Name: Sachin Saj T K

Roll No: CB.EN.P2CEN18012 (10 digit number)

Date of Submission: 29/5/2019

==========

!!! STRICTLY DO NOT COPY PASTE FROM GOOGLE !!!

ANSWER ALL THE TASKS IN ONE OR TWO LINES WITH APPROPRIATE IMAGES (IF, NECESSARY)

==========

01TASK01: ATTACKS

Google for any one recent HACKING ATTACK and mention in few words about the following categories.

1. Attack name :
   Ransomware : LockerGoga
2. Attack source (hacker group/agency and motive behind it) :
   No Information about the hacker group. Their motive was to negotiate the price by asking the affected companies to contact them via email.
3. Technology involved (algorithm, port, protocols, services)
   AES- 256 or RSA-4096 algorithms
4. Attack pattern (how it works, flow, steps) Hack value ($ or Rupees) :
   a. Modifies the user accounts in the infected system by changing their passwords
   b. It would relocate itself into a temp folder then rename itself using cmd.
   c. LockerGoga encrypts files stored on the system.
   d. Each time time LockerGoga encrypts a file, a register key *(HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session00{01-20}* is modified
   e. After the encryption process, LockerGoga leaves a ransom note in a text file (README_LOCKED.txt) in the desktop.
5. Vulnerability (what was the weakness in victim side)
   Wi-Fi and/or Ethernet Network adapters.
6. Exploit (How victim is attacked, What is the threat in it)
   a. Attempt to disable Wifi and/or Ethernet network adapters through *CreateProcessW* function
   b. This will disconnect the system from any outside connection.
7. Payload (what is the code used like word.docx with macro, filename.vbs, mail.exe)
   They have been written in C++ using some well known helper libraries such as Boost and Crypto++(CryptoPP)
8. Is it a zero day attack (if YES mention the Zero day, if NO mention any such attacks done earlier)
   NO.
9. Source code (if available, mention the URL)
   https://github.com/sirpedrotavares/SI-LAB-Yara_rules/blob/master/LockerGoga

==========

01TASK02: KEYWORKS

Give an **example/concept for each** keyword given below

1. Zero-Day Attack (name) : Is a cyber-attack that occurs on the same day a weakness is discovered in software. At that point, it is exploited before a fix becomes available from its creator.
2. Daisy Chaining (real world scenario) : gaining access to one network and/or computer.
3. Doxing (perform a doxing on "michelleobama" and list all her details publicly available in the internet): Publishing personally identifiable information.
4. List any 5 well known Bots : Bot Virus, Bot DDOS, Bot Phisher, Bot Spyware, Bot Sniffer
5. Confidentiality: Information is accessible only to those Authorized to have access
6. Availability: Information are accessible when required by the authorized users.
7. Integrity: The trustworthiness of the data or resources
8. Authenticity: Data that ensures the quality of being genuine.
9. Non-Repudiation: is the assurance that someone cannot deny the validity of something.
10. List any 2 APT
    Total Site Takeover
    Intellectual property theft
11. List top 10 viruses of all time
    Conficker
    ILOVEYOU
    Morris Worm
    Mydoom
    Stuxnet
    CryptoLocker
    Sasser & Netsky
    Anna Kournikova
    Storm Worm
    Brain
12. List top 5 worms of all time
    Morris
    ILOVEYOU
    Nimda
    Code Red
    Melissa
13. Insider Attack: is a malicious threat to an organization that comes from people within the organization such as employees, who has inside information of the organization.
14. Network threat: is a malicious threat that comes from network, which can cause serious damage.
15. Host Threat: An host that may or may not happen, but has the potential to cause serious damage.
16. Application Threat: An application that may or may not happen, but has the potential to cause serious damage.
17. Operating system vulnerability : Weakness in operating system, which can be exploited by an attacker.
18. Web Application: Is a software application that runs on a remote server
19. Web Browser: Is a software application for accessing information on world wide web.
20. Web Server : To serve the files that form Web pages to users, in response to their requests.

