**Contestant Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Time: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Rank: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**



**COMPUTER SECURITY**

(320)

**REGIONAL 2022**

**CONCEPT KNOWLEDGE:**

Multiple Choice (50 @ 2 points each) (100 points)

**TOTAL POINTS (100 points)**

**Test Time: 60 minutes**

**GENERAL GUIDELINES:**

*Failure to adhere to any of the following rules will result in disqualification:*

1. Member must hand in this test booklet and all printouts if any.
2. No equipment, supplies, or materials other than those specified for this event are allowed in the testing area. No previous BPA tests and/or sample tests (handwritten, photocopied, or keyed) are allowed in the testing area.
3. Electronic devices will be monitored according to ACT standards.

**MULTIPLE CHOICE**

Identify the letter of the choice that *best* completes the statement or answers the question.

1. What is the best way to recover a forgotten windows password?

1. Use Windows Live Web site.
2. Use a bootable USB
3. Reinstall Windows
4. Reset to factory Defaults

2. When is the meaning of Zero Day Vulnerability on Windows?

a. 1999/2000 bug

b. This vulnerability is unknown

c. The vulnerability is undefined

d. 2016 Side Channel vulnerability

3. How do most computers get infected in 2021?

a. Hidden attachment

b. Visiting web sites they should not be visiting

c. Not using a password

d. user accepts what they see on the screen without reading or understanding the prompt

4. Who is in charge of the nation's National Cyber Response team?

a. Dept. Of Homeland Security

b. Federal Bureau of Investigation (FBI)

c. Dept. f Defense/Intelligence community/NSA/Cyber Command

d. All are correct

5. What is the preferred SSL/TLS protocol for security on windows in 2021

a. SSL

b. TLS 1.2

c. TLS 1.425.2

d. TLS

6. Which SSL/TLS protocol was recently deprecated in most platforms, including windows?

a. SSL

b. TLS 1.0

c. TLS 1.2

d. TLS

7. What is Windows Hello?

a. A new Password App

b. An alternative to a password

c. A game secured with new Windows security

d. A handshake algorithm

/

8. How does windows Hello work with Azure in non-domain clients

a. Hello affords Multi-Factor Authentication

b. Multi-Factor Authentication does not need Azure

c. Azure is incompatible unless domain joined

d. Hello waves to azure and they unlock your computer.

9. AES Vs. DES Encryption cyphers - which is the current standard?

a. Alternative encryption standard (2020)

b. Delta Evading Signals (1968)

c. Advanced Encryption Standard (1999)

d. Data Encryption Standard (1976)

10. Perfect Forward Secrecy (PFS) is on the rise for security. What is PFS?

a. Makes sure users can't find the session passwords

b. Hides the registry from hackers

c. Forces the sessions to re-negotiate (ephemeral) session keys frequently

d. A policy not to share your passwords with friends going forward.

11. What Certificate signing request key length is best?

a. 128

b. 256

c. 1024

d. 2048

12. What is a windows/Azure Security Principal?

a. A User, Computer or Service

b. The Token given to a Logged in user

c. The SPN of a computer

d. A users GUID

13. What is the difference between secpol.msc and gpedit.msc?

a. They are the same thing.

b. secpol is a subset of gpedit.

c. gpedit is a subset of secpol.

d. They are not related.

14. You can enable usb write protection, for usb drives, by going to the registry and adding a DWORD called StorageDevicePolicies in Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\

and then adding a WriteProtect key with a value of 1?

a. 1

b. 0

c. 3

d. 4

15. How does execution policy make a windows machine more secure?

a. It prevents scripts from running on a machine when restricted

b. It's not really a security command

c. It's an old policy that doesn’t work any longer

d. It’s a DOS security feature

16. Why are some files marked as block/unblock?

a. They are marked by the internet as possible security issues

b. It’s a function of the NTFS file system

c. It’s not Dependent on the disk subsystem

d. It’s a feature of Defender

17. What new Security Item is part of Windows after version 1703?

a. Windows Defender

b. Windows Defender Security Center

c. Windows Firewall

d. Windows PowerShell security Snap in.

