UOW
MALAYSIA
KDU PENANG
UNIVERSITY COLLEGE

PART OF THE UNIVERSITY
OF WOLLONGONG AUSTRALIA
GLOBAL NETWORK

# Fundamentals of Security in Ethical Hacking

DCS22104

Lesson 3: Malware

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 2

1. Internet protocol (IP) addresss is a numerical identifier for a device in a network.
2. IPv4 and IPv6 are the protocol formats used to transmit from one IP to another.
3. Host is a device that is connected to a network.
4. A host with IPv4 can have up to 2^16 = 65,536 or 16 bits port numbers. Since IPv4 has address size of 32 bits = 16 bits network IP + 16 bits device IP.
5. A host with IPv6 can host 2^64 = 18,446,744,073,709,551,616 or 64 bits port numbers. Since IPv6 has address size of 128 bits = 64 bits network IP + 64 bits device IP.
6. A network service is an application programming interface (API).
7. Network enumerator is a tool to scan a computer network. E.g. NMAP.
8. Basic search parameters that can be found using a network enumerator are service name (Services that is available), port number, ping sweep (network connectivity), domain name & traceroute table.

# Topic learning outcomes

1. Identify the type of a malware based on its behaviours.

2. Explain the strategy on how to detect malicious code.

# Lesson 3: Lecture and lab sessions

| Start time | End time | Topics |
|---|---|---|
| 1:00pm | 1:30pm | Reviews on Lesson 2 |
| 1:30pm | 2:00pm | Lecture 1: **Malware** |
| 2:00pm | 2:15pm | Break time |
| 2:15pm | 2:45pm | Lecture 2: **Malware detection** |
| 2:45pm | 2:50pm | References |

# Lecture 1: Malware

# Malware I

- It is a shortened form for malicious software.
- Sometimes it refers to computer virus.
- It is a malicious file which contains an executable file.
- The file will not be executed unless it is opened by a user.
- Virus behaviours consisted of **Trojan**, **worm**, **time bomb**, **zombie**, **rabbit**, **ransomware**, and **spyware**.

# Malware II

- It can infect any hardware and software platform.
- It modifies hidden and read-only files.
- It appears anywhere in a system.
- It spread anywhere where sharing occurs.
- It cannot remain in volatile memory after a completed reboot.
- It can be malevolent, benign or benevolent.
- Firmware viruses exist.

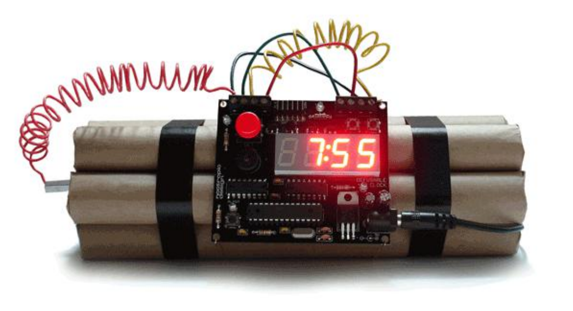
# Behaviour I: Trojan

- It appears to be unharmed to a computer.
- Main purpose is to create backdoors for malicious party.
- i.e. TR/Crypt.XPACK.Gen2 found in the Arduino software.

# Behaviour II: Worm

- It spread virus across a network or the Internet.
- It needs a protocol to propagate the virus either via email, messenger, or SMS.
- i.e. Worm/Brontok.C spread via email.

# Behaviour III: Time Bomb



- Also called logic bomb.
- The virus executes at a specific event/ time.
- It automatically reset system settings, such as reset system clock.
- Worse of all, it could erase data in the hard drives.