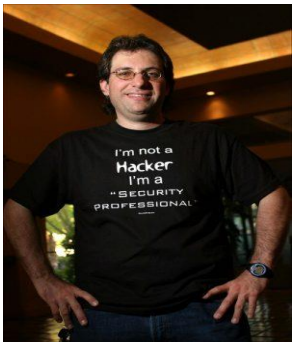
21. Security policy and its types:
    Firewall Policy
    Intrusion Prevention Policy
    Application and Device control
    Virus and spyware Protection Policy
22. Disaster recovery : Allows an organization to maintain or quickly resume mission-critical functions following a disaster.
23. EISA : is a part of enterprise architecture focusing on information security throughout the enterprise.
24. DMZ : is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the internet.
25. Physical security :
    describes measures designed to ensure the physical protection of IT assets from damage and unauthorized physical access.
26. Incident response team :
    Is a group of people who prepares for and respond to any emergency incident. Eg Cyber attacks
27. Blue team Vs Red team :
    Red team attacks something and blue team defend it.
28. Types of PEN TEST :
    Black Box Penetration Testing
    White Box Penetration Testing
    Grey Box Penetration Testing
29. Abbreviate (CEH, CHFI, ECSA, LPT, OWASP, OSSTMM, ISSAF, PCI-DSS, ISO-IEC, HIPPA, SOX, DMCA, FISMA)
    CEH : Certified Ethical Hacker
    CHFI : Computer Hacking Forensic Investigator
    ECSA : EC-Council Certified Security Analyst
    LPT : Licensed Penetration Tester
    OWASP : Open Web Application Security Project
    OSSTMM: Open Source Security Testing Methodology Manual
    ISSAF : Information Systems Security Assessment Framework
    PCI-DSS : Payment Card Industry Data Security Standard
    ISO-IEC: International Organization for standardization- International Electro technical Commision
    HIPPA : Health Insurance Portability and Accountability Act 1996
    SOX : Sarbanes-Oxley Act
    DMCA : Digital Millennium Copyright Act
    FISMA : Federal Information Security Management act
30. Ransomware : Type of Malicious software, designed to deny access to a computer system or data until ransom is paid.

==========

01TASK03: HACKERS (collect names with photos preferably)

Name any 5 real world hackers of the following types:

1. Black hats
    a. Kevin Mitnick



    b. Vladimir Levin

    c. Mathew Bevan

    d. Michael Calce

e. Adrian Lamo

2. White hats

a. Kevin Mitnick

b. Joanna Rutkowska

c. Charlie Miller

d. Greg Hoglund

e. Tsutomu Shimomura

3. Grey hats
    a. Vladmir Levin
    b. Max ray butler
    c. Syrian electronic army
    d. Astra
    e. Adrian Lamo

Name any 2 real world hackers of the following types:

1. Suicide hackers –Adrian Lamo, Leanson James Ancheta
2. Script kiddies – Betsy Davies, Reuben Paul
3. Cyber terrorists – Pak Cyber army protector of Indian cyberspace, lizard squad
4. State sponsored hackers – Hidden Lynx (China), Bureau 121 Pyongyang (North Korea)
5. Hactivist – Anonymous, Morpho

==========

01TASK03: STEPS IN HACKING

Explain a case on your own with respect to all these 5 hacking steps in order. (like if you are hacking into ABC corporation, how will you follow the steps)

1. Reconnaissance

   It is a preparatory phase, where the attackers seeks to gathering information about the target before launching the attack. Firstly, collect all the information's related to the ABC corporation. The information can be acquired either by passive reconnaissance or active reconnaissance.

2. Scanning

   This is termed as pre-attack phase, first we will scan the network for specific information on the basis of information gathered during reconnaissance. Scanning can include use of dialers, port scanners, network mappers, ping tools, vulnerability scanner, etc. Then we have to extract information such as live machines, port, port status, OS details, device type, system uptime etc, so that we can launch an attack.

3. Gaining access

   Gaining access refers to the point where we can have access to the operating system or application on the victim computer or network, then we can escalate privileges to obtain complete control of the system.

4. Maintaining access

   This refers to the phase when we can retain ABC corporation's ownership of the system, by keeping Backdoors, rootkits or Trojans, which will help in securing exclusive access. Through we can upload, download or manipulate data, application and configure the system.

