



Scanning Exercise: Summary Post

Course: MSc Computer Science

Module: Network and Information Security Management

Assignment: ePortfolio

Date: Saturday 30th October 2021

Student ID: 126853

Post:


Our initial posts to this Collaborative Discussion Forum contained a series of tools/utilities which we could use for host identification tasks, such as identifying the Hosting Provider, Domain Owner and Email Servers. In addition, a series of commonly available tools such as Ping, Traceroute, Whois and NSLookup were used to get specific information from the domain assigned to us for investigation.

Throughout this discussion, we identified that the investigated sites were hosted on sub-domains of the *.elasticbeanstalk.com domain, therefore attempts to gain Whois information were unsuccessful. In such cases, we were required to perform a lookup of the root domain (elasticbeanstalk.com), which does not provide information about the responsible parties, but that of Amazon Web Services.

Within the contents of the three modules, we compared the OSI and TCP network models, identifying why TCP has become adopted over the conceptual OSI standard. During initial discussions, it was highlighted that the TCP standard, being open-source, was far cheaper for vendors to implement in their technologies and significantly easier to implement changes. In addition, the International Standardization organisation managed the OSI stack; therefore, any changes would have required overall agreement from all involved parties.

Finally, in Unit 6, we have investigated a series of Penetration Testing utilities that could be used within our Executive Summary document to be produced within Unit 11. All of the discussed tools had a large following within the penetration testing community, most of which received regular software updates and enhancements to identify the newest released vulnerabilities. Following further research, these tools were selected to be included in our Design Document, which would be used to compile a comprehensive vulnerability analysis in Unit 11.

Screenshot:


[Kieron Holmes](#)

Summary Post
48 secs ago

Our initial posts to this Collaborative Discussion Forum contained a series of tools/utilities which we could use for host identification tasks, such as identifying the Hosting Provider, Domain Owner and Email Servers. In addition, a series of commonly available tools such as Ping, Traceroute, Whois and NSLookup were used to get specific information from the domain assigned to us for investigation.

Throughout this discussion, we identified that the investigated sites were hosted on sub-domains of the " elasticbeanstalk.com domain, therefore attempts to gain Whois information were unsuccessful. In such cases, we were required to perform a lookup of the root domain (elasticbeanstalk.com), which does not provide information about the responsible parties, but that of Amazon Web Services.

Within the contents of the three modules, we compared the OSI and TCP network models, identifying why TCP has become adopted over the conceptual OSI standard. During initial discussions, it was highlighted that the TCP standard, being open-source, was far cheaper for vendors to implement in their technologies and significantly easier to implement changes. In addition, the International Standardization organisation managed the OSI stack; therefore, any changes would have required overall agreement from all involved parties.

Finally, in Unit 6, we have investigated a series of Penetration Testing utilities that could be used within our Executive Summary document to be produced within Unit 11. All of the discussed tools had a large following within the penetration testing community, most of which received regular software updates and enhancements to identify the newest released vulnerabilities. Following further research, these tools were selected to be included in our Design Document, which would be used to compile a comprehensive vulnerability analysis in Unit 11.

Reply

Edit

Delete