Team: Team 07

Inject Number: 16

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 09 Feb 2019 19:35:30 +0000

From: CISO

To: Infrastructure Team

Subject: Install Wireshark and Monitor Network

Deliverable: Provide a business memo response to the CISO that includes four (4) sections:

1) Confirmation of Wireshark installation on the Windows 10 machine (include screenshot of running application not the icon);
2) An executive summary of the analysis and findings for the required remote access ports and traffic (include mention of any suspicious traffic was discovered);
3) the proper configuration parameters for capturing only the described remote access ports (screenshot or text description) and
4) two screenshots - the first for the DNS traffic verification showing valid traffic captured and second the capturing of the described remote access ports (whether traffic is seen or not).

As part of monitoring the network there is a need to audit/verify compliance and monitor for common intrusion vectors on the network. Download and install wireshark from https://www.wireshark.org/ on the Windows 10 machine outside the firewall. Once installed, verify packets can be seen by monitorign on UDP port 53 to verify DNS traffic can be seen (monitor/audit known remote access TCP ports for 5 minutes both in and out of the network with any of the following destination ports (ssh - 22, telnet - 23, rexec - 512, rlogin - 513, rsh - 514, rdp - 3389, X-Windows - 6000-6002).

Download and install WireShark (http://www.wireshark.org/download.html) develop and deliver the requested business memo.

Thank you.

CISO