MS Exploit (Office, Windows, etc): code that takes advantage of vulnerabilities in the MS office code

Network Reconnaissance: the information gathering stage of hacking where you collect data about the target system

Powershell: execute code from a command line

Sandbox: a virtual machine environment

EDR: endpoint detection and response, cybersecurity protocol that continually monitors end point devices for threats

Process Hollowing: Hacker removes code in a file and replaces it with a malicious code. Makes user have to execute malicious code

C2 Server: command and control server, typically a separate server apart from hacker’s PC

Dumping Credentials: stealing credentials from a victim PC or a database and storing them for use or posting them online

SMB Connection: a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network

DLL: dynamic link library, a collection of smaller programs that larger programs can use for specific tasks

Privilege Escalation: a cyberattack designed to gain unauthorized privileged access into a system

Infiltrate & Exfiltrate: the attacker getting into a system and downloading/moving data into their own local computer

1. List two biggest takeaways from this video.

One thing I can take away is that your files and personal data can be compromised just through clicking a malicious link in an email. Another thing I can take away is how intricate the hacking process is and that the majority of the population does not know when or how they are being hacked and it is usually too late to reverse it when they find out.

2. Describe the importance of visibility in a situation like this.

Being able to catch the attacker before they got more privileges in the system would have prevented the data breach

3. If you were tasked to conduct an assessment report of the attack, where would you start?

I would start with the initial intrusion and find out what exploit the attacker used to gain access and train employees more on avoiding phishing emails. I then would look at what data was stolen and from where.