5. Clearing tracks

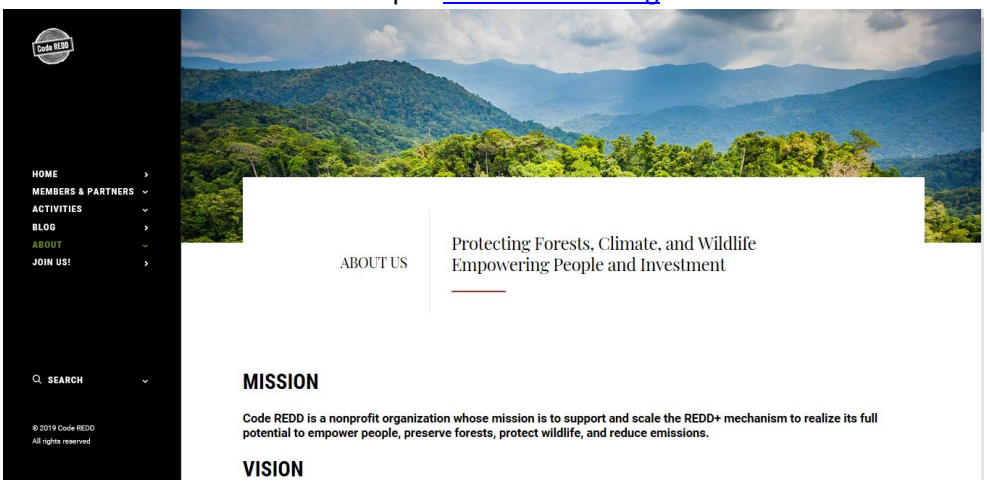
   This is a process in which we hide all the malicious acts, through this act we can be continuously remain unnoticed and uncaught by deleting evidence that might lead to our prosecution

