



# Cyber Security Simplified الأمن السيبراني مبسطا

INSTRUCTOR : KARAM LAHLOOB

# Contents



1. WHAT TYPE OF HACKER ARE YOU!
2. HOW HACKERS HACK
3. SOCIAL ENGINEERING
4. SOFTWARE VULNERABILITIES
5. MALWARE
6. CRYPTOGRAPHY
7. INTRUSION DETECTION/APTS
8. FIREWALLS
9. HONEYPOTS
10. PASSWORD HACKING
11. PENETRATION TESTING
12. SECURE OS
13. IOT HACKING
14. COMPUTER SECURITY EDUCATION
15. GUIDE FOR PARENTS WITH YOUNG HACKERS
16. HACKER CODE OF ETHICS

# 1. What Type of Hacker Are You!

- \* MOST HACKERS AREN'T GENIUSES
- \* DEFENDERS ARE HACKERS PLUS
- \* HACKERS ARE SPECIAL
- \* HACKERS ARE PERSISTENT
- \* HACKER HATS

# 2. How hackers hack



- \*THE SECRET TO HACKING
- \*THE HACKING METHODOLOGY
- \*HACKING IS BORINGLY SUCCESSFUL
- \*AUTOMATED MALWARE AS A HACKING TOOL
- \*HACKING ETHICALLY

# 3. Social Engineering

- \*SOCIAL ENGINEERING METHODS

- \*PHISHING

- \*TROJAN HORSE EXECUTION

- \*OVER THE PHONE

- \*PURCHASE SCAMS

- \*IN-PERSON

- \*CARROT OR STICK

- \*SOCIAL ENGINEERING DEFENSES

- \*BE CAREFUL OF INSTALLING SOFTWARE FROM THIRD-PARTY WEBSITES

- \*EV DIGITAL CERTIFICATES

- \*GET RID OF PASSWORDS

- \*ANTI-SOCIAL ENGINEERING TECHNOLOGIES



# 4. Software Vuln

- \*NUMBER OF SOFTWARE VULNERABILITIES
- \*WHY ARE SOFTWARE VULNERABILITIES STILL A BIG PROBLEM
- \*DEFENSES AGAINST SOFTWARE VULNERABILITIES
- \*SECURITY DEVELOPMENT LIFECYCLE
- \*CODE AND PROGRAM ANALYSIS
- \*THIRD-PARTY PROTECTIONS AND VENDOR ADD-ONS

# 5. Malware

- \*MALWARE TYPES
- \*NUMBER OF MALWARE PROGRAMS
- \*MOSTLY CRIMINAL IN ORIGIN
- \*DEFENSES AGAINST MALWARE
- \*FULLY PATCHED SOFTWARE
- \*TRAINING
- \*ANTI-MALWARE SOFTWARE
- \*APPLICATION CONTROL PROGRAMS
- \*SECURITY BOUNDARIES
- \*INTRUSION DETECTION

# 6. Cryptography

- \*WHAT IS CRYPTOGRAPHY
- \*WHY CAN'T ATTACKERS JUST GUESS ALL THE POSSIBLE KEYS
- \*SYMMETRIC VERSUS ASYMMETRIC KEYS
- \*POPULAR CRYPTOGRAPHY
- \*HASHES
- \*CRYPTOGRAPHIC USES
- \*CRYPTOGRAPHIC ATTACKS
- \*MATH ATTACKS
- \*KNOWN CIPHERTEXT/PLAINTEXT
- \*SIDE CHANNEL ATTACKS
- \*INSECURE IMPLEMENTATIONS



# 7. Intrusion Detection/APTs

- \*EVENT MESSAGE
- \*ADVANCED PERSISTENT THREATS (APTS)
- \*TYPES OF INTRUSION DETECTION
  - \*BEHAVIOR-BASED
  - \*SIGNATURE-BASED
- \*INTRUSION DETECTION TOOLS AND SERVICES
- \*INTRUSION DETECTION/PREVENTION SYSTEMS
- \*EVENT LOG MANAGEMENT SYSTEMS
- \*DETECTING ADVANCED PERSISTENT THREATS (APTS)

