Hacking Demystified: The Writer's Guide to Hacking and Cybercrime

Casey Smith
Warren Hammond
RMFW: Colorado Gold 2016

Industry Qualifications

Microsoft Certified Systems Expert: Server Infrastructure

Microsoft Certified Systems Expert: Private Cloud

Microsoft Certified Systems Expert: Enterprise Devices and Apps

Microsoft Certified Trainer

Cisco Certified Network Associate: Security

Certified Cisco Systems Instructor

Security+

Microsoft CISCO CompTIA

Warren Hammond

warrenhammond.net

warren.hammond@hotmail.com

facebook.com/warren.hammond

@whammondauthor

Industry Qualifications

Microsoft Certified Trainer*

Cisco Certified Network Professional*

Certified Cisco Systems Instructor*

Security+*

Information Security Analyst Financial Industry

*Former

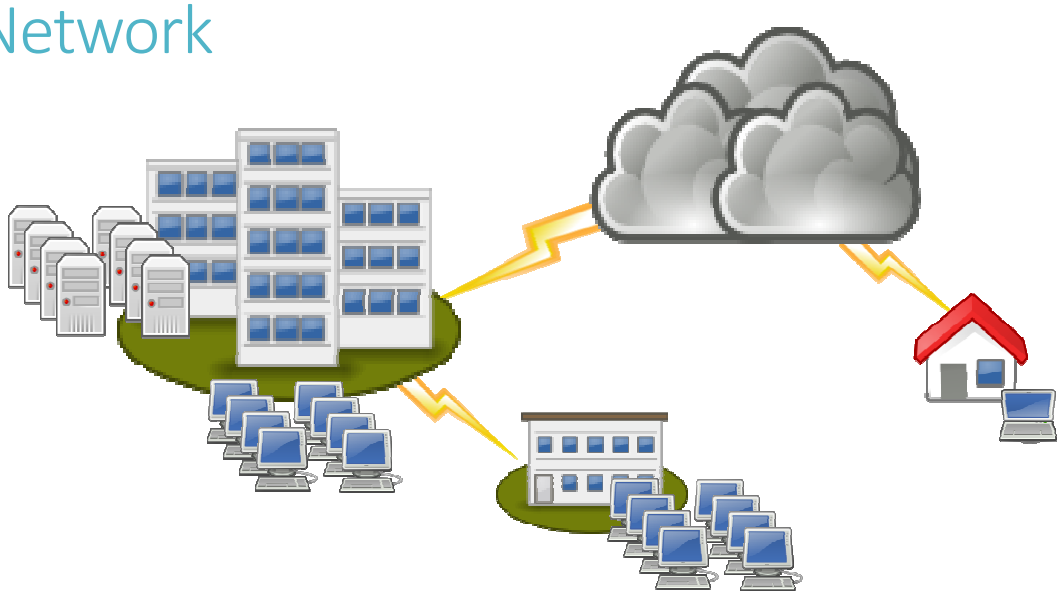
Casey Smith

github.com/subTee

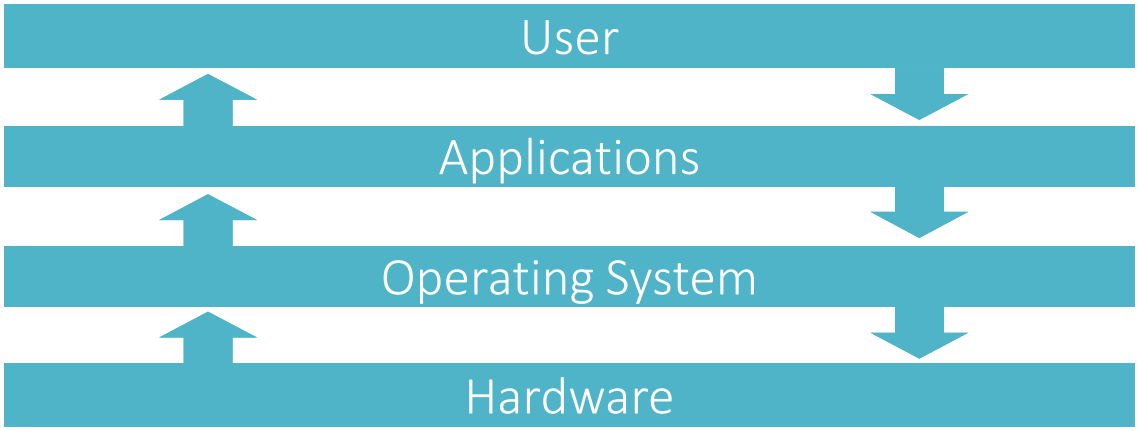
subTee@outlook.com

@subTee

Network



Computer architecture



Operating systems

Mobile (phones and tablets)	Computer (desktops and laptops)	Servers
• iOS • Android • Windows	• Windows • Mac OS X	• Windows Server • Linux/Unix

Applications

Mobile (phones and tablets)	Computer (desktops and laptops)	Servers
• Instagram • Facebook • Web browser • Snapchat • Twitter • Camera/gallery • Google Maps	• Word • Photoshop • Web browser • Outlook • InDesign • Scrivener • PowerPoint	• Email hosting • Web hosting • Directory services • Backup • Database • Imaging • Monitoring

