Career and Technical Education
Phase IV Learning-in-Place Plan
Cyber Security Fundamentals

HIGH SCHOOL

Learning-in-Place Period	Student Activity **Below are weekly items to be completed by students for review and introduction of new material. All activities will be expanded upon by the teacher during virtual sessions or other methods. Please contact your teacher or school directly for any needed assistance with accessing the sessions or content.**
May 18-21, 2020	**Types of Hackers: look up the definitions and provide a brief description for each.** • Black hat *White hat *Gray hat *Suicide *State-sponsored *Script kiddie *Cyber terrorist
May 22-27, 2020 (May 23-24: Weekend)	**Exploring important terminology: Look up the definitions and provide a brief description for each. Please ensure that the definition you pick is Cyber Security related.** • Threat *Asset *Vulnerability • Exploit *Risk *Zero-day *Hack value
May 28-29, 2020 (May 30-31: Weekend)	**Penetration testing approaches: The following are different approaches to performing a penetration test on a target organization: Briefly explain what each of these entails.** 1. White box 2. Black box 3. Gray box
	Types of penetration testing : Listed below are types of penetration testing. Give a brief explanation of each. • Web application *Mobile application • Social engineering *Network • Cloud penetration testing *Physical
June 1- 2, 2020	**Hacking phases During any penetration test training, you will encounter the five phases of hacking. These phases are as follows: Please give a brief explanation of each** • Reconnaissance *Scanning *Gaining access • Maintaining access *Covering tracks
June 3-5, 2020	**Complete Post-Test: See attached**

Cyber Security Post-Test

1. This is a class of programs that searches your hard drive and floppy disks for any known or potential viruses.
A. intrusion detection B. security identifier
C. Antigen D. antivirus software

2. What is the name for a program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document?
A. Spyware B. Virus C. Firewall D. Norton.

3. Which is a good choice in this situation? "If someone from your bank calls you and asks you to update your personal information including bank account number and social security number you will"
A. Give all the information as it is good for my bank to have my updated information.
B. Just give social security number, the bank should know your account number already.
C. Give bank account number and other details except social security number.
D. Offer to visit the nearest branch and update as required or call the bank with the number you know is authentic.

4. You receive an email from an unknown source asking you to download a patch that will make your computer more secure. You will
A. download the patch and not forward to anyone.
B. download, install & burn on a cd as backup for future use
C. download the patch and forward the email to all your friends to help them.
D. ignore, report as spam and delete the email.

5. Someone from a charity calls and asks you for a donation over the phone and you want to donate money. What will you do?
A. Give credit card or bank account information over the phone to donate money.
B. Request the caller to mail information to you by post so you can research about them before donating.
C. Ask them a postal address and mail them a check.

6. You have a Mac so you don't have to worry about viruses.
A. False B. True

7. Windows XP Professional with SP2 is COMPLETELY secure.
A. False B. True

8. The next time you order checks, you will do this for security reasons:
A. Your social security number printed near your name.
B. Have only your initials (instead of first name) and last name put on them.

9. How can you prevent intruders from accessing your wireless network?
A. Encrypt network traffic with WPA or WEP
B. Restrict access to trusted MAC addresses
C. Both

10. You receive an email that claims that if you forward the email to 15 of your friends you will get lucky otherwise you will have bad luck for the next few months. What will you do?
A. You will forward the email. B. Ignore and just delete the email.

11. What governs the type of traffic that is and is not allowed through a firewall?
A. rule base B. gateway C. access control list D. partition

12. What is the term for an attempt to determine the valid e-mail addresses associated with an e-mail server so that they can be added to a spam database?
A. X-mail harvest B. Directory harvest attack
C. Spambot attack D. Email validator

13. What protocol ensures privacy between communicating applications and their users on the Internet?
A. F-Secure B. Privacy Control Protocol
C. Secure Shell Authentication D. Transport Layer Security

14 . This standard being developed by IBM, Microsoft, Novell and others will allow different manufacturers' biometric software to interact. A. IDEA B. Twofish C. BioAPI

15. This two-level scheme for authenticating network users functions as part of the Web's Hypertext Transfer Protocol.
A. SSL B. CRAM C. LUHN formula

16. This standard being developed by IBM, Microsoft, Novell and others will allow different manufacturers' biometric software to interact. A. IDEA B. Twofish C. BioAPI

17. What is the term for an attempt to determine the valid e-mail addresses associated with an e-mail server so that they can be added to a spam database?
A. X-mail harvest B. Directory harvest attack
C. Spambot attack D. Email validator

18. What governs the type of traffic that is and is not allowed through a firewall?
A. rule base B. gateway C. access control list D. partition

19. This two-level scheme for authenticating network users functions as part of the Web's Hypertext Transfer Protocol.
A. SSL B. CRAM C. LUHN formula

Cyber Security Post-Test

20. What protocol ensures privacy between communicating applications and their users on the Internet?
A. F-Secure B. Privacy Control Protocol
C. Secure Shell Authentication D. Transport Layer Security

21. This is a common type of denial-of-service attack that involves sending more traffic to a network address than the temporary data storage area is intended to hold, thereby shutting down the service and possibly corrupting or overwriting valid data
A. war dialing B. buffer overflow
C. smurf attack D. bucket brigade

22. Microsoft's Passport is an example of this technology, which allows users to register their personal information once to access multiple applications.
A. Microsoft Point-to-Point Encryption. B. Single Signon
C. Relative Identifier. D. Biometric Verification

23.: Anti Virus programs protect your computer from spyware
A. True B. False

24 : This is a computer system on the Internet that is expressly set up to attract and "trap" intruders.

