**Course Name: Securing your network from Attacks**

*NOTE: Mark the correct answers with Yellow highlight*

**Chapter Number 4**

1. When it comes to patching…

a. You should develop a patch cycle to ensure everything stays up to date.

Reason – Correct, flaws and exploits are found on a regular basis and it is critical to make sure our systems are up to date.

b. It should be avoided as much as possible, patches can break things.

Reason – Incorrect, while there are occasional patches that have caused issues, they do get fixed quickly. It is still critical to keep systems up to date, even if you decide to wait a day to 2 to vet the patch before applying.

c. Only your OS (Windows, Linux, OSX) needs to be patched.

Reason – Incorrect, switches, routers, application software, etc. also need patches.

d. Should only be applied if it’s a critical flaw.

Reason – Incorrect, while a critical flaw will generally expedite it’s place in a patch cycle other updates should be applied as they do help with overall stability and or functionality.

2. Anti-virus software….

a. Is an out dated idea.

Reason – Incorrect, Anti-viruses still have a solid place in network security as they are able to identify and stop many viruses, malware and crypto ware.

b. Is not necessary if you maintain your patches and limit your user rights.

Reason – Incorrect, while I have heard this argument repeatedly, I still find that even the most carefully configured network just needs a single flaw to be exploited or one careless action from a user. A anti-virus is just another layer of protection.

c. Is still a worthwhile protection that should be implemented

Reason – Correct, Anti-viruses still have a solid place in network security as they are able to identify and stop many viruses, malware and crypto ware.

d. Cause more issues for the users than it is worth and should not be used.

Reason – Incorrect, while a misconfigured anti-virus can cause problems you should spend some time to adjust it accordingly.

3. Limiting users rights…

a. While is rarely an easy process to limit, is necessary for security.

Reason – Correct, limiting user rights tend to cause angry users and can be difficult to determine how much rights there needs to be, however this will reduce insider attacks and other attacks.

b. Is not a best practice as this will hamper the user’s ability to work.

Reason – Incorrect, limiting user rights tend to cause angry users and can be difficult to determine how much rights there needs to be, however this will reduce insider attacks and other attacks.

c. Only needs to be applied to high value users who may be targeted for an attack.

Reason – Incorrect, every user should be protected and limited to what they need in order to do their work (or as close as possible).

d. Is entirely determined by IT and user input is not necessary.

Reason – Incorrect, proper information gathering on what your end users need/want, and proper communication as to why the user rights are what they are to be set at is important for a healthy and productive work environment.

4. Scareware…

a. A old outdated attack method.

Reason Incorrect, sadly scareware in one form or another is quite alive and well.

b. Generally relies on scaring the user into taking an immediate action that is not in their best interest.

Reason – Correct, scareware generally will utilize fear, authority, scarcity or combination to force a user to take immediate action.

c. Encrypts your files and forces you to pay a ransom.

Reason – Incorrect, that would be ransomware.

d. Will do damage in one way or another if you do not take action.

Reason – Incorrect, most scareware is just that, designed to scare you into taking action. Most often there is no negative impact from not reacting.

5. A VPN….

a. Is only used by criminals to hide their activities.

Reason – Incorrect, journalists, activists, security professionals, businesses, government, and home users tend to use VPNs for privacy and security.

b. Is a efficient way to make your internet connection private by encrypting your traffic and masking your true IP address, location, and ISP.

Reason – Correct, a good VPN will do just that, also making it harder for attackers to spy on you, or launch a MiTM attack and steal your credentials.

c. Have little to do with security.

Reason – Incorrect, VPNs are a very important part of security protecting our identity, encrypting our traffic and more.

d. Only works on a Windows computer

Reason – Incorrect, VPNs exist for Windows, Linux, OSX, iPhone, Android, etc.