



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



The poster features a blue-tinted city skyline of Chicago in the background. On the left, there is a logo consisting of a stylized 'S' inside a square. Below the logo, the text 'EVOLVESEC' is displayed in large, bold, white capital letters. Underneath that, 'Chicago' is written in white. Further down, the title 'Cyber Warfare: The Digital Arms Race' and the name 'Michelle Stalling' are listed in white. On the right side, there is a black and white portrait of Michelle Stalling, a woman with dark hair, smiling. To the right of the portrait, the date 'JUNE. 7. 2018' is written vertically in white. Above the date, the word 'meetup' is written in a red, cursive font.


EVOLVESEC
Chicago
Cyber Warfare: The Digital Arms Race
Michelle Stalling

meetup
JUNE. 7. 2018

Windows Users

Please download PuTTY

<https://www.putty.org/>

Burpsuite

Download:

<https://portswigger.net/burp/communitydownload>



EVOLVE
Security Academy

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.



EVOLVE
Security Academy

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- Outdated software / Patch Management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



EVOLVE
Security Academy

Let's keep hacking

www.hackthis.co.uk



EVOLVE
Security Academy

Challenges

hack.evolvesecurity.io

www.hackthebox.eu



EVOLVE
Security Academy

Thank you.

Q&A



EVOLVE
Security Academy

Contact

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

www.EvolveAcademy.io



EVOLVE
Security Academy

Brain Teaser Answer

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

