EVOLVE

Security Academy

Presents:

Hacking 101

Disclaimer

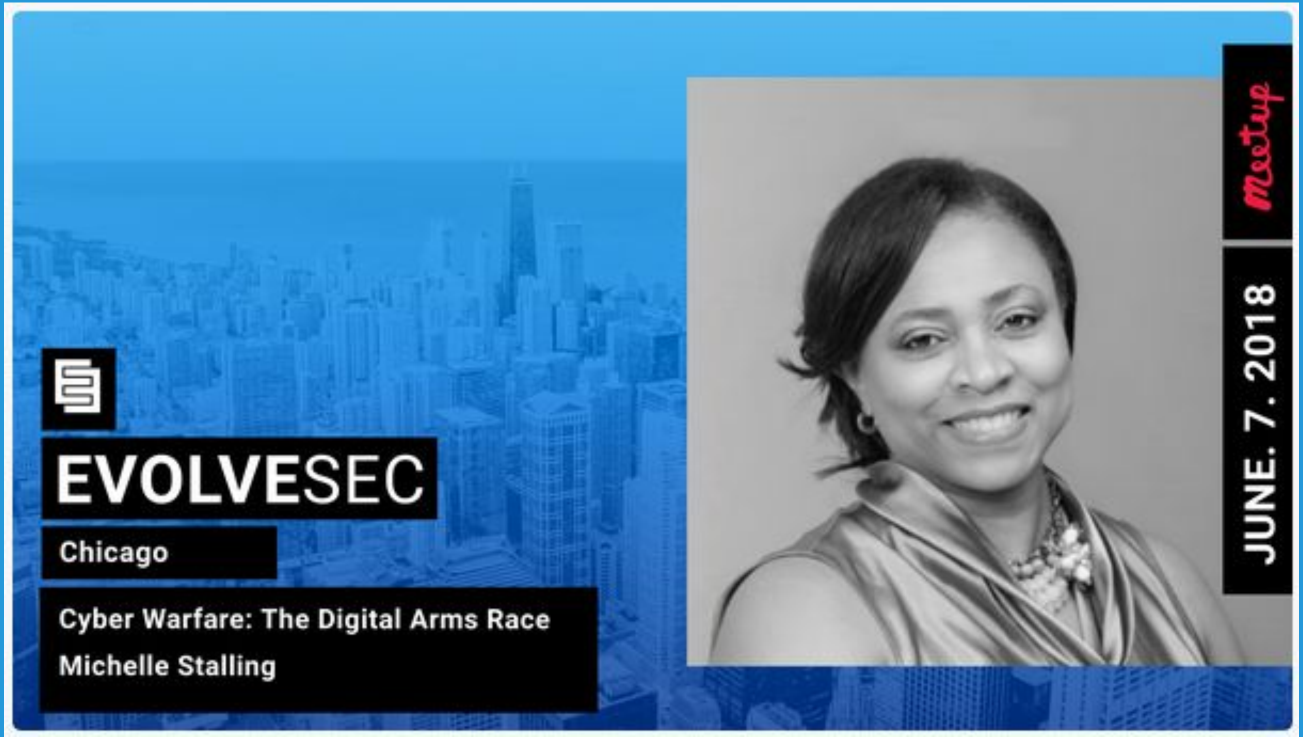
Don’t try to hack into companies or people’s personal accounts.

It is illegal and you will be arrested.

Use your own lab.

EVOLVE
Security Academy

Upcoming Evolve Event



EVOLVESEC

Chicago

Cyber Warfare: The Digital Arms Race

Michelle Stalling

JUNE. 7. 2018

Meetup

Windows Users

Please download PuTTY

https://www.putty.org/

Burpsuite

Download:

https://portswigger.net/burp/communitydownload

Brain Teaser

Use each of the numbers 1, 3, 4 and 6 only once using the four basic math operations to total the number 24.

Hacking

- 1960’s (MIT Model Railroad Club)
- Today
    1. Malicious/illegal activities
    2. Writing programs to solve complex problems well

Elite hackers don’t rely on automated tools.

Terms

- CIA Triad
- Vulnerabilities, Threats, Exploits
- Malicious code

Hats & Hacking

- White Hat
- Grey Hat
- Black Hat

Threat Actors

1. Script Kiddies
2. Hacktivism
3. Organized crime
4. Nation States (APTs)

Network Vulnerabilities

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- Outdated software / Patch Management

Application Vulnerabilities

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 and monitoring

Popularized Attacks

- DDOS
- Phishing
- Ransomware - Virus/Trojan

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

The Common Tools

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

OK let’s hack

www.overthewire.org

Let’s keep hacking

www.hackthis.co.uk

Challenges

hack.evolvesecurity.io

www.hackthebox.eu

Thank you.

Q&A

EVOLVE
Security Academy

Contact

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

www.EvolveAcademy.io

Brain Teaser Answer

$6 / (1 - (3/4))$