Discussion Forum 2: Summary and Reflection

The outcome of many of the information gathering scans carried out paved the way for further analysis both for the design document as well as the Executive Summary report, submitted in Unit 11. I would say one outcome of these tests was to see how much information could be gathered throughout the recon stage. Perhaps more important is deciding what information is relevant and can stay, relative to what might appear to be good information that really isn't imperative to future results. For example, running the dig or whois commands would turn up a great deal of information regarding DNS and registrar information, but once it's ascertained that the website is hosted by Amazon, the remaining information is largely inconsequential. This wouldn't have been the case if the site was self hosted though and important contact information (listed as the domain registrar contact) may make useful targeting information for future social engineering experiments.
Tools such as Nikto would ultimately prove the most useful. Many of the vulnerability scanners would go on to prove the most informative, but only Nikto was used at this point. As covered in other posts and reflective pieces, one of the drawbacks of these scanners is they improve performance and thoroughness at the cost of subtlety. These scans will provide a great deal of information covering an entire domain, but will likely be caught by most intrusion prevention and detection platforms. This makes these types of tools great for contract penetration and compliance testing and auditing. Where a bit of stealth can be sacrificed in the spirit of finding as many holes and vulnerabilities in a target.

Discussion Forum 2: Initial Post

Over the last week Group 1 has largely performed scans centered on information gathering and reconnaissance; no exploit or attack has been attempted on the Amazon Web Services (AWS) site as of yet. Many reconnaissance tools were used throughout the early stages of the exercise, but to keep this post's length within guidelines only a truncated list of tools tested will be elaborated on.

Nmap:
Nmap is an open source network scanning utility used for network discovery and security auditing. Our Nmap scans largely targeted layer three of the OSI model using specialized ICMP packets to perform host discovery and network scans (NMAP, 2017). Nmap has the broadest range of network scanning capabilities of the tools used. Our tests predominantly used ping scans to identify open ports on our webserver. Using nmap we were able to identify that port 80 (HTTP) was open. As a test a number of

additional services such as ssh and telnet were opened and the subsequent scans found that ports 22 and 23 were open. The Nmap command was also tailored to only scan for open UDP ports, finding all UDP ports to be closed (represented by an “open|filtered” output). The lack of response on these ports is indicative of no UDP services being open on the server.

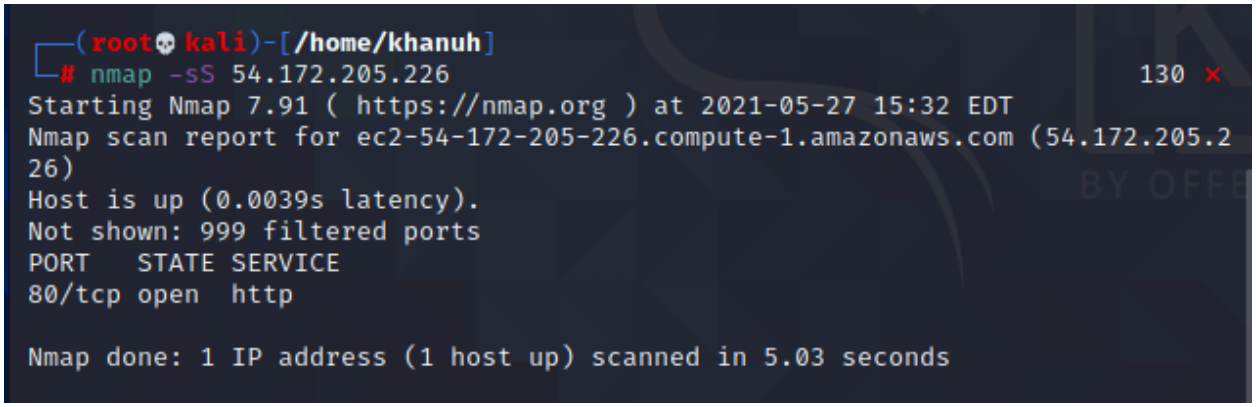

Figure 1: Nmap ping scan showing port 80 for HTTP to be the only open port.

Whois:

The “whois” function is a useful application layer reconnaissance tool that specializes in retrieving organizational and high level technical information on potential targets. Whois queries domain name systems (DNS) and can be used to find details such as the domain owners, where the server is hosted from and domain registrar information (Hoffman, 2020, pp.58–59). Our scans found that our AWS server was owned/hosted by Amazon and located in the Eastern United States; including registrant contact information, phone numbers and associated name servers.