A. Exploit B. demilitarized zone
C. Trojan horse D. honeypot

25. Your friend sends you a website link requesting you to update your address information. What will you do?

A. Click on the link and update the information
B. Read the privacy policy on the website and decide if you want to provide the information or not.
C. Update and forward the link to all your friends.
D. Report your friends email address as spam.

26 : Which of the following methods does spyware use to install on an end user's machine?
A. Bundling with free peer-to-peer programs
B. Social engineering
C. Search toolbars
D. All of the above

27 : WEP is a security protocol, specified in 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. What does WEP stand for?
A. Wired Equivalent Privacy
B. Wireless Equivalent Protocol
C. Wireless Equivalent Privacy

28 . Firewall is a software or hardware that can protect a computer from virus. A. False B. True

29 : While you were browsing the web, you get a pop up window that says "Congratulations! You just won a TV, click here to claim". You ...
A. feel very happy, click on it & give all the information it asks
B. just close the window and ignore it

30 . Windows XP is secure by default. A. False B. True

31 : What do you call a program used to detect unsolicited and unwanted email and prevents those messages from getting to a user's inbox?
A. anti-spammer B. email guard C. virus filter D. spam filter

32 : You receive an email from an unknown source asking you to download a patch that will make your computer more secure. You will
A. download patch & forward the email to all your friends
B. download the patch and not forward to anyone.
C. ignore, report as spam and delete the email.
D. download, install & burn to a cd as backup for future use

33.: HTTPS is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. What does HTTPS stand for?
A. Hypertext Transfer Protocol Security
B. Hypertext Transfer Protocol over Secure Socket Layer
C. Hypertext Transfer Protocol over Sublayer

34.: What is SSL used for?
A. Encrypt data as it travels over a network
B. Encrypt passwords for storage in a database
C. Encrypt files located on a Web server
D. Encrypt digital certificates used to authenticate a Web site

35. In order to protect yourself from identity theft you should
A. Order and review your credit report from the credit reporting bureaus at least once a year.
B. Never give personal information over the phone such as social security number or financial information unless you initiated the phone call.
C. Review your credit card statements and bank statements for discrepancies.
D. All of the above.

36 : How does spyware differ from other forms of malware, such as worms and viruses?
A. The delivery mechanism is unaware that it contains spyware.
B. Spyware installs without the user's knowledge.
C. Not all spyware is malicious.
D. Spyware replicates itself.

37. Phishing and Pharming are forms of social engineering.
A. True B. False

Cyber Security Post-Test

38. Once you have logged on to your bank's website you can determine that SSL is being used on the site by looking for
A. A small padlock icon, usually in the lower right corner of your Web browser window. A closed, or locked padlock indicates a secure connection.
B. https:// -- in the address line of your browser.
C. Both

39. On average, how long does it take for an unprotected networked computer to be compromised once it is connected to the internet?
A. 1 Week B. 20 minutes C. 10 hours D. 7 Days

40. What type of attack relies on the trusting nature of employees and the art of deception?
A. Social Engineering B. Fraud
C. Phishing D. Dumpster Diving

41. You may give someone your password if:
A. It is never OK to give out your password
B. Your Boss asks you for your password
C. The helpdesk asks you for your password
D. Your Boss says it is OK to give someone your password

42. What can a firewall protect against?
A. Viruses
B. Unauthenticated interactive logins from the outside world
C. Fire
D. Connecting to and from the outside world

43. The National Security Alliance in 2004 estimated what percentage of home PCs are infected with spyware?
A. 20% B. 40% C. 60% D. 80%

44. In comparison to the illegal drug trade, Cyber crime generates:
A. Less Money
B. Mainly done by computer geeks for kicks instead of money
C. More Money

45. This is a document that states in writing how a company plans to protect the company's physical and IT assets.
A. Data Encryption Standard B. Security policy
C. Public key certificate D. Access control list

46. This is a program or file that is specifically developed for the purpose of doing harm:
A. Buffer overflow B. Bastion host
C. Malware D. Ping sweep

47. This is a program in which malicious or harmful code is contained inside apparently harmless programming or data.
A. War dialer B. Spam trap C. Trojan horse D. Email

48. What are the three most important things you can do to secure desktop PCs? a. Turn on Automatic Updates b. Turn on Windows Firewall c. Install anti-virus software d. Remove the hard drive
A. a, c, and d B. a, b, and c C. b, c, and d
D. a, b, and d E. only c

49. Which of the following is an example of a strong password?
A. Password B. J*p2le04>F
C. Your real name, user name, or company name

50. If you set your anti-virus software to auto-update then you don't need Windows Automatic Updates. A. True B. False

51. What is "phishing?“
A. "Spoofed" e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords
B. A type of computer virus
C. An example of a strong password
D. A boring activity that uses a rod and bait.
E. None of the above

52. You receive an e-mail message from someone you know well with Subject: line 'Here it is' and the file attachment is named draft.doc. What do you do?
A. Open the attachment
B. Save the attachment to disk and scan it for viruses
C. Contact the sender to determine if he/she created and sent the draft.doc attachment

53. You are using e-mail to send and receive private information (e.g. medical data, salary information, social security numbers, passwords). What do you do?
A. Put all of the information in one large message before sending it to reduce the chance that it will fall into the wrong hands
B. Encrypt the information before sending it through e-mail
C. Put the information in many small messages so that only a small information will be exposed if it falls into the wrong hands

54. You are receiving bothersome or threatening e-mail messages. What do you do?
A. Save messages and report the problem to your supervisor
B. Ignore the messages and delete them
C. Contact the police
D. Hire a hit man to rough them up

55. You learn about a new screen saver that you can download from the Internet to put on your PC at work. What do you do?
A. Don't download screen saver. This action is not allowed.
B. Download the screen saver and scan it for viruses before installing it.
C. Search internet for reports describing this screen saver.