The default Windows firewall and security settings might contribute to the inability to detect an attacker probing from inside your network because firewalls can cause the loss of visibility and control over applications, users, and content. Before it was easy for firewalls to control traffic because applications were tightly tied to ports and protocols. Now, applications are no longer tied to specific ports or protocols they are being used to build to use any open port or they use SSL. This means to always make them accessible to users, despite possible issues. The security settings contributions to the inability to detect an attacker probing from inside your network is change what you are looking and for and how. The issue needs to be resolved. Security settings are setup for pre-defined signatures, hashes, software behaviors and URLS. Attackers must be detected by operational activities. Network detection must look at full network activity. This will allow the company to who is doing what to whom. You must determine a normal network activity from something that is both anomalous and malicious. Separating between anomalous and malicious is another issue in detecting an active network attacker called noise. Today security system is set up to alert on every sign and signal of technical artifact, systems produce many alerts that are dominated by false positives. The network needs constant monitoring to detect anomalous.

* This was just a single system on a local LAN. How much more complicated would this process be for 100 computers? What about an enterprise with 10,000 computers on their LAN/WAN? In terms of Virus and Trojans can be detected in time before attacks have occurred. This can lead to a lot of information lost or destroyed. The more computers the longer it would take for attack to detected. System updates might not run correctly if each computer does not have updates on them.
* Consider a cloud-hosted Infrastructure as a Service (IaaS) environment with many new, internet-accessible systems regularly being built and brought online. What advantages or challenges might there be protecting such systems from malware and from attack? Some challenges are misconfiguration. When setting up a new cloud server, IT staffers sometime don’t properly configure their authentication leaving sensitive information vulnerable to unauthorized access. Changes in visibility is a compounder for other risks. IT team will have as much visibility into this kind of environment as an on-premises one that is controlled by an organization. Blocking data exfiltration because a user does not have full control of this environment it will be hard to block exfiltration to someone that has legitimate credentials or who is using legitimate credentials illicitly. Cloud email isn’t always secure. Clouds have many vulnerabilities as other email products. The major vulnerability is human error. These email platforms offer less protection than secure email gateway products. These do not translate to the cloud. Emails that should to go the inbox will be reported to the cloud email provider as a phishing email.
* Finally, conclude this week's assignment with a page explaining how the same types of tools demonstrated in this lab might be used by an infrastructure administrator to help secure an environment. The types of tools demonstrated in this lab that might be used by infrastructure administrator to help secure an environment. There are three components is compromise of the virtual environment, the management of applications and operations in the virtual machines, and the use of a virtual administrative network to manage virtual hosts. A virtual environment is more than just the virtualization host. The virtual environment components include management tools, backup tools, storage, and both virtual and physical networking. Management of the guest OS does not require access to VM management tools; namely access to the remote console. It often does require access to a console, but that can be granted using tools like the Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), or a Secure Shell (SSH). The main reason for limiting access to the virtual infrastructure client is that, currently, the roles and permission protections within the client are not granular enough to limit actions sufficiently. They also are often confusing to set up as they are the reverse of all the other types of permissions in most OSes. Using a virtualization administrative network is extremely tricky as access to any of the management tools could lead to deeper access whether by using the virtual infrastructure client, VI SDK, or other tools. The other part of using a virtualization administrative network is placing the appropriate systems within this network. Each virtualization administrative network should contain the VMware ESX or VMware ESXi hosts service console or management appliance, the VMware vCenter server and the VMware Infrastructure Management Appliance. Even though a Secure Sockets Layer (SSL) is used for all communication, this network should be firewalled from the other networks in the environment.