Scanning Exercise: Initial Post

Course: MSc Computer Science

Module: Network and Information Security Management

Assignment: ePortfolio

Date: Wednesday 22nd September 2021

Student ID: 126853

Post:

I am submitting this post on behalf of Team C. The following summary contains details of the basic scanning/host identification tools which can be used to gain information about a domain or the associated IP address space. All commands below were run on a clean Ubuntu 20.04 LTS install within WSL2 on Windows 10.

Number of hops from originating machine to the destination website:

In order to get the number of hops between the originating PC and the destination website, the Traceroute tool was used. The Traceroute tool is a command-line utility which can be used to trace the path that an IP packet takes to its destination (Microsoft, n.d.)

Command: traceroute -I Nismphp-env.eba-kptvqjff.us-east-1.elasticbeanstalk.com

Result: When executing the above command on my PC, there were 7 responses to the traceroute query. The longest delay was within steps 8 and 9, which took 106.091 and 105.324 ms to respond to the request.

Main nameservers for the website:

In order to get details of the websites nameservers, we were required to use the dig utility against the root domain (elasticbeanstalk.com). The dig utility provides an interface for interrogating DNS servers, returning the results to the user (IBM, n.d.).

Command: dig 8.8.8.8 elasticbeanstalk.com NS

Result: This query was executed using the Google Public DNS servers. A total of 4 nameservers which were responsible for the resolution of *.elasticbeanstalk.com were returned, all of which were in the following format: ‘ns-{num}.awsdns-{num}.{tld}’.

Registered contact for the website:

In order to get the details of the registered contact for the site, we were required to run the whois utility against the root domain (elasticbeanstalk.com). The whois utility provides access to data about a domain and its owners held by ICANN accredited registrars (ICANN, n.d.), which help maintain the integrity of the domain name and website ownership processes (DomainTools, n.d.)

Command: whois elasticbeanstalk.com

Result: This query returned the WHOIS data of the ElasticBeanstalk root domain, including the registrant details and the abuse contacts.

MX Record for the website:

In order to get the MX record for the site, we were required to run the dig utility against the root domain (elasticbeanstalk.com). An MX record is also known as a ‘Mail Exchange’ record, which directs email messages to a specific server (Cloudflare, n.d.).

Command: dig 8.8.8.8 elasticbeanstalk.com MX

Result: No MX records existed for the elasticbeanstalk.com root domain.

Website hosting details:

In order to get details of the website host, we are first required to get the IP address of the responding server. This can then be queried using the whois utility, returning details about the organisation that owns the address space, as well as the RIR responsible for controlling the address space.

Command: nslookup Nismphp-env.eba-kptvqjff.us-east-1.elasticbeanstalk.com & whois 44.198.4.25

Result: The nslookup command above resolved the domain provided by Team B to the IPV4 address of 44.198.4.25. When performing a WHOIS search on the IP address, it resolved to IP address space allocated to “Amazon Web Services, Inc.” issued by the ARIN regional address registry.

Screenshot:

Initial Post (Team C)
54 days ago

3 replies
Last 44 days ago

I am submitting this post on behalf of Team C. The following summary contains details of the basic scanning/host identification tools which can be used to gain information about a domain or the associated IP address space. All commands below were run on a clean Ubuntu 20.04 LTS install within WSL2 on Windows 10.

Number of hops from originating machine to the destination website:

In order to get the number of hops between the originating PC and the destination website, the Traceroute tool was used. The Traceroute tool is a command-line utility which can be used to trace the path that an IP packet takes to its destination (Microsoft, n.d.)

Command: traceroute -I Nismphp-env.eba-kptvqjff.us-east-1.elasticbeanstalk.com

Result: When executing the above command on my PC, there were 7 responses to the traceroute query. The longest delay was within steps 8 and 9, which took 106.091 and 105.324 ms to respond to the request.

Main nameservers for the website:

In order to get details of the websites nameservers, we were required to use the dig utility against the root domain (elasticbeanstalk.com). The dig utility provides an interface for interrogating DNS servers, returning the results to the user (IBM, n.d.).