Other network devices

- Router
- Switch
- Wireless access point (WAP)
- Cable/DSL modem
- Firewall

Types of hackers

Black hat

White hat

Adversaries/motivations

Nation state
Hacktivist
Cyberterrorist
Professional criminal
Corporate rival
Script kiddies

Passwords

Offense: password guessing, brute force, cracking

Defense: account lockout, complex passwords, multifactor authentication

Reconnaissance

Offense: network scanning, access public information

Defense: firewall, security policy

Software and applications

Offense: exploit, zero day

Defense: patch, intrusion prevention, exploit mitigation

Software and applications

Offense: malware, virus, worm, malicious file

Defense: anti-virus, application white-listing

Email

Offense: email spoofing, phishing

Defense: email server verification, digital signature, spam filters

Data

Offense: theft

Defense: permissions, encryption

Illicit activity

Offense: TOR, anonymization, hiding identity

Defense: source routing, java exploit

Network communication

Offense: man-in-the-middle, sniffing

Defense: certificate pinning, encryption (SSL), VPN

Wifi

Offense: sniffing, war driving, evil twin

Defense: complex passwords, encryption

Other terms

- Social engineering
- Denial of Service (DOS)
- Distributed Denial of Service (DDOS)
- Supply chain attack

- Honeypot
- Audit trail
- Watering hole
- De-militarized zone (DMZ)

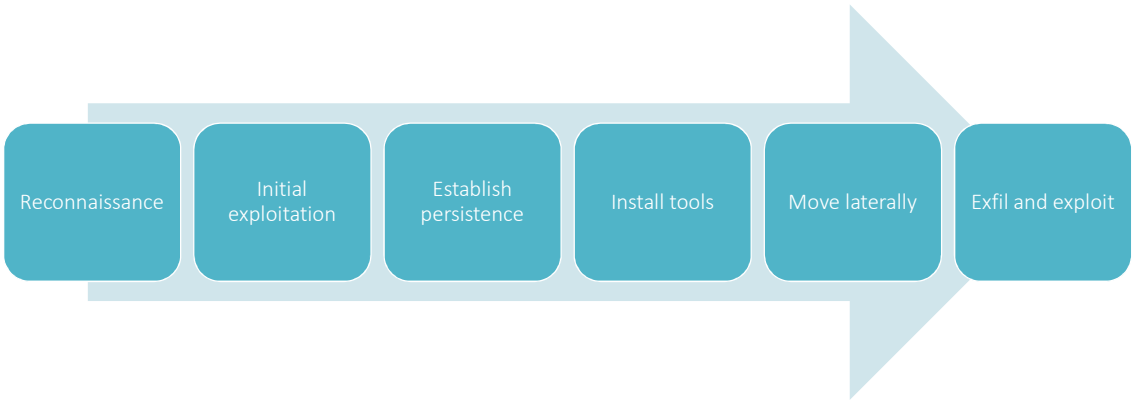
Other terms

Insider attack

Ransomware

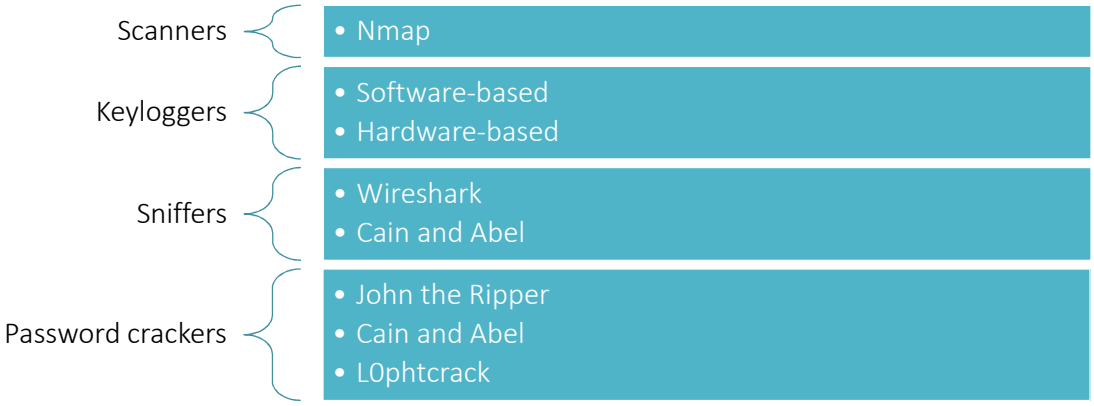
Dropped drive

Hacking phases



Rob Joyce, National Security Agency
https://www.youtube.com/watch?v=bDJb8WOJYdA

Hacking tools



Cringe-worthy moments in fiction

- Keep him/her talking so we can trace the call!
- Mocked up interfaces
- Technobabble
- Ridiculous on-screen pop-ups of villainy
- Two people/one keyboard

Myths

- Only Windows gets viruses
- Anti-virus software keeps a computer/network safe
- We haven't been hacked yet
- I'm safe as long as I don't open email attachments
- I'm not a target

Resources

Books:

The Cuckoo's Egg, Cliff Stoll
Hacking: The Art of Exploitation, Jon Erickson
Daemon, Daniel Suarez
Kingpin, Kevin Poulsen
Ghost In The Wires: My Adventures as the World's Most Wanted Hacker, Kevin Mitnick

Reference:

https://www.paloaltonetworks.com/threat-research/cybercanon

Reports:

APT1, Exposing One of China's Cyber Espionage Units – Mandiant February 2013

Questions