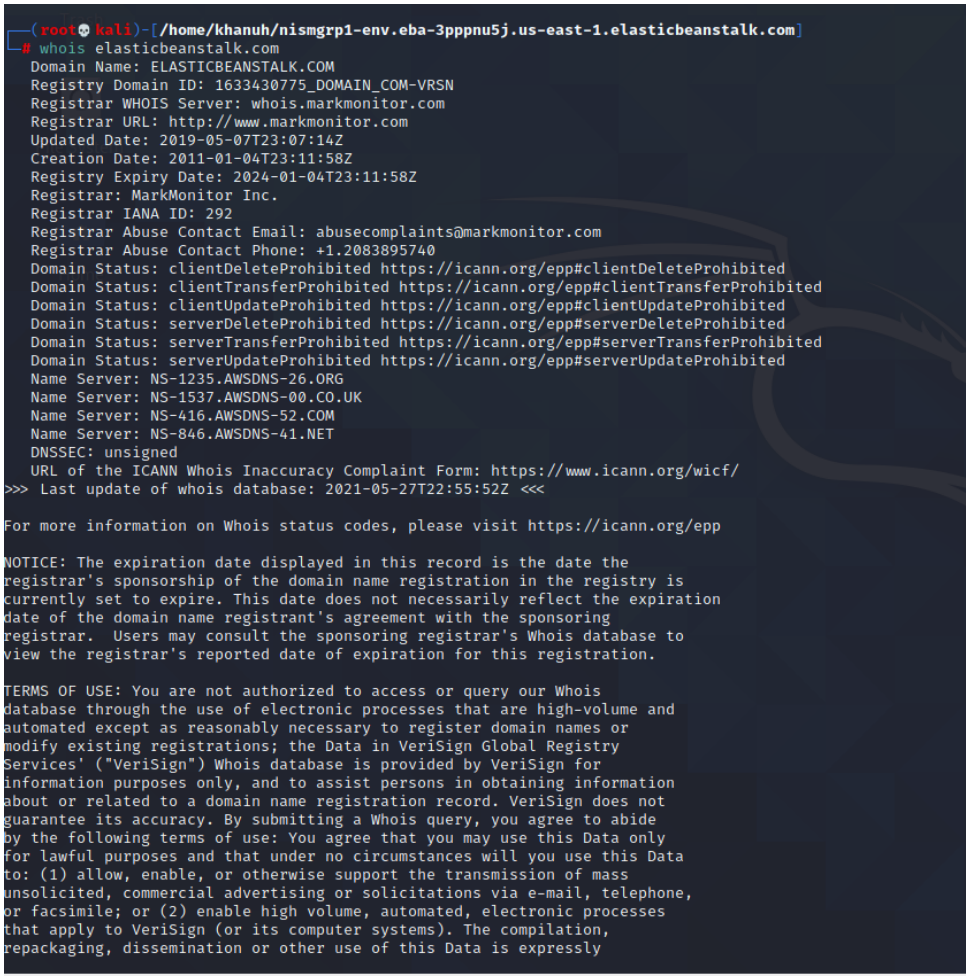

Figure 2: Whois output listing domain registrar and contact information

Nikto:

Nikto is an open source webserver vulnerability scanner capable of identifying outdated server versions, including unique problems present on over 270 different servers. Nikto is also adept at checking for weak configuration files or indexes. While Nikto can gather valuable information the developers also acknowledge that its purpose is to gather as much information as quickly as possible which results in a noisy program who's scans will show up in an intrusion detection or prevention system or a webserver log (Cirt.net, 2019).

Our Nikto scan was able to identify the server and server version as nginx v1.18.0, which is an up to date version of a popular open source webserver. The scan also identified that no anti-clickjacking policy was in place. No CGI directories were found on our AWS setup

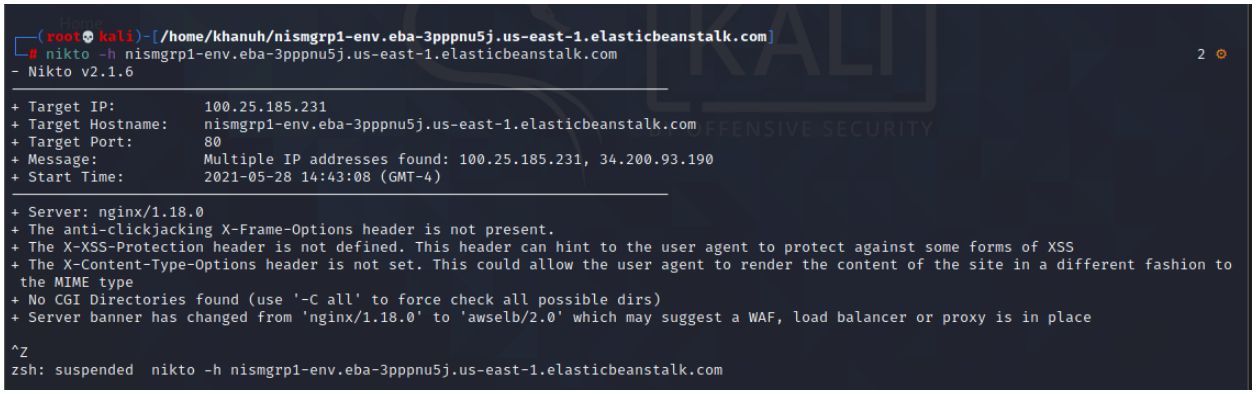

Figure 3: Results of a Nikto scan with information and vulnerabilities listed below the basic network information

Glossary:

UDP | User Datagram Protocol

TCP | Transmission Control Protocol

HTTP | Hypertext Transfer Protocol

AWS | Amazon Web Services

ICMP | Internet Control Message Protocol

References:

Hoffman, H. (2020). *Ethical Hacking With Kali Linux: Learn Fast How To Hack Like A Pro*. Independently Published, 2020, pp.58–59. Available at: https://edu.anarcho-copy.org/Against%20Security%20&%20%20Self%20Security/Ethical%20Hacking%20With%20Kali%20Linux%20Learn%20Fast%20How%20To%20Hack.pdf [Accessed 28 May 2021].

Cirt.net. (2019). *Nikto2 | CIRT.net*. Available at: https://cirt.net/Nikto2 [Accessed 31 May 2021].

NMAP (2017). *Nmap*. Nmap.org. Available at: https://nmap.org/ [Accessed 28 May 2021].