UOW
MALAYSIA
KDU PENANG
UNIVERSITY COLLEGE

PART OF THE UNIVERSITY
OF WOLLONGONG AUSTRALIA
GLOBAL NETWORK

Fundamentals of Security in Ethical Hacking

DCS22104

Lesson 4: Social engineering attacks

Department of Computing

Course outline

Week	Topic
1	Introduction to ethical hacking and reconnaissance
2	Network enumerators and system vulnerabilities
3	Malware
4	Social engineering attacks
5	Hacking web servers and web applications
6	Session hijacking
7	Script injections
8	Hacking wireless network
9	Buffer overflow attacks
10	Cryptography
11	Evading IDS, firewall, and honeypot
12	Penetration testing

Assessments

#	Components	Marks(%)	Week
1	Test 1 (Topics 1 to 5)	10	6
2	Midterm examination	20	7
3	Test 2 (Topics 1 to 11)	20	12
4	Final examination	50	Exam week

Reviews on lesson 3

- Malicious software. It is a malicious file which contains an executable or binary file. The file will not be executed unless it is opened by a user.
- Seven behaviours of malware include Trojan, zombie, rabbit, worm, spyware, ransomware, and time bomb or logic bomb.
- Trojan remains stealth or looks unharmed. It is mainly used to create backdoors.
- Spyware acts as a normal software. It is mainly used to log information in the victim's computer.

Reviews on lesson 3

- Worm malware spreads across a computer network, usually via emails.
- Rabbit malware replicates itself to form buffer overflow attacks.
- Ransomware locks user access in an operating system, need to follow certain instructions to unlock.
- Four approaches to detect a malware:

a. Real time antivirus protection.

b. Cryptograhic protocols. ie. TLS, SSL, CURL to protect files from injections with malware by the malicious party.

c. Cryptographic checksum to match file with the original checksum, and to avoid malware being installed in the victim's computer.

d. Firewall protection, where suspicious files will be dropped at the transport layer.

Topic learning outcomes

1. Define the authentication protocols and processes for human.

2. Discover the types of authentication and role of access control in safeguarding the information.

Lesson 4: Lecture and lab sessions

Start time	End time	Topics
1:00pm	1:30pm	Reviews on Lesson 3
1:30pm	2:00pm	Lecture 1: **Social engineering attacks**
2:00pm	2:15pm	Break time
2:15pm	2:45pm	Lecture 2: **Authentication and access control**
2:45pm	2:50pm	References

Lecture 1: Social engineering attacks

People

- Human being can be manipulated.
- Presumed to be innocent in nature.
- Naturally trusting others, want to be helpful, and courteous.
- Social engineering is a method of attack in which the attacker takes advantage of these human psychological traits.

Insiders

- People who work inside an organization are more familiar about the company internal operations as compared to outsiders.
- Insider have more privileges to access to company assets.
- Insider misbehaved due to either greediness or threaten.

Computer forensics

- They establish facts to information security incident.
- Gather evidence on circumstances of
    (a) How the breach is happened?
    (b) Who is responsible for the breach?
- Establish legal guilt or innocence for a security breach.
- They have no privileges to collect all information in a computer network.

Attacks on Privacy

- **Voice phishing (Vishing)**, using voice to lure information by simply asking.
- **Photographing**, taking photos using a camera without consent and obtain permission from a person.
- **Voice recording**, record voices using a recorder without consent and obtain permission from a person.
- **Fingerprint forgery**, retrieve a copy of an authentic print from a person.
- **Space and time invasion**, intercept and distract someone for a specific duration of time to create a window of opportunity to hack.

Voice phishing (Vishing)

Exercise 1 (10 minutes)

1. How a hacker can sniff personal information through social engineering?

2. State three vulnerabilities of a human.

3. State three job descriptions for a computer forensics.

Break time

Duration: 15 minutes.

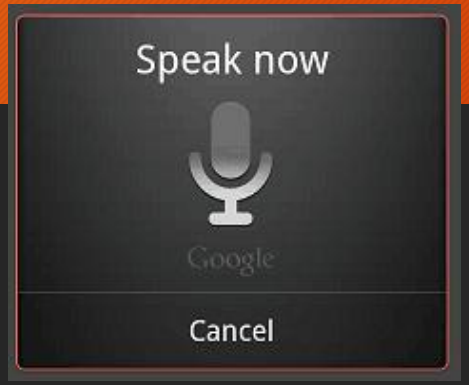
Lecture 2: Authentication and access control

Authentication

- Additional clearance to verify a user whether he/she is a legitimate user or an illegal user.
- Authentication methods includes:

No.	Methods	Description
1	One-time password (OTP)	A generated pass code to be used upon request only.
2	Synchronous tokens	Current time is embedded in the pass code.
3	Challenge response authentication	System will provide a set of questions and user have to provide valid answers. (i.e. Q&A and CAPTCHA)
4	Response generating tokens	Interactive features, such as image selection, solve a puzzle, and voice verification.
5	Continuous authentication	Time out or need further verification from time to time.
6	Multi-authentication	Passwords, biometric, machine-to-machine re-authentication.

Biometrics



- Human characteristics as authentication.
- Biometrics machine included
  - (a) Fingerprint reader
  - (b) Iris scanner
  - (c) Facial recognition
  - (d) Palm recognition
  - (e) Voice recognition
  - (f) DNA scanner

Palm scanner

Retinal scanner

Principle of least privilege

- Prevent up to 90% of malicious code attacks.
- Difficult for malware to impact critical parts.
- Prevent non-administrative users from installing unknown programs.
- Allows security personnel to focus their efforts on fewer points of attack.

Exercise 2 (10 minutes)

State and explain five methods of authentication.

References

- CEH course materials
- Goodrich, M (2010) *Introduction to Computer Security*, Addison Wesley, 1st Ed
- Purpura, P (2010) Security: An Introduction, CRC Press, 1st Ed
- Stallings, W (2007) Computer Security: Principles and Practices, Prentice Hall, 1st Ed
- Jacobson, D (2008) Introduction to Network Security, Chapman and Hall, 1st Ed
- Fischer, R (2008) Introduction to Security, Butterworth-Heinemann, 8th Ed