# 8. Firewalls

- \*WHAT IS A FIREWALL
- \*FIREWALL RULES
- \*WHERE ARE FIREWALLS
- \*ADVANCED FIREWALLS
- \*WHAT FIREWALLS PROTECT AGAINST

# 9. Honeypots

- \*WHAT IS A HONEYPOT
- \*INTERACTION
- \*WHY USE A HONEYPOT
- \*HONEYPOT RESOURCES TO EXPLORE

# 10. Password Hacking

- \*AUTHENTICATION COMPONENTS
- \*PASSWORDS
- \*AUTHENTICATION DATABASES
- \*PASSWORD HASHES
- \*AUTHENTICATION CHALLENGES
- \*AUTHENTICATION FACTORS
- \*HACKING PASSWORDS
- \*PASSWORD GUESSING
- \*PHISHING
- \*KEYLOGGING
- \*HASH CRACKING
- \*CREDENTIAL REUSE
- \*HACKING PASSWORD RESET PORTALS
- \*PASSWORD DEFENSES
- \*ACCOUNT LOCKOUT
- \*DON'T USE PASSWORDS
- \*CREDENTIAL THEFT DEFENSES

# 11. Penetration Testing

- \*MY PENETRATION TESTING HIGHLIGHTS
- \*HACKED EVERY CABLE BOX IN THE COUNTRY
- \*HACKED A MAJOR CREDIT CARD COMPANY
- \*CREATED A CAMERA VIRUS
- \*HOW TO BE A PEN TESTER
- \*HACKER METHODOLOGY
- \*GET DOCUMENTED PERMISSION FIRST
- \*GET A SIGNED CONTRACT
- \*REPORTING
- \*CERTIFICATIONS
- \*BE ETHICAL
- \*MINIMIZE POTENTIAL OPERATIONAL INTERRUPTION
- \*



# 12. Secure OS

- \*HOW TO SECURE AN OPERATING SYSTEM
- \*SECURE-BUILT OS
- \*SECURE GUIDELINES
- \*SECURE CONFIGURATION TOOLS
- \*SECURITY CONSORTIUMS
- \*TRUSTED COMPUTING GROUP
- \*FIDO ALLIANCE

# 13. IOT Hacking

\*HOW DO HACKERS HACK IOT

\*IOT DEFENSES

# 14. Computer Security Education

- \*COMPUTER SECURITY TRAINING TOPICS
  - \*END-USER/SECURITY AWARENESS TRAINING
  - \*GENERAL IT SECURITY TRAINING
  - \*INCIDENT RESPONSE
  - \*OS AND APPLICATION-SPECIFIC TRAINING
  - \*TECHNICAL SKILLS
  - \*CERTIFICATIONS
- \*TRAINING METHODS
  - \*ONLINE TRAINING
  - \*BOOKS

# 15. Guide for Parents with Young Hackers

- \*SIGNS YOUR KID IS HACKING
- \*THEY TELL YOU THEY HACK
- \*OVERLY SECRETIVE ABOUT THEIR ONLINE ACTIVITIES
- \*THEY HAVE MULTIPLE EMAIL/SOCIAL MEDIA ACCOUNTS YOU CAN'T ACCESS
- \*YOU FIND HACKING TOOLS ON THE SYSTEM
- \*NOT ALL HACKING IS BAD
- \*HOW TO TURN AROUND YOUR MALICIOUS HACKER
- \*GIVE GUIDANCE
- \*GIVE LEGAL PLACES TO HACK
- \*CONNECT THEM WITH A GOOD MENTOR