Command: dig 8.8.8.8 elasticbeanstalk.com NS

Result: This query was executed using the Google Public DNS servers. A total of 4 nameservers which were responsible for the resolution of *.elasticbeanstalk.com were returned, all of which were in the following format: 'ns-{num}.awsdns-{num}.{tld}'.

Registered contact for the website:

In order to get the details of the registered contact for the site, we were required to run the whois utility against the root domain (elasticbeanstalk.com). The whois utility provides access to data about a domain and its owners held by ICANN accredited registrars (ICANN, n.d.), which help maintain the integrity of the domain name and website ownership processes (DomainTools, n.d.)

Command: whois elasticbeanstalk.com

Result: This query returned the WHOIS data of the ElasticBeanstalk root domain, including the registrant details and the abuse contacts.

MX Record for the website:

In order to get the MX record for the site, we were required to run the dig utility against the root domain (elasticbeanstalk.com). An MX record is also known as a 'Mail Exchange' record, which directs email messages to a specific server (Cloudflare, n.d.).

Command: dig 8.8.8.8 elasticbeanstalk.com MX

Result: No MX records existed for the elasticbeanstalk.com root domain.

Website hosting details:

In order to get details of the website host, we are first required to get the IP address of the responding server. This can then be queried using the whois utility, returning details about the organisation that owns the address space, as well as the RIR responsible for controlling the address space.

Command: nslookup Nismphp-env.eba-kptvqjff.us-east-1.elasticbeanstalk.com **&** whois 44.198.4.25

Result: The nslookup command above resolved the domain provided by Team B to the IPV4 address of 44.198.4.25. When performing a WHOIS search on the IP address, it resolved to IP address space allocated to "Amazon Web Services, Inc." issued by the ARIN regional address registry.

References:

Microsoft. (n.d.) How to Use TRACERT to Troubleshoot TCP/IP Problems in Windows. Available from: **https://support.microsoft.com/en-us/topic/how-to-use-tracert-to-troubleshoot-tcp-ip-problems-in-windows-e643d72b-2f4f-cdd6-09a0-fd2989c7ca8e** [Accessed 4th September 2021].

IBM. (n.d.) dig Command. Available from: **https://www.ibm.com/docs/en/aix/7.1?topic=d-dig-command** [Accessed 4th September 2021].

ICANN. (n.d.) About WHOIS. Available from: **https://whois.icann.org/en/about-whois** [Accessed 5th September 2021].

DomainTools. (n.d.) What is Whois Information and Why is it Valuable?. Available from: **https://www.domaintools.com/support/what-is-whois-information-and-why-is-it-valuable** [Accessed 5th September 2021].

Cloudflare. (n.d.) What is a DNS MX record?. Available from: **https://www.cloudflare.com/en-gb/learning/dns/dns-records/dns-mx-record/** [Accessed 5th September 2021].

References:

Cloudflare. (n.d.) What is a DNS MX record?. Available from: https://www.cloudflare.com/en-gb/learning/dns/dns-records/dns-mx-record/ [Accessed 5th September 2021].

DomainTools. (n.d.) What is Whois Information and Why is it Valuable?. Available from: https://www.domaintools.com/support/what-is-whois-information-and-why-is-it-valuable [Accessed 5th September 2021].

IBM. (n.d.) dig Command. Available from: https://www.ibm.com/docs/en/aix/7.1?topic=d-dig-command [Accessed 4th September 2021].

ICANN. (n.d.) About WHOIS. Available from: https://whois.icann.org/en/about-whois [Accessed 5th September 2021].

Microsoft. (n.d.) How to Use TRACERT to Troubleshoot TCP/IP Problems in Windows. Available from: https://support.microsoft.com/en-us/topic/how-to-use-tracert-to-troubleshoot-tcp-ip-problems-in-windows-e643d72b-2f4f-cdd6-09a0-fd2989c7ca8e [Accessed 4th September 2021].