Kojo Acquah - A00384405 - Assignment 4

1.
    a. Whaling : A kind of phishing attack that target high-profile employees of firms and companies to gain access to sensitive information

    b. Malware: Any software that's intended to harm a system and/or its user

    c. Host based IDS : THese are detection systems run on individual hosts or devices or nodes in the network. The most basic implementation is they work by taking screenshots of the system including critical files and alert the admin to any changes that occur when the images are compared with the screenshots

    d. Network based IDS : These run on the network itself and monitor the traffic within an entire subnet. If the traffic has a match in a library of known attacks (based on signature), the system will report this to the admin.

    e. IPS: Similar to IDS, IPS go a step further to attempt to block or hinder any suspicious activity on a network/system.

    f. Virus : Computer programs that spreads and runs on a system without the user's knowledge. Their goal is usually to deceive the user into executing them and also spread them to other users' systems

    g. Trojan : Like the name implies, it's a program /piece of code that seems harmless but is actually intended to do some form of harm to the system. It could be opening a backdoor to the system, copying confidential files or even permitting remote access to the system for it's creator

    h. Tor: A software program focused on protecting user privacy on networks by hiding packet information such as the source and destination using a technique called onion routing where it encrypts and bounces packets off relays across the web

2. One way would be to modify the firmware or completely replace it with another driver so that the computer is fooled into believing it's another device, for instance a keyboard. In the modified firmware, add code to download malware/virus online or copy the virus from the drive itself using pre-programmed keystrokes that are actually shell commands. The computer should accept them since it believes the usb is actually a keyboard.
   To propagate, the virus itself would be a program that is setup to reprogram any and all flash drives that are connected to the computer witht the same

malicious firmware.

Two methods have been suggested, one more proactive than the other:

a. Have a hardware lock on the usb device to prevent tampering with the firmware after it leaves the factory.

b. Another method is to disable autoplay for all removable drives to prevent the program running on its own. Then install an antivirus program on the flash itself teh protects it from being reprogrammed when inserted into a computer.

3. Code Red worm from 2001 infected Windows 2000 and Windows NT systems by exploiting a buffer overflow vulnerability in the IIS Web Server. It would spread to other systems by overflowing the buffer with a series of “N” and then adding a payload to the end. The payload was intended to deface the website.

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNN
%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3
%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a  HTTP/1.0
```

The way to stop the infection was finally discovered by Kenneth D. Eichman and a patch was released by Microsoft to patch the vulnerability.

4. Solution files included in zip

https://payatu.com/understanding-stack-based-buffer-overflow/

https://www.youtube.com/watch?v=1S0aBV-Waeo

References

https://www.pcworld.com/article/2460540/most-usb-thumb-drives-can-be-reprogrammed-to-silently-infect-computers.html