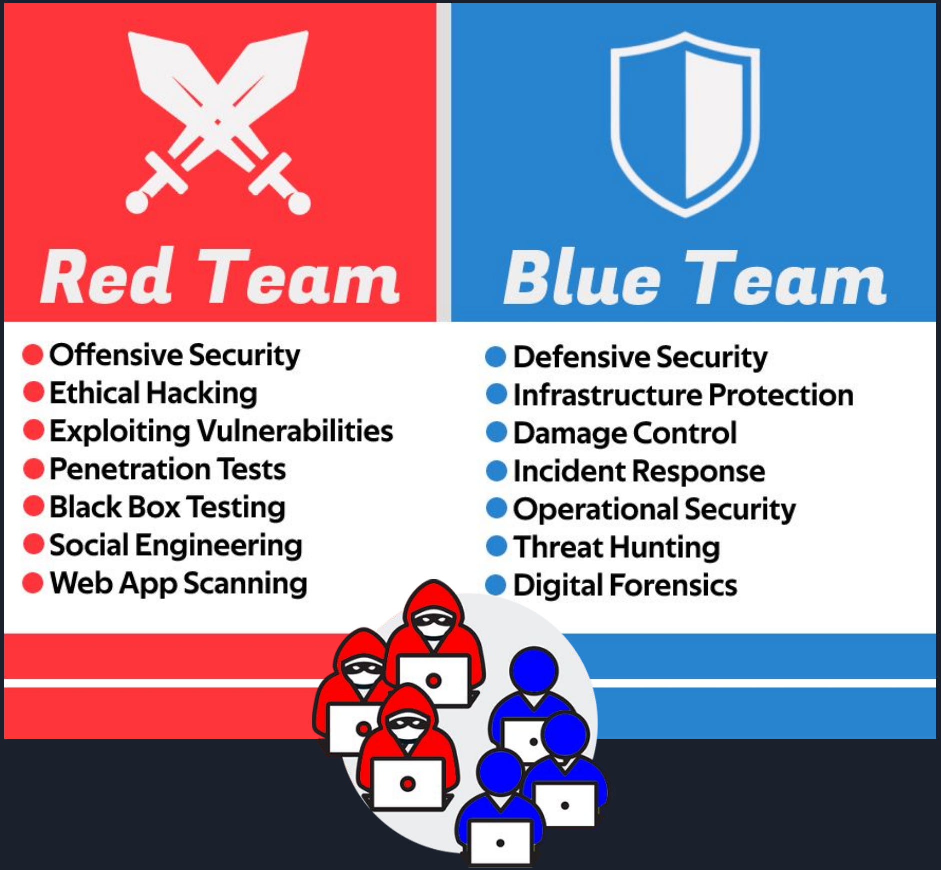
https://github.com/josephdoba

About me

Overview

1: Introduction
2: Penetration Testing Concepts
3: Methodology
4: Tools
5: Conclusion

Blue Team and Red Team



Red Team

- Offensive Security
- Ethical Hacking
- Exploiting Vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

Blue Team

- Defensive Security
- Infrastructure Protection
- Damage Control
- Incident Response
- Operational Security
- Threat Hunting
- Digital Forensics

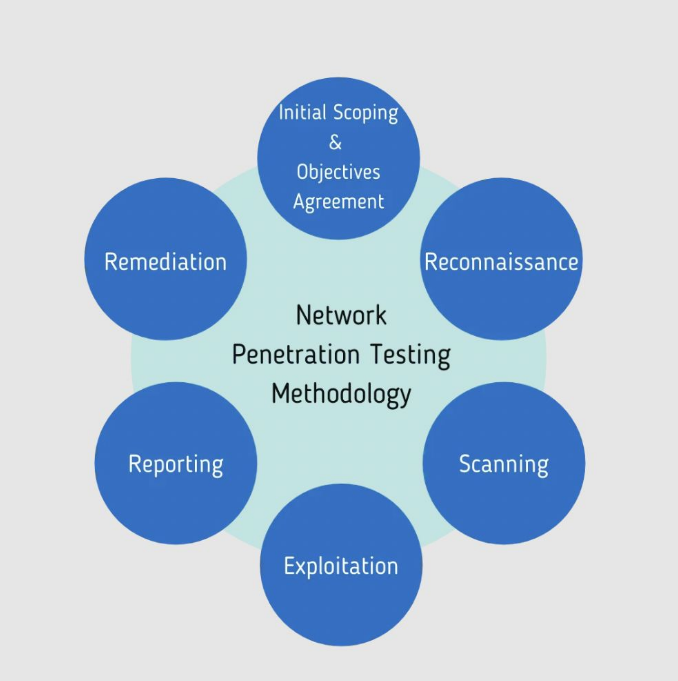
What is Penetration Testing?

