CYSE 280 – Windows Systems Management and Security

Professor Malik A. Gladden

Homework 3

1. What are the main characteristics of a network operating system?

The main characteristics of a network operating system are things such as printers, PCs, and workstations. This list includes many other things like network security and file sharing.

2. Compare DHCP with APIPA. What are the benefits of having both of these protocols available within a network?

First, we need to understand what the acronyms mean. DHCP stands for Dynamic Host Configuration Protocol sometimes this refers to the Boot Protocol server. This allows its user to configure IP on a network interface. Then APIPA is the automatic private IP addressing, this is for automatic address assignment. Having both of these can be beneficial to use when configuring a network. This can save a lot of time and resources when operating with both.

3. What are the main differences between a PowerShell variable and a constant?

The main difference between the two is that PowerShell variables are a list of things commands that still output the result. Constants will only have one command to the output. PowerShell variables are more commonly used because some commands are used across different platforms/command prompts.

4. Compare the System File Checker tool to the File Signature Verification tool (Sigverif). What are the benefits of having both of these tools available within PowerShell?

The system file checker typically scans system files for integrity. Then replace damaged or overwritten files with updated versions. The file signature verification tool is a scan-only tool to see if it's the proper version and that it has not been altered. When combining these two tools it can verify system files extensively.

5. The Shadow Brokers are believed to be affiliated with which country, and what do we know about their origins and allegiances?

Possibly Russia? Their origins were unclear but it was noted that English was a second language, which doesn't narrow down too much. It was believed to be Russia because anytime Russian hackers were brought up in the media, they would come out of hiding. Another believed person that could be behind the group is a person named Harold. This is because of a past event that could be a potential staging ground for an attack like this.

6. The Shadow Brokers declared their allegiance to which President of the United States, and what implications did this decision have?

Their allegiance was found out in a pro-Trump tweet that showed their support. The implication of this, made people think the president might have some connection to Russian hackers or something of that sort.

7. Once the Shadow Brokers group stole NSA hacking tools, what did they attempt to do with stolen tools, and should we have questions about the security of government networks and the safety of confidential data?

The shadow brokers group released one tool to the public for free and then auctioned the rest. This did not amount to what they were expecting, so they stated they would release all of them to the public for one million bitcoins. Again, this did not amount to anything so they went away for a while and then listed IPS addresses that were supposedly associated with the NSA. Throughout my time learning about cyber security, I have been told that not everything can be secure. I do not question the security of government networks and confidential data because they are far better than what is known or released. These attacks provide a new way to protect and defend against groups like this. It's a complicated system where it will be safer after these types of attacks.