# Behaviour IV: Slave/ Zombie

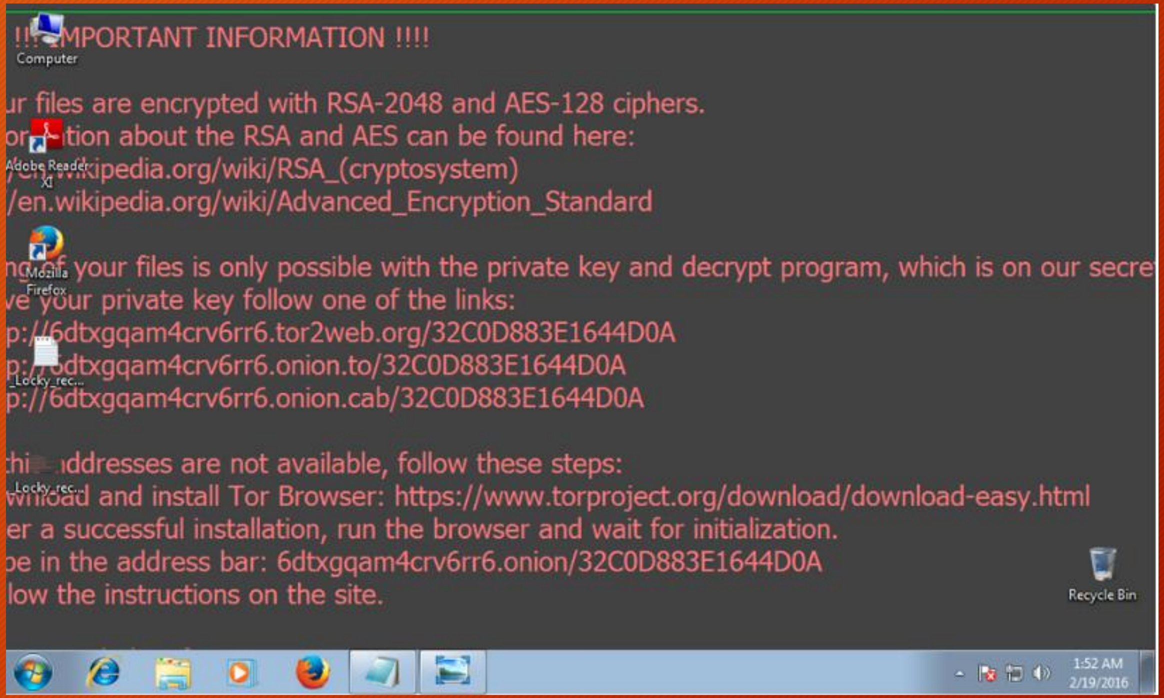
- A computer or a host that become a carrier for a virus.
- May be used to generate backdoors from a Trojan file.
- May be used to launch distributed denial-of-service (DDOS) attacks.

# Behaviour V: Rabbit

- Also called computer backteria.
- A virus that replicate itself to form buffer overflow attacks.
- Slow down the performance of a computer.
- i.e. plant viruses in every folder in an operating system.

# Behaviour VI: Ransomware

- Lock user access, need to follow certain instructions to unlock.
- Demand either for questionnaire, spread the virus or even money.
- i.e. Locky.



!! MPORTANT INFORMATION !!!!

ur files are encrypted with RSA-2048 and AES-128 ciphers.
or tion about the RSA and AES can be found here:
/en.wikipedia.org/wiki/RSA_(cryptosystem)
/en.wikipedia.org/wiki/Advanced_Encryption_Standard

n f your files is only possible with the private key and decrypt program, which is on our secre
ve your private key follow one of the links:
p://6dtxgqam4crv6rr6.tor2web.org/32C0D883E1644D0A
p: dtxgqam4crv6rr6.onion.to/32C0D883E1644D0A
p://6dtxgqam4crv6rr6.onion.cab/32C0D883E1644D0A

thi ddresses are not available, follow these steps:
wnload and install Tor Browser: https://www.torproject.org/download/download-easy.html
er a successful installation, run the browser and wait for initialization.
pe in the address bar: 6dtxgqam4crv6rr6.onion/32C0D883E1644D0A
low the instructions on the site.

# Behaviour VII: Spyware

- Sometimes refer to keylogger.
- Monitor and collect user information without consent from the user.
- i.e. TR/Spy.Gen found in a DVD ripper software.

# Exercise 1 – Malware behaviours (10 minutes)

1. What is malware?
2. List seven behaviours of a malware.
3. Explain a Trojan.
4. Explain a spyware.
5. Explain a worm malware.
6. Explain a rabbit malware.
7. Explain a ransomware.