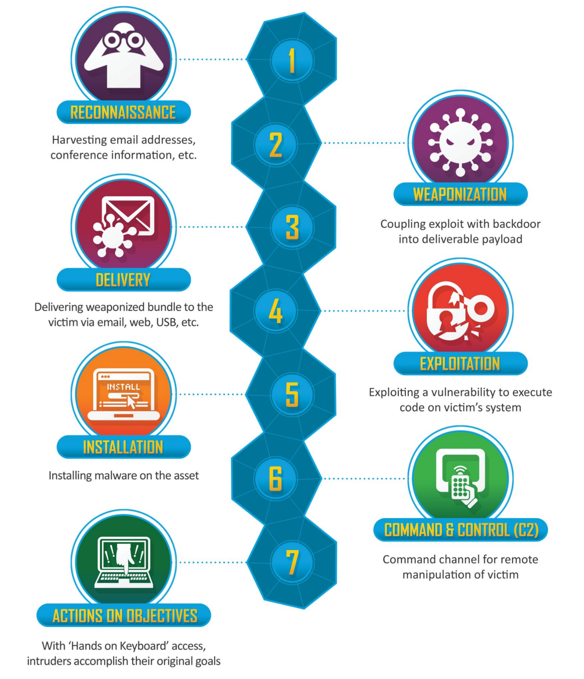
NIST-800-115: *“Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers.”*

TL;DR:

- Simulates a real attack to test the effectiveness of security measures.
- Uncover hidden vulnerabilities by thinking like an attacker
- The goal is to see how deep they can get into a network, by exploiting as many vulnerabilities.
- Report their findings and remediation to Blue Team

Methodology of a Penetration Test


Initial Scoping & Objectives Agreement
Reconnaissance
Scanning
Exploitation
Reporting
Remediation
Network Penetration Testing Methodology



RECONNAISSANCE: Harvesting email addresses, conference information, etc.

WEAPONIZATION: Coupling exploit with backdoor into deliverable payload

DELIVERY: Delivering weaponized bundle to the victim via email, web, USB, etc.

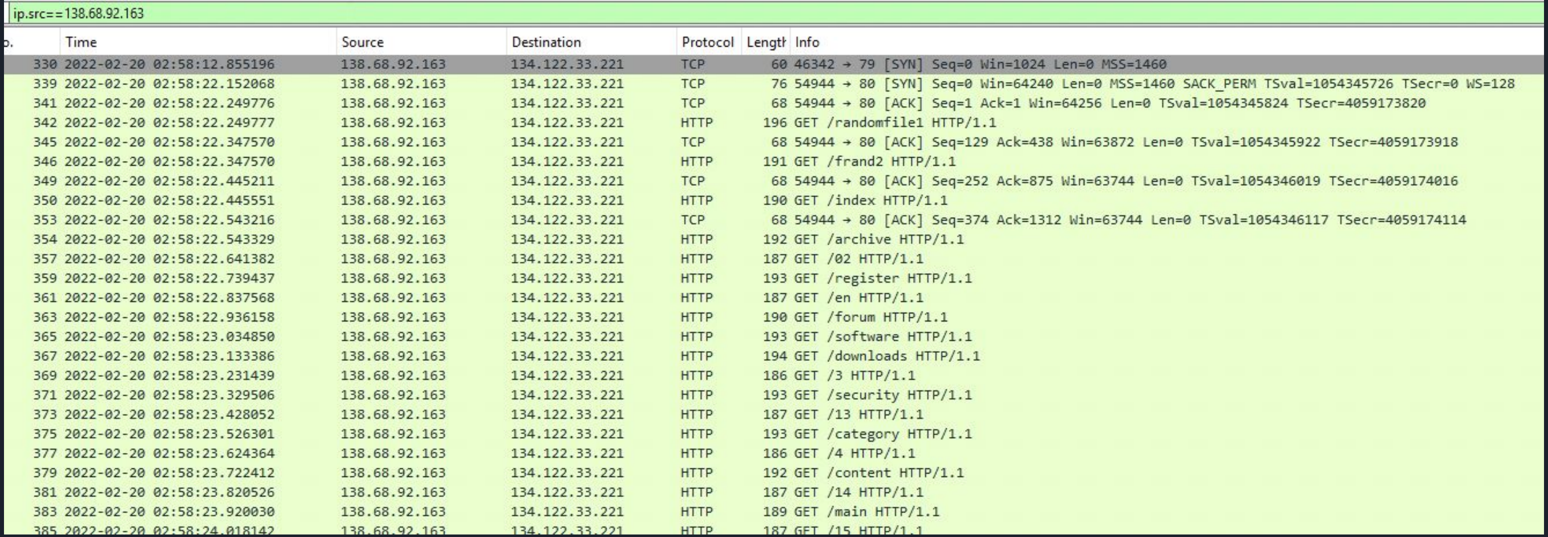
EXPLOITATION: Exploiting a vulnerability to execute code on victim's system