18. How can you track down a virus running from the browser and potentially stop it?

a. Task Manager, Processes, Open containing folder, Search registry, Stop service, Delete files and registry

b. Format the drive and clean install

c. cmd, netsh winsock reset, devmgmt.msc and delete any bangs

d. Boot outside the OS and hit F8 to boot to Service Restore mode

19. What change has Microsoft made to the DisableAntiSpyware Policy setting, since the advent of viruses like TrickBot, Novter, Clop Ransomware, Ragnarok Ransomware, and AVCrypt Ransomware?

a. Microsoft set this policy mandatory

b. Microsoft changed the key name.

c. Microsoft removed this key from use, because these viruses were targeting this setting

d. Microsoft disabled this feature entirely

20. What is mimikatz used for?

a. It is a common hack tool for saving cached passwords and hashes

b. It is an internet download for Azure

c. It is an Exploit used with viruses

d. It can be used to test hardening of your environment

21. One kind of key is used for 1x1 encryption and the other is used for 1 to many encryption. Name both of those methods:

a. public/Private

b. SSL/TLS

c. symmetric/Asymptotic

d. Symmetric/Asymmetric

22. Application layer Gateways are used to make companies more secure. Can you name what may be making deep packet inspection obsolete? feature of application layer gateway?

a. The Internet

b. Ports and Protocols

c. Secure Encrypted connections

d. The new Microsoft feature enabled at HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\ALG2.0

23. Microsoft has a more secure mode called S mode. What differentiates S mode from regular windows?

a. S mode will not allow installed apps to run

b. S mode applications have special certificate in programs and features

c. S mode only allows app store apps

d. S mode is made up. There is no such mode.

24. Role Based access control (RBAC) is applied by a domain you associate with. Pick out the Authenticating agent and the authorizing agent in order.

a. AD/RBAC

b. RBAC/AD

c. AD/ADFS

d. ADFS/RBAC

25. What user has admin rights to the schema admin group in AD security in a default install and what is the roll called?

a. Schema user and Administrator Group

b. Administrator and Administrator Group

c. No user and Schema Group

d. Administrator and Schema Group

26. List the Elements of RBAC.

a. Security principal, Role assignment (Role Definition, Scope)

b. Security User, Role Definition (Target and scope)

c. Security Object, (Role and scope)

d. Security Definition, Target role (User and scope)

27. Is Internet Explorer 11 still supported on Windows 10?

a. Yes but it ends June 15th 2022.

b. No, Chrome has replaced it

c. No, Microsoft uses Edge now.

d. Yes, it will support IE11 into the future.

28. What is this called in the windows nomenclature [\\localhost\c$](file:///C:\c$) ?

a. Administrative share

b. The Back-Door Share

c. The Hackers way

d. The windows Share

29. You get people in your office saying they are not getting emails from your self-hosted mail server. MX toolbox says his mx record is correct and the mail server is sending mail. What is the most likely issue?

a. Mail is piling up on their desk.

b. Something is really broke

c. They are on a blacklist

d. They have not paid their bills.

30. What is a blacklist?

a. Government lock down

b. Third party companies like spamCop or MultiRBL or ISP like Comcast.

c. A group of ICANN resources who police the internet

d. Dept. of the ASPCA

31. Name the top Network Threat in the list below.

a. Email

b. IOT Internet of things (My smart Fridge).

c. Television

d. The human mind

32. What two things can protect against modern threats like side channel vulnerabilities?

a. Better organizations

b. IT deployments

c. Patching, Drivers and Firmware

d. User Being more careful

33. What is the signs you have been involved in a ransomware attack on your Hyper-V cluster?

a. The Server won't start

b. A telephone call from a person with a voice generator

c. Your VMS won't start and there is a text file in your folder where your virtual machines go.

d. The Server Starts but a message pops up saying you're not getting your data back.

