**Discussion Forum 2: Summary Post**

During the Collaborative Learning Discussion 2, we have shared and discussed various tools used for scanning. This was a group project, and Group 1 has primarily performed scans centred on information gathering and reconnaissance; no exploit or attack has been attempted on the Amazon Web Services (AWS) site yet. Many reconnaissance tools were used throughout the early stages of the exercise, and only shortlisted tools only discussed here.

Pathping, which the tutor recommended during our Initial Post also discussed in the post. In addition, Golismero, a tool used to scan the site, is also discussed here.

**Pathping:**

The pathping command is an excellent alternate for the tracert command, which can identify the path from a source system to the destination system. Even though the high-level information provided by both of them are similar, tracert provides the path between source and destination. At the same time, pathping offers details about network latency and network loss at intermediate hops between the source and the destination systems.

**Nmap:**

Nmap is an open-source network scanning utility used for network discovery and security auditing. Our Nmap scans primarily targeted layer three of the OSI model using specialised 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 the 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.

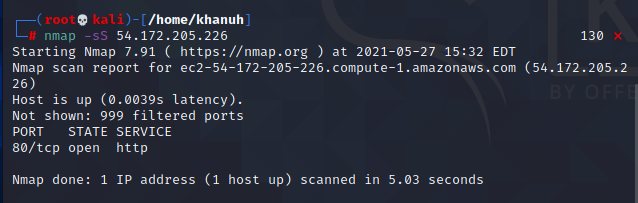


Figure 1: Nmap ping scan showing port 80 for HTTP to be the only open port.

**Whois:**

The “whois” function is a helpful application layer reconnaissance tool specialising in retrieving organisational 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). For example, 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.

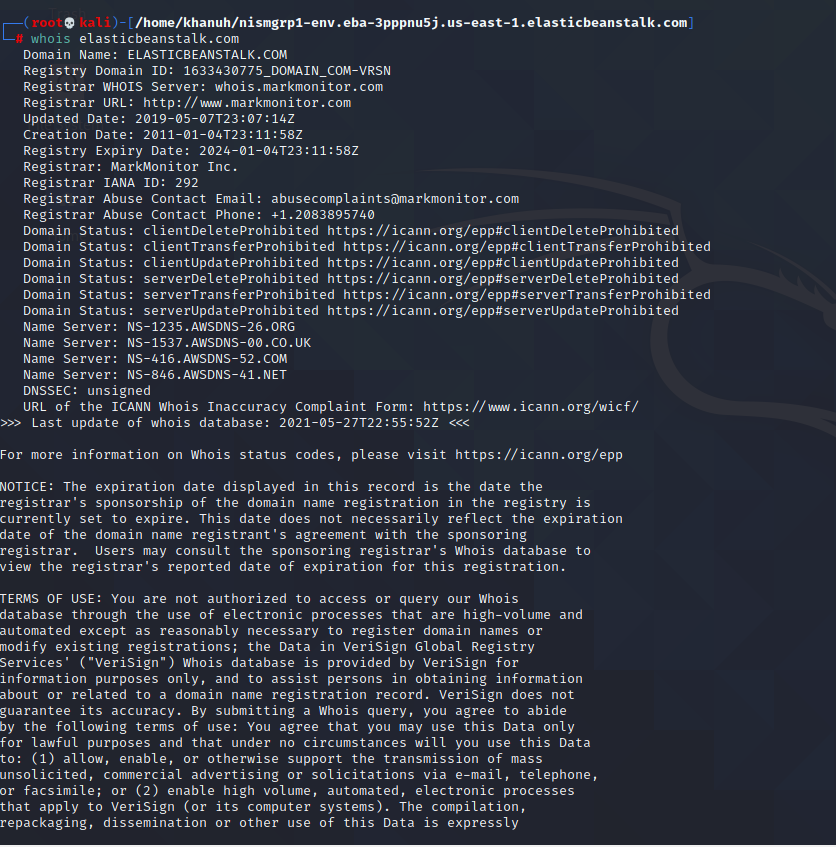


Figure 2: Whois output listing domain registrar and contact information

**Nikto:**

Nikto is an open-source web server 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 possible, resulting in a noisy program whose scans will show up in an intrusion detection or prevention system or a web server 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 web server. The scan also identified that no anti-clickjacking policy was in place. No CGI directories were found on our AWS setup

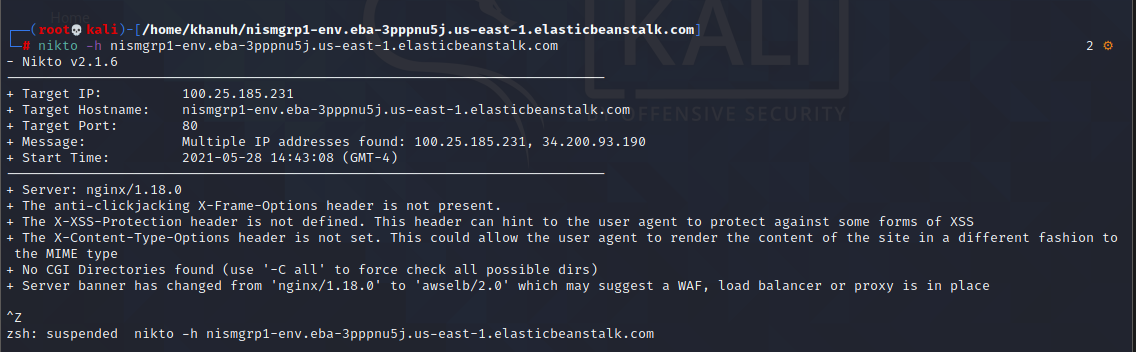
****

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

**Golismero:**

Golismero is an open-source framework that can be used for security testing. Even though it is targeted towards web security, it can be extended to other types of assessments. However, the GoLismero scan performed didn’t identify any vulnerabilities and scan results are presented below.

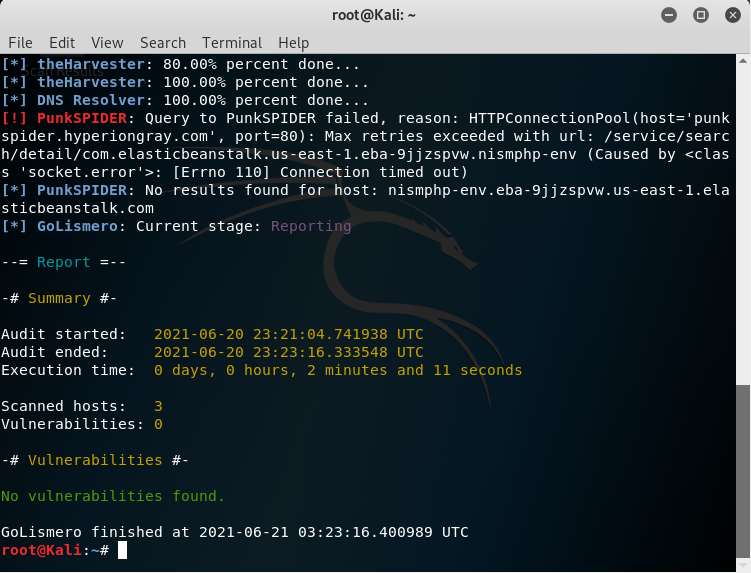


Figure 4: Results of a Golismero scan with information – no vulnerabilities were identified.

**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].