INSTALLATION: Installing malware on the asset

COMMAND & CONTROL (C2): Command channel for remote manipulation of victim

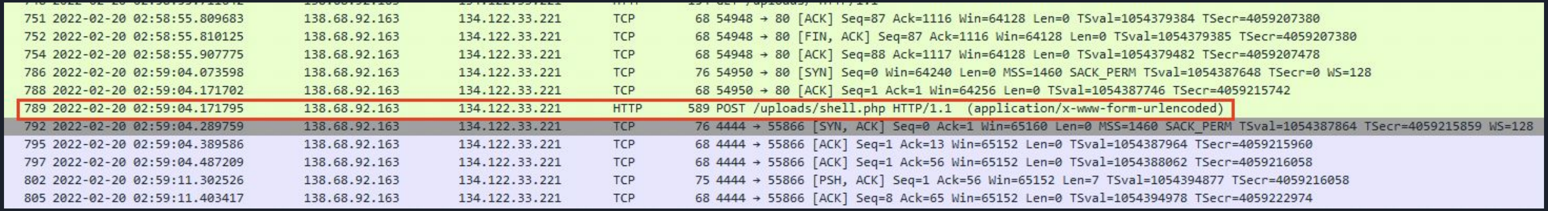
ACTIONS ON OBJECTIVES: With 'Hands on Keyboard' access, intruders accomplish their original goals

