Mentor Project - Questions & Answers

Report on the weaknesses on the following protocols and how they can be secured to prevent data leakage.

HTTP

- Is an application protocol that sends hypermedia documents.
- Unencrypted data that can be interfered by 3rd parties to be gathered from 2 system.
- We can use HTTPS protocol to protect the integrity of the users computer and the site.

DNS

- DNS servers will share information such as server names and IP Addresses to anyone that requests it internally. The most effective ways to harden DNS servers would be to disable zone transfers, Use firewalls to control access and enable DDNS for secure connections.
- DNS cache poisoning or (Man-in-the-middle) would be another common attack where an attacker will enter false information into the DNS cache which would trick the DNS server to be directed to the wrong websites. The best way to prevent this kind of an attack would be to implement DNSSEC.

EMAIL

- Email has many protocols such as Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP3), and Internet Message Access Protocol (IMAP).
- SMTP main weakness is that users are not verified when their is a connection established. Implementing SSL/TLS would provide an extra layer of security as it encrypts the messages exchanged between email client and email server.
- POP3 Sends information using clear text which is a security issue.
- IMAP has a lack of support for user authentication along with sending information in plaintext, Reconfiguring clients and servers to use port 993 will help harden IMAP security.

FTP

- FTP is a communication protocol that transfers files from a server to a clients Computer.
- It is a protocol that isn’t using encryption which makes it accessible to hacker attacks.
- We can use SFTP to secure our files as the SFTP uses encryption and secures the Integrity of the files and information.
- SSH is a form of cryptography that is used in a process of transferring data in a secure way, it also communicates with both computers safely.

Explain how DHCP works and how a system administrator can prevent 'rogue severs' and 'man in the middle attacks'.
DHCP is a network management protocol. It automates IP addresses to there assigned hosts either connected wirelessly or wired. An example of DHCP is when a device tries to gain access to a network that is using DHCP, The DHCP server sends the IP address to the device.

System administrators can use a feature called "DHCP Snooping". It is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. DHCP snooping builds and maintains it's binding database as well as containing information from untrusted IP addresses.

With 'IOT' becoming more prevalent, what are the security and ethical issues when using this technology?
With Internet of things devices becoming more prevalent the rise of bigger botnets has become more prevalent as well. Botnets contain malware which enables attackers to access a IOT device and attack an organizations network. This kind of IOT attack is more prominent in appliances such as smart fridges or even smart doorbells.

Attacks can also have ethical issues as IOT devices become more prevalent such as misuse of personal information and lack of oversight and acceptance of responsibility.

Discuss the use of "ransomware" in recent attack and how they can be prevented.
Ransomware is a malicious cyberattack that encrypts your file/s which prevents the user from accessing it, only the attackers have a decryption key which can access the encrypted files.

A recent cyber attack was against the Irish Health Service (HSE). This attack was believed to have happened with a spoof email send to a high up person in the HSE which contained a Microsoft Excel File, Once this file was executed the HSE servers were infected, 2 months later the ransomware attack was executed. This is known as a zero day attack.

We cannot completely stop the ransomware attacks but we can take necessary percussions to decrease the damage of the attack.
Backup files,Anti-ransom software,User training on suspicious activity,Updates to software, these are just some examples on how to prevent a ransomware attacks.