==========

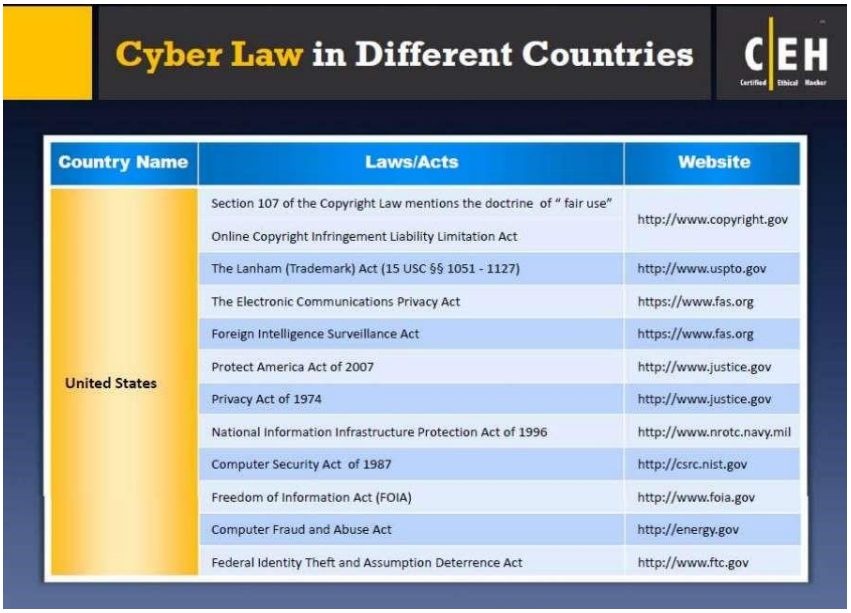
01TASK04: VISIT THE WEBSITES

04.01

Example: www.codredd.org

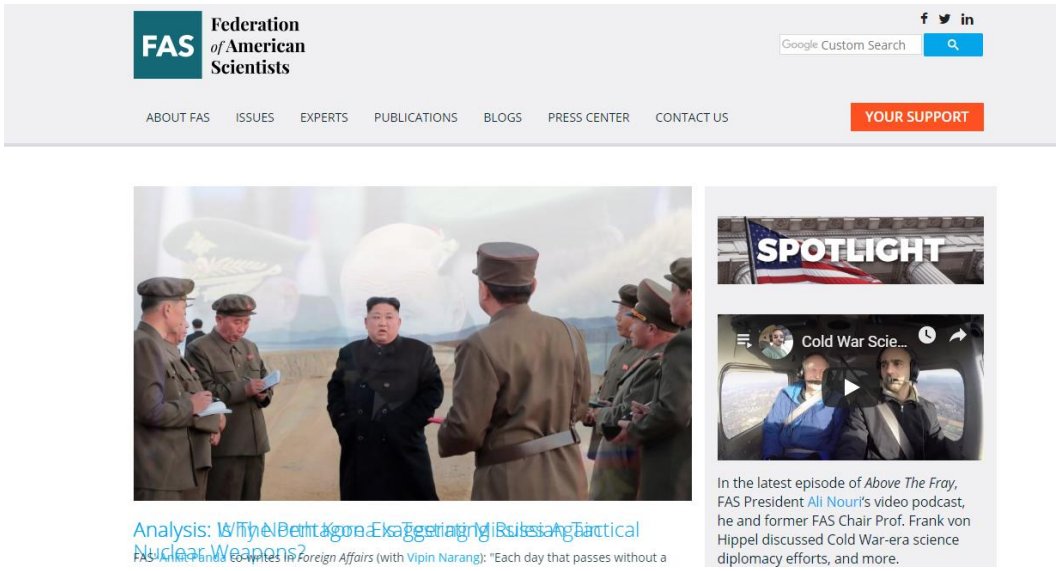


04.02

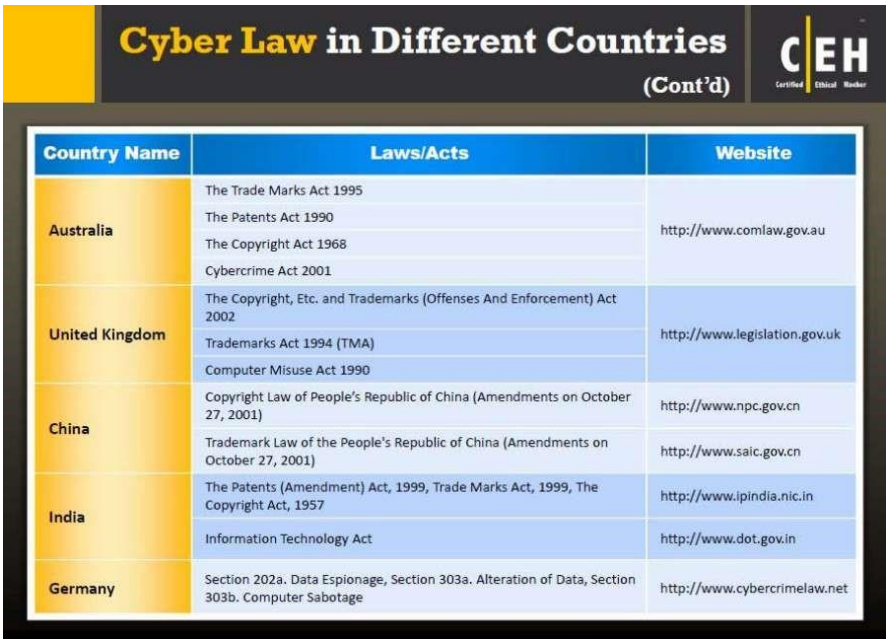


Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of " fair use"	http://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	http://www.uspto.gov
	The Electronic Communications Privacy Act	https://www.fas.org
	Foreign Intelligence Surveillance Act	https://www.fas.org
	Protect America Act of 2007	http://www.justice.gov
	Privacy Act of 1974	http://www.justice.gov
	National Information Infrastructure Protection Act of 1996	http://www.nrotc.navy.mil
	Computer Security Act of 1987	http://csrc.nist.gov
	Freedom of Information Act (FOIA)	http://www.foia.gov
	Computer Fraud and Abuse Act	http://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	http://www.ftc.gov

Example:www.fas.gov



04.03



Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	http://www.comlaw.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	http://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.saic.gov.cn
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	http://www.dot.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	http://www.cybercrimelaw.net

Example- www.npc.gov.cn

04.04

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	http://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	http://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	http://www.laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	http://www.statutes.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	http://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	http://home.heinonline.org
	Industrial Design Protection Act	http://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	http://www.wipo.int
	Computer Hacking	http://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	http://www.mosstingrett.no
Hong Kong	Article 139 of the Basic Law	http://www.basiclaw.gov.hk

Example : www.cybercrimelaw.net

==========

==========

==========