Case Study: Premium House Lights



```
ip.src==138.68.92.163

o.   Time                        Source          Destination     Protocol Length Info
 330 2022-02-20 02:58:12.855196  138.68.92.163   134.122.33.221  TCP        60 46342 → 79 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 339 2022-02-20 02:58:22.152068  138.68.92.163   134.122.33.221  TCP        76 54944 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1054345726 TSecr=0 WS=128
 341 2022-02-20 02:58:22.249776  138.68.92.163   134.122.33.221  TCP        68 54944 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1054345824 TSecr=4059173820
 342 2022-02-20 02:58:22.249777  138.68.92.163   134.122.33.221  HTTP      196 GET /randomfile1 HTTP/1.1
 345 2022-02-20 02:58:22.347570  138.68.92.163   134.122.33.221  TCP        68 54944 → 80 [ACK] Seq=129 Ack=438 Win=63872 Len=0 TSval=1054345922 TSecr=4059173918
 346 2022-02-20 02:58:22.347570  138.68.92.163   134.122.33.221  HTTP      191 GET /frand2 HTTP/1.1
 349 2022-02-20 02:58:22.445211  138.68.92.163   134.122.33.221  TCP        68 54944 → 80 [ACK] Seq=252 Ack=875 Win=63744 Len=0 TSval=1054346019 TSecr=4059174016
 350 2022-02-20 02:58:22.445551  138.68.92.163   134.122.33.221  HTTP      190 GET /index HTTP/1.1
 353 2022-02-20 02:58:22.543216  138.68.92.163   134.122.33.221  TCP        68 54944 → 80 [ACK] Seq=374 Ack=1312 Win=63744 Len=0 TSval=1054346117 TSecr=4059174114
 354 2022-02-20 02:58:22.543329  138.68.92.163   134.122.33.221  HTTP      192 GET /archive HTTP/1.1
 357 2022-02-20 02:58:22.641382  138.68.92.163   134.122.33.221  HTTP      187 GET /02 HTTP/1.1
 359 2022-02-20 02:58:22.739437  138.68.92.163   134.122.33.221  HTTP      193 GET /register HTTP/1.1
 361 2022-02-20 02:58:22.837568  138.68.92.163   134.122.33.221  HTTP      187 GET /en HTTP/1.1
 363 2022-02-20 02:58:22.936158  138.68.92.163   134.122.33.221  HTTP      190 GET /forum HTTP/1.1
 365 2022-02-20 02:58:23.034850  138.68.92.163   134.122.33.221  HTTP      193 GET /software HTTP/1.1
 367 2022-02-20 02:58:23.133386  138.68.92.163   134.122.33.221  HTTP      194 GET /downloads HTTP/1.1
 369 2022-02-20 02:58:23.231439  138.68.92.163   134.122.33.221  HTTP      186 GET /3 HTTP/1.1
 371 2022-02-20 02:58:23.329506  138.68.92.163   134.122.33.221  HTTP      193 GET /security HTTP/1.1
 373 2022-02-20 02:58:23.428052  138.68.92.163   134.122.33.221  HTTP      187 GET /13 HTTP/1.1
 375 2022-02-20 02:58:23.526301  138.68.92.163   134.122.33.221  HTTP      193 GET /category HTTP/1.1
 377 2022-02-20 02:58:23.624364  138.68.92.163   134.122.33.221  HTTP      186 GET /4 HTTP/1.1
 379 2022-02-20 02:58:23.722412  138.68.92.163   134.122.33.221  HTTP      192 GET /content HTTP/1.1
 381 2022-02-20 02:58:23.820526  138.68.92.163   134.122.33.221  HTTP      187 GET /14 HTTP/1.1
 383 2022-02-20 02:58:23.920030  138.68.92.163   134.122.33.221  HTTP      189 GET /main HTTP/1.1
 385 2022-02-20 02:58:24.018142  138.68.92.163   134.122.33.221  HTTP      187 GET /15 HTTP/1.1
```



```
751 2022-02-20 02:58:55.809683  138.68.92.163  134.122.33.221  TCP    68 54948 → 80 [ACK] Seq=87 Ack=1116 Win=64128 Len=0 TSval=1054379384 TSecr=4059207380
752 2022-02-20 02:58:55.810125  138.68.92.163  134.122.33.221  TCP    68 54948 → 80 [FIN, ACK] Seq=87 Ack=1116 Win=64128 Len=0 TSval=1054379385 TSecr=4059207380
754 2022-02-20 02:58:55.907775  138.68.92.163  134.122.33.221  TCP    68 54948 → 80 [ACK] Seq=88 Ack=1117 Win=64128 Len=0 TSval=1054379482 TSecr=4059207478
786 2022-02-20 02:59:04.073598  138.68.92.163  134.122.33.221  TCP    76 54950 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1054387648 TSecr=0 WS=128
788 2022-02-20 02:59:04.171702  138.68.92.163  134.122.33.221  TCP    68 54950 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1054387746 TSecr=4059215742
789 2022-02-20 02:59:04.171795  138.68.92.163  134.122.33.221  HTTP  589 POST /uploads/shell.php HTTP/1.1  (application/x-www-form-urlencoded)
792 2022-02-20 02:59:04.289759  138.68.92.163  134.122.33.221  TCP    76 4444 → 55866 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1054387864 TSecr=4059215859 WS=128
795 2022-02-20 02:59:04.389586  138.68.92.163  134.122.33.221  TCP    68 4444 → 55866 [ACK] Seq=1 Ack=13 Win=65152 Len=0 TSval=1054387964 TSecr=4059215960
797 2022-02-20 02:59:04.487209  138.68.92.163  134.122.33.221  TCP    68 4444 → 55866 [ACK] Seq=1 Ack=56 Win=65152 Len=0 TSval=1054388062 TSecr=4059216058
802 2022-02-20 02:59:11.302526  138.68.92.163  134.122.33.221  TCP    75 4444 → 55866 [PSH, ACK] Seq=1 Ack=56 Win=65152 Len=7 TSval=1054394877 TSecr=4059216058
805 2022-02-20 02:59:11.403417  138.68.92.163  134.122.33.221  TCP    68 4444 → 55866 [ACK] Seq=8 Ack=65 Win=65152 Len=0 TSval=1054394978 TSecr=4059222974
```

Tools of the Trade

- Nmap – Network Scanner
- Metasploit - Exploitation Framework
- Kali Linux - Specialized offensive security distribution
- Burp Suite - Web application security testing
- Nessus - Vulnerability scanner

Conclusion

Penetration Testing is building resilience in a system by simulating scope-defined attacks and providing remediation.

Plus you can tell your friends you’re an (***ethical***) hacker! 😎

Thank you!