34. Name the item below which is not a side channel vulnerability in windows:

a. Spectre

b. Meltdown

c. Mimikatz

d. Foreshadow

35. When someone uses a fake web site, and you purchase something from that site, and your money goes into an offshore account in china, you never get your hardware. What is this an example of?

a. Phishing

b. Hacking

c. Your Dumb

d. Virus

36. What is TCP port 53 used for?

a. Videos

b. Apple

c. DNS

d. DHCP

37. You're Not able to reach the share on the domain from your window 10 computer. What is the problem?

a. Weak Host Model of window network is enabled

b. Network and sharing "pubic folder sharing" is disabled

c. DNS is incorrect on the Domain controller

d. All are correct

38. Which three ways is it possible to take ownership of SQL Database queries?

a. Add Sysadmin Role to user

b. Add DbOwner permission to database

c. Add a SQL server Login Password and login with user and password

d. All/any of the above

39. Why is an arp request going to a hub, a bad security choice?

a. Arp requests are only 1/2 duplex.

b. Arp requests go to all other devices on the network

c. Arp requests are much slower on a hub

d. A hub is not IEEE approved.

40. Why is an arp request to a hub susceptible to a hack?

* 1. Broadcasts go to all devices, increasing the attack surface to the whole network as a single broadcast domain

1. Tools can be used to reply to the arp and poison the arp cache
2. Man in the middle attacks or denial of service attacks are possible
3. All are correct

41. What are the 3 ways to authenticate someone?

a. Something you know, something you have, something you are.

b. Something you are, something you want, something you need.

c. Something you wear, something you think, something you eat.

d. Something you hide, something you keep, something you share.

42. What is the difference between data protection at rest vs. data protection in transit?

1. There is little difference. What is important is how valuable the data is. If data is valuable, it needs to be protected in either state.
2. Data at rest can use reactive security. Data in transit is where the spend is most important
3. Data at rest can is most important. Data in transit can get away with a firewall and router.
4. None of these are important. What is important is physical security. Keep the doors and desktops locked.

43. Choose two items which match the description of the three-way handshake.

a. Kepler’s algorithm

b. Client TCP(Syn 500)->ServerTcp (SYN501) (Ack 7000))-> Client Tcp (Ack 7001)

c. A requests B, B Replies A, A sends both to C

d. Client UDP(ACK 500)->Server UDP (SYN500) (Ack 7000))-> Client UDP (Ack 7000)

44. What type of attack intercepts communication between parties to steal or manipulate the data?

a. replay

b. MAC spoofing

c. man-in-the middle

d. ARP poisoning

45. You install a third-party anti-virus. You find two antivirus applications are actually running now. Which is true?

a. Two AV are double the protection

b. Two AV are mitigated by windows Defender

c. Windows Defender takes precedent over the other

d. There are likely incompatibilities which will require resolution.

46. What is an Antivirus signature definition update?

a. The signatures are patterning the Av looks for to identify an intrusion vector

b. A vector the Av can use to inoculate a system to be impervious to a virus

c. A regular update to an antivirus application

d. A bunch of text files with templates in them

47. Does Windows come with an antivirus application?

a. No. It's just a spyware app

b. Yes. Windows Defender Security Center

c. No. Defender is not classified as an actual antivirus

d. Yes. It has 2 Security center and Defender

48. Wired Equivalent Privacy (WEP) has been insecure for years. But today Windows will tell you your insecure if you use WiFi Protected Access (WPA2), in some circumstance. What would make WPA2 Acceptable to Microsoft?

1. By another router that includes VPN
2. WPA2 is also infective and insecure
3. Advanced Encryption Standard (AES) is generally considered to have no weaknesses. It is recommended with WPA2.
4. Use Temporal Key Integrity Protocol (TKIP). It used the RC4 cipher and is most secure for Windows.

49. What two truly really illustrate the condition of security for Wi-Fi.

1. Experts agree but WPA2-(AES) is not the choice. Many Argue WPA3 should be recommended but not enough data exists for analysts to say.
2. Experts Agree WPA2-(AES) is what most use, but WPA2-TKIP is what they should be using. WPA3 is not released yet.
3. Experts Disagree. This is why there is no real standards today.
4. Experts Disagree. To the point that there is a flaw in this discussion. AES is not even an Encryption protocol. When you say AES, you really mean (CCMP) Cipher Block Chaining Message Authentication Code

50. As a hardware security specialist, you charge by the hour for consulting. Your customer has asked for a way to make sure the songs he/she writes cannot be stolen if he/she loses their laptop. Their laptop does not have a TPM module inside. How would you fulfill the need?

1. Shared Secret
2. Network Security
3. Third Party
4. Bit locker