The hacking skill and technology keeps updating and advancing, so our network protection strategy should always be updated.

Although traditional firewalls and anti-virus software are still important to defend our systems and networks, but there are more advanced hacking techniques, and we need to defend. One of the latest threats is the DNS injection. Hackers able to change the DNS record of the server, by using port 53. Hackers can redirect the Alias or A records to their target server, and the users who are redirected by these vulnerable DNS servers may suffered different level of data loss, or their client maybe controlled by the hackers.

DNS injection, or DNS Server Dynamic Update Record Injection, can be executed by tools, such as Nmap and Nessus. That means the hackers don't need any specialise knowledge, for example, coding and scripting. The software will do everything for them and create damages (Mike, 2019).

Only firewall cannot defend this kind of attack, as it will treat it as permitted, as port 53 is essential for DNS request. I will deploy Cisco (2021) Umbrella for defence: Companies or Users only need to point their clients and servers to the Cisco Umbrella, the DNS resolver every query will be scanned and filtered by Cisco Umbrella. Cisco Umbrella is an intelligent cloud network, which able to process 620 billion daily internet requests, check the resolved IP against its intelligence and database, able to block any connection between users and known or unknown malicious sites.

Besides Cisco Umbrella, Cisco Talos also playing another part to protect users' data. Talos able to analysis every possible threat, and it update and exchange related internet security data with Cisco WSA, ESA, routers, which have connected to the internet and subscribed the Talos services. This forms the largest threat intelligence hub around the globe.

Although static ARP can prevent Man-in-a-middle attack by banning other 3rd party IoT or mobile devices logging into our network, but each person has more than one mobile device nowadays. Especially in the medical network environment, doctors and nurses sometimes cannot only rely on one mobile device; they may use their personal device to communicate with the hospital, even when they are not on duty. Static ARP table may block them from accessing the network when emergency.

In order take a balance between security and useability, WLAN and wireless security measure should be deployed. Cisco Unified Wireless Network Architecture (2021) has created a secure wireless topology but will not affect the useability of users: 802.1X with Cisco Secure Services Client has be installed on the WLAN client; the AP and Wireless Lan Controller (WLC), combining with LWAPP split-MAC architecture, which will be the authenticator.

The WLC able to provide ARP protection, which is a subsidy of static ARP but giving the largest flexibility to users. WLC acts as a relay agent between the WLAN client and DHCP server, performs various checks before sending DHCP request for the client. The primary check is to verify the MAC address included the DHCP request, must be exactly match with the WLAN client which the WLC communicates with. Also, the client should be Cisco Secure Services Client only. By restricting one WLAN client to one DHCP address, DHCP exhaustion attack will be eliminated; also, by default, the WLC blocks any broadcast message from the WLAN clients to the WLAN, this will prevent any WLAN client pretends as a DHCP server and broadcast any confusing DHCP information.

The WLC also acts as an ARP proxy for WLAN clients, it able to maintain records of the associations between MAC and IP addresses. With the MAC-IP database, WLC able to stop any communication of a duplicated IP address, that also can prevent the ARP spoofing. Direct ARP communication between WLAN clients is prohibited, every communication should be screened by WLC, this also prevents the ARP spoofing attacks to other WLAN client devices directly.

Cisco WLC also able to do Dynamic ARP Inspection (DAI) and stop any Man-in-the-middle attack. DAI is enabled on per-VLAN basis, the WLC records and compare ARP requests and responses, including the gratuitous ARPs (GARPs), only those clients with a valid MAC-IP mapping on the DHCP binding table will be able to continue the authentication process. Any ARP message and packet will be dropped and logged if there is no valid entry on the DHCP binding table. This will prevent any further ARP spoofing attack, but also eliminates any further network attack, such as SYNflood and DDOS, etc.

A secure network needs to protect every single point and make them work together. Authentication is another key of network defence. MFA becomes a solution, and it has many options for users and companies to deploy. In the wireless network, the Cisco AP and WLC support both the EAP standards, including Cisco EAP-FAST, PEAP MS-CHAPv2, PEAP EAP-GTC and EAP-TLS. All of them supports the Microsoft AD as AAA Server and single sign-on. Combining with Microsoft Azure AD, the Hybrid Microsoft AD environment allows MFA to passwordless authentication: Companies can choose biometrics, tokens, smart cards, Authenticator apps, SMS and phone calls for authentication (Microsoft, 2021).

Although traditional hacking is still one of the main cause of data loss and network disturbance, human error becomes another main cause of cyber security breach. Education to staffs on cyber security, becomes more important, besides the deployment of network security measures. The National Cyber Security Centre (2021) has advice and guidance, with different topics, including passwords, phishing, devices, internet of things etc, educating the employees how to prevent and avoid any cyber security threat from the basics, it also has guidance for large organisations on how to deploy cloud security, mitigating malware and ransomware attack, and how to plan and deploy risk management on cyber security. These materials can educate the management level to plan, assess, and deploy any cyber security measure effectively. The NCSC also has reports and advisories regularly. The reports raise and update the latest vulnerabilities and exploitation, and warns the enterprises to prevent any possible cyber security threat and risk.

Reference:

Mike, S (2019) *DNS Record Injection using Nmap and Nessus,* Available at: *https://whttps://shellsharks.com/dynamic-dns-injectionww.itgovernance.eu/blog/en/pros-and-cons-of-penetration-testing* (Accessed: 28th May 2021).

Andera, G (2021) *Protective DNS: What it is, why it matters, and what you need,* Available at: *https://umbrella.cisco.com/blog/protective-dns-what-it-is-why-it-matters-and-what-you-need* (Accessed: 28th May 2021).

Cisco (2021) *Cisco Unified Wireless Network Architecture—Base Security Features. Enterprise Mobility 4.1 Design Guide* [Online]. Available at: *https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch4_Secu.html* (Accessed: 13th May 2021).

Microsoft (2021) *How it works: Azure AD Multi-Factor Authentication,* Available at: *https://docs.microsoft.com/en-GB/azure/active-directory/authentication/concept-mfa-howitworks* (Accessed: 28th May 2021).

National Cyber Security Centre (2021) *The National Cyber Security Centre,* Available at: *https://www.ncsc.gov.uk/* (Accessed: 28th May 2021).