Project 2:

The Network Sleuth

Please complete the following for submission as project 2

DUE BY: 11/1/2024 @ 11:00pm

Network Analysis

Introduction

You have gained covert access to the network of a known hacker and set up monitoring to determine what they are up to.

Entities:

- The IP address of the device on the network being watched is 172.16.27.8.
- The routing/gateway device can be found at 172.16.27.30 and is managed via HTTP.
- The local mail server can be found at 172.16.27.25 and provides the SMTP service and is managed via TELNET.
- The local web server can be found at 172.16.27.6 and provides the HTTP service and is managed via TELNET.

The packet capture contains network activity captured passively via a device on the network. You have been provided a packet capture and the shared keys used for all "secure" traffic. Please determine at least the following information:

5 points each (25 total)

1. What is the MAC address of the device being watched? (hex in colon-separated format)
2. What is the MAC address of the gateway device? (hex in colon-separated format)
3. What was the IP of the first device that was pinged (ICMP Echo Request)?
4. What DNS server(s) is/are being used to resolve names to IPs?
5. According to DNS in the capture, what IPv4 address hosts the duckduckgo.com website (A record)?

10 points each (50 total)

6. What account was used to log into the router device via HTTP? (username and password)
7. What account was used to log into the local mail server via TELNET? (username and password)
8. At the time of the capture, how long had the local mail server been up (uptime found in TELNET)?
9. Who did the target send e-mail as and to during the interaction via SMTP and what was the content of the message? (provide the from and to email addresses)
10. What version of the Linux kernel is the local mail server running, which can be found via TELNET interactions? (it is of the format "Linux 6.x.y-z-amd64")

15 points each (75 total)

11. According to the HTTP2 GET requests, embedded in the HEADERS, what was the first, complete search request sent by the user, via www.duckduckgo.com (they require the use of the ssl keys provided)?
12. According to the HTTP2 GET requests, embedded in the HEADERS what was the last, complete search request sent by the user, via www.duckduckgo.com (they require the use of the ssl keys provided)?
13. What information was provided on the webpage loaded from the local web server?
14. What record on the local web server was changed (two requests for the same page … you will need to compare)?
15. What vendor made the local router and what model is it, which can be found via HTTP interactions?

Your analysis MUST include a packet number as well as a note as to how you interpreted the data in that packet to arrive at your conclusion as well as any filters you used to reach the information in question.

Grading as follows:

- 150pts – broken down as described above (includes the answer and the details of how you found the answer. Answers alone will not result in full credit; you must account for how and where you found the answers. This can include display filters and screen shots as needed.
- TOTAL - 150pts

Extra credit, in an amount to be determined by me, will be given for pertinent information beyond what is asked above. Depending on the seriousness and/or value of the information, up to 20pts per data-point may be assigned with a maximum total value of 100pts.

You must submit your analysis through Sakai with a filename as follows LASTNAME.xxx (where LASTNAME is replaced with your last name. The xxx is the extension of the application used to write your analysis … e.g. .txt, .docx, .pdf, .rtf, etc.).