Team: Team 3

Inject Number: 42

Inject Duration: 75 Minutes

Inject Start Date/Time: Sat, 24 Mar 2018 13:41:55 -0500

From: Chief Information Security Officer

To: Infrastructure Team

Subject: [O-211] Network Analysis

To ensure the company/team is keeping current with network forensics and analysis of packet captures, I have decided to conduct an exercise to provide some on the job training and measure the capabilities of the team. The use of Wireshark with required dissectors is required for this exercise. Utilizing Windows Network Monitor or other packet capture tools will result in no points being awarded and may require that you consider employment elsewhere. The exercise is to capture all traffic on tcp ports 139 and 445 on the 2008 R2 AD/DNS Exchange Server network connection. The packet capture should run until you can capture the following events:
1) Successful domain login from the Windows 8.1 machine,
2) Failed domain login from the Windows 8.1 machine,
3) Successful file access from the Windows 8.1 machine to the domain controller,
4) Successful domain login from the Ubuntu 12.04 machine,
5) Failed domain login from the Ubuntu 12.04 machine, and
6) Successful file access from the Ubuntu 12.04 machine to the domain controller.

Once captured, isolate the 6 events described above. Include in a business memo, a breakout of six events and the detailed packet capture of each event. Do not include packets unrelated to each event. Then answer these questions in the memo for the captured data
a) are the transactions (fully, partially, not) encrypted,
b) The stated size in the IP header is smaller than the stated size by Wireshark? What is the difference (numerically) between the two numbers for a specific packet? What causes this difference?
c) What is the source port of the transaction?
d) How is the source/destination port chosen by each application?
e) In the SMB transactions, how many different SMB protocol options (not IP or TCP, but within the SMB protocol) are there that can be set by

individual/discrete flags (provide evidence via a screen capture to support your answer)?

Thank you.

Chief Information Security Officer