

EVOLVE Security Academy

Presents:

How Hacking Works

Disclaimer

Don't try to hack into other companies or other peoples personal accounts.

It is illegal and you will be arrested.

Use your own lab.



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 / Spying
- 3. Hacktivism



Network Vulnerabilities

- Weak / Default Passwords
- Buffer Overflows
- Man in the middle attacks
- Default / Weak configurations
- Outdated software / Patch Management



Application Vulnerabilities

OWASP Top 10 2013

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross Site Request Forgery (CSRF)
- A9 Using Components with Known Vulnerabilities
- A10 Invalidated Redirects and Forwards



The Tools

- Port Scanner E.g. NMAP
- Vulnerability Scanner E.g. Nessus
- Exploitation Tool E.g. Metasploit
- Brute Force Hydra
- Network Analysis Wireshark



Great hackers don't rely on automated tools.



Typical Steps

- Identify target
 - Random OR Targeted
- Choose attack vector
 - External exploitable vulnerability
 - Social Engineering (Phishing email)
- Gain access & understand working system environment (root?)
- Establish foothold (install backdoor / persistence)
- Pivot throughout the network
- Exfiltration of data



Top Vulnerabilities

- Weak or Default Passwords
- JBoss
- Cross-site scripting



OK let's hack

- The set up
 - We are targeting a hospital for medical records (ransom)
 - IP address: 172.28.3.95
- Kali Linux will be our attacking host
 - Windows users: Download Putty
 - Mac users open Terminal
 - SSH to root@172.28.3.93
 - Password = 55555%%%%%%%



Discovery

- Port scan host 172.28.3.95
- NMAP
 - -# nmap 172.28.3.95
 - ssh root@172.28.3.95 -p222



Brute Force

- Password attack w/ Hydra
 - https://www.thc.org/thc-hydra/
 - Standard password list
 - # hydra -l root -P /usr/share/set/src/fasttrack/wordlist.txt 172.28.3.95 ssh -s 222



Pivoting

- From the inside
 - Social engineering
 - Email
 - Telephone
- From the outside
 - Vulnerabilities / Passwords



Take the data (Exfiltration)

First person who does it receives an Evolve t-shirt.

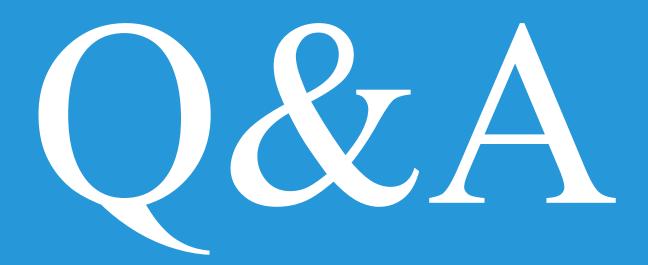


Evolve Academy Lab

Coming soon!



Thank you.





Contact

- Paul Petefish
 - Paul@EvolveAcademy.io
- Andrew Hamilton
 - Andrew@EvolveAcademy.io

www.EvolveAcademy.io

