Network and Information Security Management May 2021 A

« Collaborative Learning Discussion 2

Charlotte Wilson

Team Initial Post

18 days ago

4 replies


Last 4 days ago

The post below is on behalf of our whole team: myself, Freya Basey, Craig Watts, Dinko Isic, Jan Kufner.

For the scan of the opposite team's website, multiple scans and tools were used such as: Nmap, Traceroute, Nslookup, Whois, MTR, Ping and Dig. As a team, we collated our results together to provide the following information. The exercise seems to emulate reconnaissance which is the first step of the network security assessment methodology. The purpose of reconnaissance is to map the network, hosts and sometimes users to provide a foundation for further assessment activities, such as vulnerability scanning (McNab, C., 2016).

Using Traceroute (Linux) or tracert (Windows), we were able to see the distance between our machines to the target website. We found collectively that we had a few timeouts / no TTL expiry replies from some servers along the route while the command was running; however, on average we saw between 13 - 30 plus hops. These scans used ICMP packets, which have low priority and are sometimes simply blocked by some firewalls.

Utilising MTR and Nmap we were able to send TCP packets for trace-routing, which assemble a more realistic route for traffic, since standard HTTP requests to load a website are typically sent via TCP. Nmap additionally gave some more features to e.g. fragment packets, to circumvent web application firewalls (WAF), which Amazon Web Services (AWS) likely does have in place. Our results for this were varied, some showing only two hops which is unrealistically short. This however could be explained by the fact that the router from our home networks handled the majority of TCP traffic, which led to skipping of hops in the result of the scan. Using mobile phone WiFi spots, or cloud hosted Kali installations, we were able to circumvent the issue and managed to see 5 to 11 hops.

We were also able to identify the hosting locations and multiple nameservers through our scans. We also were able to find the MX records of the website using Nslookup; however, some of our team did experience issues with finding this information, initial scans not showing any MX record available.

A number of us did encounter issues with network diagnostic tools utilising ICMP, such as Traceroute. This may be due to security controls encountered on the route the packets take, for example firewalls (Parziale, L., et al, 2006). That being said, we were able to overcome challenges and collectively find useful information using basic scans against the opposite website.

REFERENCES

McNab, C. (2016) *Network Security Assessment: Know Your Network*. 3rd ed. O'Reilly Media.

Parziale, L., Britt, D., Davis, C., Forrester, J., Lui, W., Matthews, C. & Rosselot, N. (2006) *TCP/IP Tutorial And Technical Overview*. 8th ed. New York: IBM.

Reply

4 replies

1

Post by **Kin Wong**

15 days ago

Peer response

It is possible that the connection for testing, from the client to the server, could make a huge difference to the result, including number of hops and latency.

Latency means the speed of data, but it is affected by bandwidth, which means the capacity of the network. Although a high bandwidth doesn't mean you will achieve an optimal network performance. Packet loss, latency, jitter may also slow down the network even it has a high-speed connection.

But on the other hand, bandwidth and latency are affecting with each other. Latency will increase if the connection has not enough bandwidth, as latency is used to measure the speed of the data packets reaching the destination. A high-speed network with huge bandwidth can help to reduce the latency and network performance, but also prevent any packet dropping (DNSstuff, 2021).

Although MTR and Nmap can display the routes and number of hops, but the results could be varied every time, and we may not discover where is the bottle-neck. Under a complicated internet environment nowadays, a more advanced networker analyser is needed, if we want to analyse the connection compre-hensively. Solarwinds (2021) Network Packet Analyzer is an example. Its Net-work Performance Monitor able to measure the network path latency of every hop, identify irregularities and bottlenecks at any point. Packet-level information not only can provide network performance data, but also the response time and traffic count of a specific application. This helps us to discover the root causes of end-user impact about the network performance, but not just in general.

