**DV155\_Mansoor\_14\_PAS On Network Services**

**Self-Assessment Sheet**

1. What is a Web Server?

*Many organizations will have one or many different web servers, and those servers are responsible for responding to browser requests that you would make from your computer.*

2. What is a File Server?

*This is a centralized storage device usually with a set of folders that you can use to store all of your information.*

3. What is Print Server?

*This is usually hardware or software that allows us to connect this printer to the network so that everyone can access that centralized resource. This print server may be software that’s running on a computer that has a printer connected to it and everyone on the network would send their print jobs to this computer so that the print server can then access those jobs and print them on the printer.*

4. What is a (Domain Name System) DNS Server?

*Almost every organization and every data center has inside of it a DNS server. DNS stands for Domain Name System and it’s a service that’s primarily responsible for converting between fully qualified domain names and IP addresses. So if you go into a browser and type www.professormesser.com. That browser will ask the DNS server what’s the IP address of www.professormesser.com? That IP address will be provided to the browser. And from that point forward, the browser uses the IP address of my web server to communicate back and forth to your browser.*

5. What is a (Dynamic Host Configuration Protocol) DHCP Server?

Another common service that you’ll find in a data center is a DHCP server. This stands for Dynamic Host Configuration Protocol, and this is the service that automatically assigns and configures IP address settings on your local device. This is a service that we’ve become very accustomed to having. We can plug in or connect to anyone’s network, and we’re automatically provided IP addresses, DNS settings, and everything else. We need to be able to communicate on that network.

6. What is a Mail Server?

*Another important service that often requires 100% uptime and availability is a mail server. This is the server responsible for sending and receiving mail for your organization. Because the service is so critical, it’s often managed by our local IT team or we may be using an ISP or cloud based service to provide these mail services.*

7. What is a Proxy Server?

*Some organizations have installed proxy servers to add additional security to their internet communications. As the name implies, a proxy sits in the middle of a conversation. Users will make a request to the proxy. The proxy then makes the request to the third party service, receives a response from that service, and then examines the response to make sure nothing within that response is malicious. Once everything is checked and everything looks OK, that response is then sent to the end user. This means that we can put a lot of security controls into the proxy. The proxy can act as access control, so it may require a username and password to gain access to the internet. It can perform caching. It can filter by URL and many other security capabilities as well.*

8. What is an Authentication Server?

*In an enterprise, we might often start our day by logging in to our local computer or we may be connecting from a VPN and we would use a username and password to provide that authentication. And often the authentication that we would use between all of these different services is identical. So how does the enterprise use the same authentication method across all of these different servers? In most cases, the organization’s using an authentication server which centralizes all of those usernames and passwords to a single service.*

9. What is SIEM (Security Information and Event Management)?

*One of the protocols that allows us to consolidate these log files is called syslog. This is a very common standard. And if your system collects logs, then it probably has the option to send those logs to a centralized database using syslog. In many organizations, we use a Security Information and Event Manager to collect all of these log files. We usually refer to this as a SIEM. As you can imagine log files take a lot of room, so the SIEM usually has a very large drive array and we’re able to store a large number of files over very extended period of time.*

10. What is Forensic Analysis?

*Forensic analysis in IT refers to the investigation of events that have occurred in order to find the root cause.*

11. What is Syslog?

*One of the protocols that allows us to consolidate these log files is called syslog. This is a very common standard. And if your system collects logs, then it probably has the option to send those logs to a centralized database using syslog. In many organizations, we use a Security Information and Event Manager to collect all of these log files. We usually refer to this as a SIEM.*

12. What is IDS (Intrusion Detection System)?

*You might also have other networking features such as CSU DSU capabilities which allow you to connect to a wide area network. These devices often act as routers and they usually might also have switch interfaces on the back of these devices. And of course, they act also as a firewall so you can allow or disallow certain traffic flows through your network. These devices can often act as intrusion detection systems or intrusion prevention systems, which can block known attacks from traversing the network. These devices can also act as bandwidth shapers or quality of service devices so that different applications can be prioritized in real time. And if you need people to connect to the network that are outside of your facility, you might want to use an encrypted tunnel through a virtual private network.*

13. What is IPS(Intrusion Prevention System)?

*You might also have other networking features such as CSU DSU capabilities which allow you to connect to a wide area network. These devices often act as routers and they usually might also have switch interfaces on the back of these devices. And of course, they act also as a firewall so you can allow or disallow certain traffic flows through your network. These devices can often act as intrusion detection systems or intrusion prevention systems, which can block known attacks from traversing the network. These devices can also act as bandwidth shapers or quality of service devices so that different applications can be prioritized in real time. And if you need people to connect to the network that are outside of your facility, you might want to use an encrypted tunnel through a virtual private network.*

14. What is All-in-one security appliance?

*Many security vendors offer “all-in-one security appliances,” which are devices that combine multiple functions into the same hardware appliance. Most commonly these functions are firewall, IDS/IPS, and antivirus, although all-in-one appliances can include VPN capabilities, anti-spam, malicious web traffic filtering, antispyware, content filtering, traffic shaping, and so on. All-in-one appliances are often sold as being cheaper, easier to manage, and more efficient than having separate solutions that accomplish each of the functions the all-in-one appliance is capable of performing.*

15. What is Endpoint Management Server?

*Endpoint management is the control of networked PCs and other devices to maintain functionality and security. In most organizations, each employee uses at least one endpoint device, and information technology (IT) teams devote considerable time and energy to managing those devices.*

*As remote and hybrid work models become more widespread, endpoint management has grown increasingly complex.*

*Internal IT teams and managed service providers (MSPs) are responsible for updating and patching software, preventing unauthorized access, and enforcing regulations and policies for devices and users in remote locations as well as on-premises.*

*Security is often the primary focus of endpoint management policies and processes, but user experience is another key concern. IT is asked to keep employees productive and happy, and endpoint device performance can contribute to user satisfaction. If performance is hampered by compute-intensive encryption, inadequate network capacity, repeated reboots, or other security-related issues, users may be tempted to bypass security protocols, creating unwanted vulnerabilities.*

*In recent years, new tools and methods have emerged to support endpoint management. The Intel vPro® platform can play an important role in improving the manageability and security of an organization’s networked devices. With Intel® Hardware Shield for built-in hardware-enabled security features and with built-in accelerators, the Intel vPro® platform can support the performance that users expect and need to maintain productivity.*

*Additionally, Intel® Threat Detection Technology (Intel® TDT), a feature of Intel® Hardware Shield that provides cyberattack monitoring and increased security performance, is enabled in leading security vendors’ software to improve security efficacy and performance while minimizing impact to user experience.*

16. What is a Legacy System?

*One common theme with data centers is once a service is installed, it’s very difficult to get that service removed from the data center. And often devices and services may sit in the data center for 10 years or even more. We often refer to these systems as legacy systems. And although they’re very old, they usually have an extremely important service that’s running on them. Very often these legacy systems are running on older software or older hardware, and it might be very difficult to resolve a problem with this device just because the software and hardware are not well supported or may be difficult to obtain.*

17. What is an Embedded System?

*Another type of service you might find in your data center is an embedded system. These are systems where you normally don’t have access to the operating system or any other aspect inside of the device. Instead it is a purpose built device that’s designed for you to only have access to the service or the application that that device provides. This might be something like an alarm system or a door security system or perhaps the time card system that you use to keep track of when people come to work and when they leave. Those devices commonly don’t have an operating system that we can update or even view. Because of that, we rely on the manufacturer of these purpose built systems to be able to provide us with support and ongoing maintenance.*