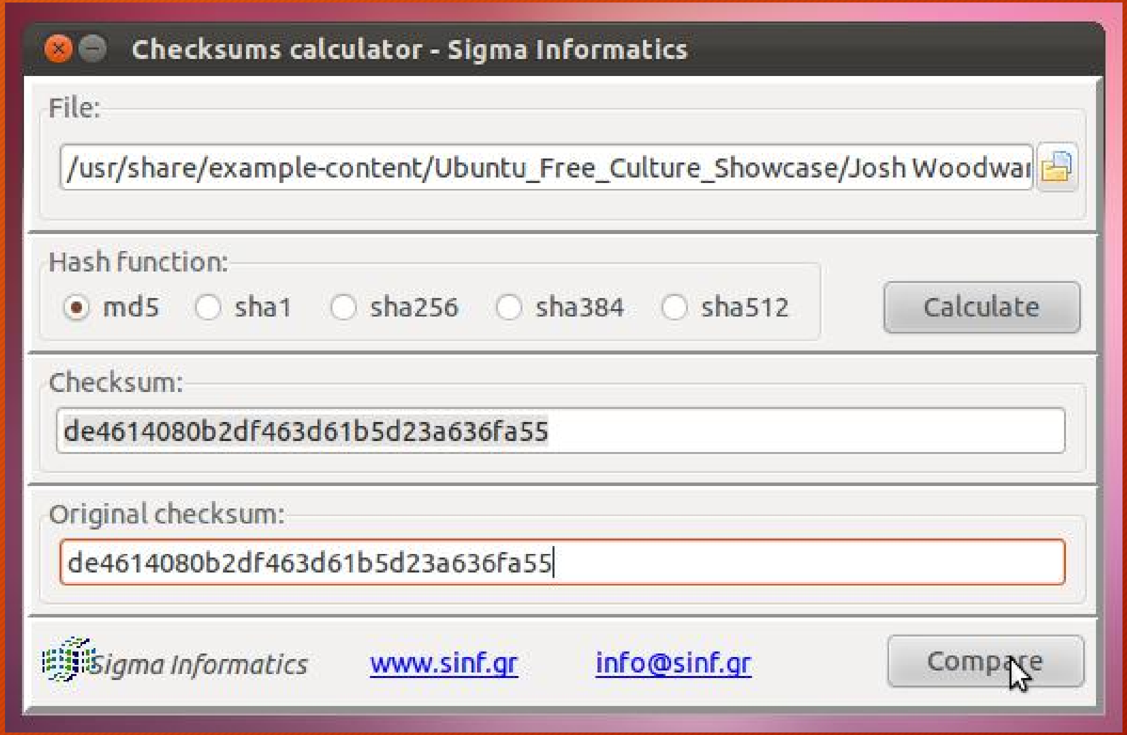
# Break time

Duration: 15 minutes.

# Lecture 2: Malware detection

# I. Cryptographic checksum

- Bit comparison using a checksums calculator.
- Checksums calculator in Ubuntu Linux.



Checksums calculator - Sigma Informatics

File:

/usr/share/example-content/Ubuntu_Free_Culture_Showcase/Josh Woodwar

Hash function:

● md5 ○ sha1 ○ sha256 ○ sha384 ○ sha512

Checksum:

de4614080b2df463d61b5d23a636fa55

Original checksum:

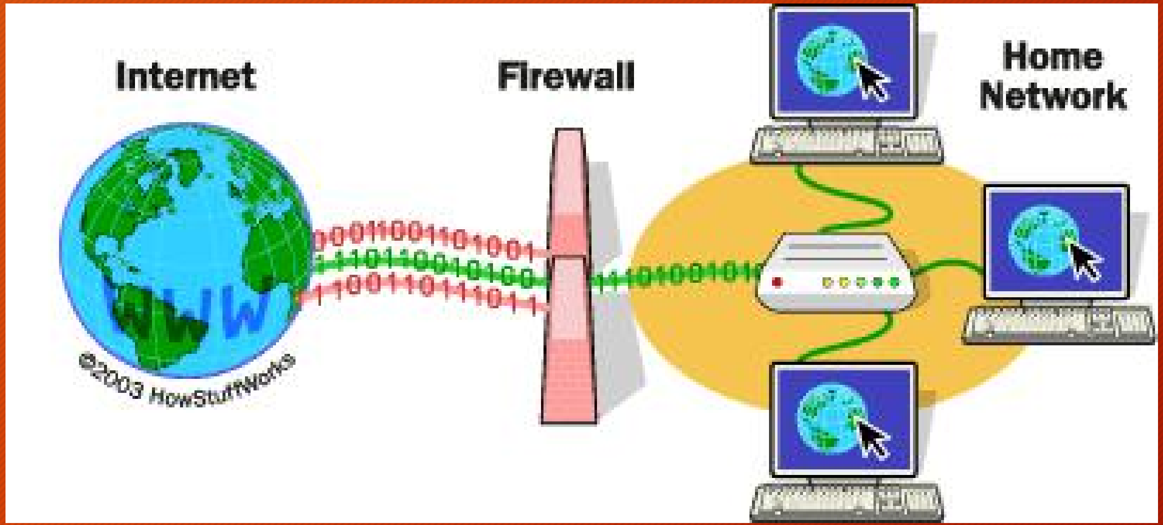
de4614080b2df463d61b5d23a636fa55

# II. Real Time Antivirus Protection

- Scan files in the current opened folder.
- If a malware is found, the antivirus should be able to intercept, provoke from user access and wait for user action.
- User able to choose to either do nothing, quarantine or remove.

# III. Firewall

- Install a firewall to prevent unauthorized access.
- Discard suspicious TCP and UDP packets.
- Prevent flooding and port scanning.



# IV. Cryptographic Protocols

- Encrypt file before sending over to the Internet.
- Secure Socket Layer (SSL)/ Transport Layer Security (TLS) protocols can be used to encrypt email, fax, instant messaging and voice-over IP (VoIP).

# Exercise 2 – Detect a malware (10 minutes)

List four approaches to detect a malware.

# Malware information

- Avira Virus Lab
- Kaspersky Lab
- Symantec

# 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