References:

DNSstuff (2021) *Network Latency vs. Throughput vs. Bandwidth,* Available at: *https://www.dnsstuff.com/latency-throughput-bandwidth* (Accessed: 2nd June 2021)

SolarWinds (2021) *Network Packet Analyzer with Network Performance Monitor,* Available at: *https://www.solarwinds.com/network-performance-monitor/use-cases/packet-analyzer* (Accessed: 2nd June 2021).

Reply

2  Post by **David Luvaha**

8 days ago

Peer Response

Similarly, as explained by Kin Wong, Elsevier (2021) explains that Pathping just like tracert provides statistics on network latency and loss between two communicating nodes by ascertain the number of hops between them. The scan produced a maximum of 30 hops and a Round Trip Time (RTT) of 10ms. High latency and data losses could be attributed to poor internet connectivity speeds between the communicating node.

References

Elsevier(2021) Pathping

Available from:

https://www.sciencedirect.com/topics/computer-science/tracert-command

[Accessed 25 May 2015]

Reply

3  New Post by **Dario De Giorgi**

5 days ago

Peer Response

I would like to add something to what my classmates are explaining, based on the OSI model the traceroute tool uses the transport and network layer, it uses the ICMP and UDP protocols. When the traceroute command is done, it sends an echo packet with a TTL of 1 to the destination host, the first router changes the TTL to 0 and sends an ICMP message back to the user executing the command, this will be repeated with TTL values to identify the exact actual path between the source and the destination. However, on the internet traceroute messages are often blocked by routers, which can make traceroute results less accurate.

References :

Parziale, L., T. Britt., D, Davis, C., Forrester, J., Liu, W.,Matthews, C., Rosselot, N. (2006) TCP/IP Tutorial and Technical Overview : Redbooks.

Learning center (N.D) What is traceroute & what is it for? Available from: https://www.thousandeyes.com/learning/glossary/traceroute [Accessed 13 June 2021].

Reply

4  New Post by **Charlotte Wilson**

4 days ago

Team Summary Post

From the discussion held regarding the initial scan of the website, it appeared that others experienced similar outcomes. This exercise has simulated an initial penetration test on a target website. From this, we have found potential vulnerabilities that can be exploited, such as the lack of MX record can cause reputational damage to a website (Fraud Watch, 2016).

It appeared that Traceroute (Linux) or tracert (Windows) provided a similar number of hops for teams scanning different websites; however, they also experienced similar issues regarding the timeouts. For example, we found a difference in hop count when using TCP route and ICMP traceroute. TCP provided less hops and a more realistic route, whereas ICMP showed more hops but an unrealistic route. This is because, generally, ICMP can be flagged as low priority traffic. ICMP packets have lower priority than TCP packets and are therefore not always sent on the shortest way along their route. (Parziale et al., 2006)

It also seems that many other teams are using similar tools, such as Tracert, NMap, and MTR to conduct the security scans of the websites. This is expected as the tools used are standard tools for penetration testing and scanning. All provide the basic information required to start exploiting vulnerabilities, but they should never be used solely in isolation.

The information identified by the scans, can be used to exploit further. For example, using ping provides the IP Address and confirmation that the server is responding to a ping command. Nmap can be used to identify potential target devices on the network. This can then be used further to monitor those identified hosts for other activities (Ferranti, M., 2018).To add to the initial scans conducted, further scanning will be planned using the tools mentioned in the discussion. This will be done following a step-by-step process in line with penetration testing standards.

References

Fraud Watch (2016) Email Security: MX Records. Available from: **https://fraudwatchinternational.com/phishing/email-security-mx-records/** [Accessed 5 June 2021]

Ferranti, M (2018) What is Nmap? Why you need this network mapper. Available from: https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html [Accessed 10 June]

Parziale, L., Britt, D., Davis, C., Forrester, J., Lui, W., Matthews, C. & Rosselot, N. (2006) *TCP/IP Tutorial And Technical Overview.* 8th ed. New York: IBM.

Reply

Add your reply

Your subject

Type your post

Dateien auswählen Keine ausgewählt

Submit

Use advanced editor and additional options

OLDER DISCUSSION

Team initial post

NEWER DISCUSSION

Initial Post