# 16. Hacker Code Of Ethics



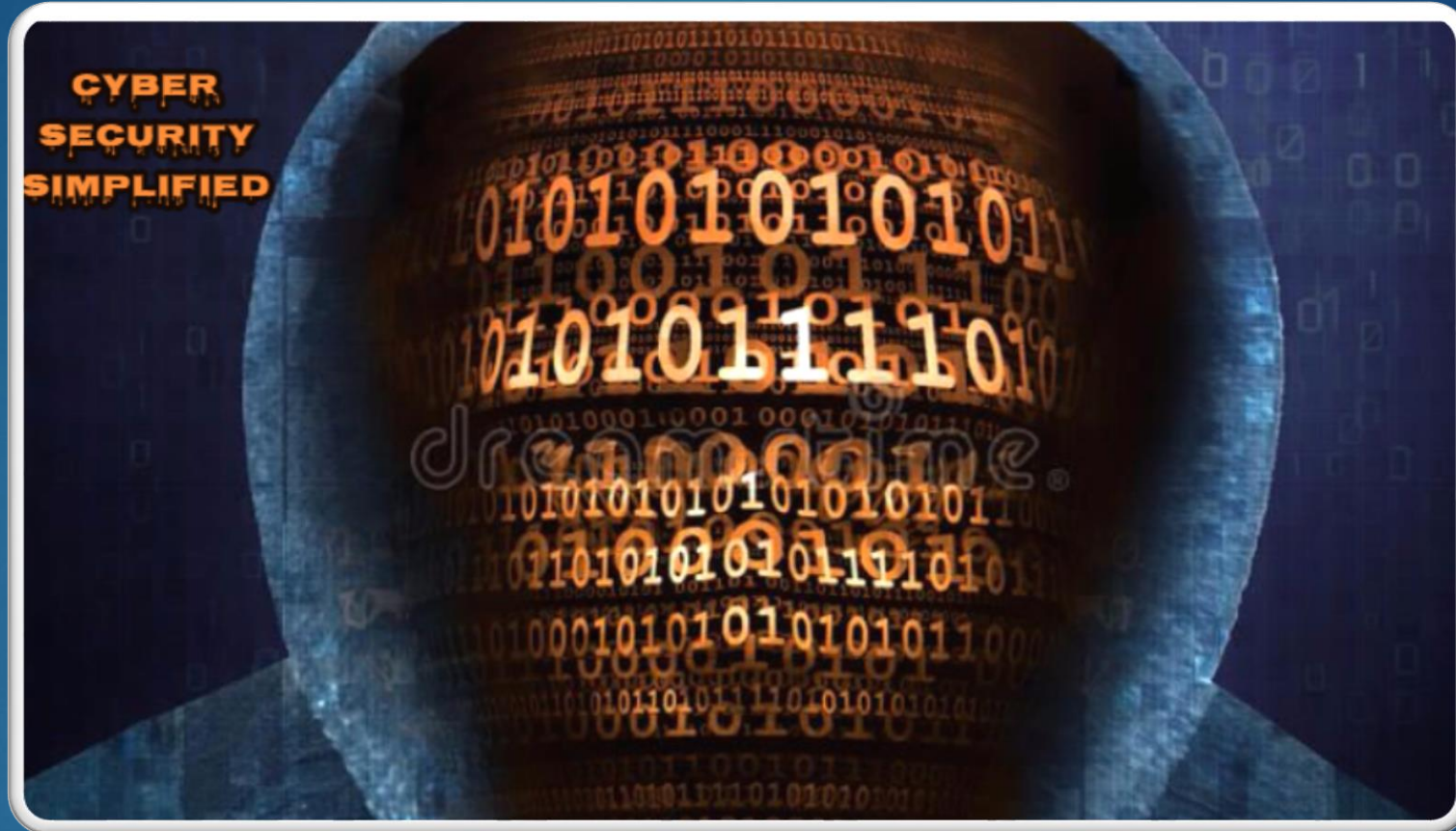
- \*HACKER CODE OF ETHICS
- \*BE ETHICAL, TRANSPARENT, AND HONEST
- \*DON'T BREAK THE LAW
- \*GET PERMISSION
- \*BE CONFIDENTIAL WITH SENSITIVE INFORMATION
- \*DO NO GREATER HARM
- \*CONDUCT YOURSELF PROFESSIONALLY
- \*BE A LIGHT FOR OTHERS



# Index

- ▶ Hacking the Hacker: Learn from the Experts Who Take Down Hackers, Roger A. Grimes © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana
- ▶ EC-Council
- ▶ ISACA
- ▶ ISC
- ▶ SANS Institute
- ▶ CISCO

# END OF THE COURSE



► INSTRUCTOR : KARAM LAHLOOB