Lab2 Network analysis and forensics

Using the 6 pcap files in the attached folder, pick and answer 10 questions from the file below. For each answer, you are supposed to justify and support your answer (e.g. with a screenshot, statement, etc.).

A small utility in an unnamed locale has a small SCADA test environment setup. The staff at this utility have installed a DSL line to enable remote access to this system. Unfortunately, the utility staff did not adequately consider the security implications of doing this, leaving the test environment open to attack from the internet.

After experiencing odd behavior on this system, the lead engineer began looking at system logs and network traffic in an attempt to troubleshoot the issue. He discovered what appeared to be unauthorized access into the system. You have been called in to examine this evidence and help determine what has occurred.

Your task, should you choose to accept it, is to examine these evidentiary artifacts to determine what has happened, and provide answers to the following questions.

Before you begin, please download and install Wireshark (1.4.6 or later), and then download the following ZIP file (containing 6 packet capture files) for analysis:
February 2012 Cyber Quest PCAP's
Section 1: Initial recon and entry

Artifacts
Packet capture - entry.pcap
Question 1
Marks: 1
What service appears to be running on port 2200?
Choose one answer.
- Industrial Control Interface
- Rockwell Automation PPTP
- Inter Carrier Interface
- Secure Shell

Question 2
Marks: 1
It appears that after running a scan, the attackers made connections to each of the open ports. Which of the following tools was most likely used to establish those connections?
Choose one answer.
- Nessus
- SSH
- Telnet
- Netcat

Question 3
Marks: 1
Which IP address had port 2200 open?
Choose one answer.
- 10.1.10.33
- 10.1.10.60
- 10.1.10.20
- 10.1.10.130

Question 4
Marks: 1
Which version of SSH was the attacker using?
Choose one answer.
- WinSSH
- PuTTY
- OpenSSH 5.3p1
- OpenSSH 5.2

Section 2: Initial Recon

Artifacts
Packet capture: init.recon.pcap
Question 5
Marks: 1
Which of the following IP addresses appear to be the same type of device?
Choose one answer.
- 10.1.10.13 and 10.1.10.29
- 10.1.10.20 and 10.1.10.29
- 10.1.10.15 and 10.1.10.13
- 10.1.10.20 and 10.1.10.130

Question 6
Marks: 1
How many IP addresses had port 3389 open?
Choose one answer.
- 1
- 2
- 3
- 4

Question 7
Marks: 1
Which of the following IP addresses appears to be running a Human Machine Interface (HMI)?
Choose one answer.
- 10.1.10.60
- 10.1.10.130
- 10.1.10.29
- 10.1.10.20

Question 8
Marks: 1
Which of the following IP addresses did NOT have port 23 open?
Choose one answer.
- 10.1.10.10
- 10.1.10.27
- 10.1.10.16
- 10.1.10.29

Question 9
Marks: 1
Which of the following ports was not included in the scan of the internal network?
Choose one answer.
- TCP 3389
- TCP 80
- TCP 23
- TCP 2200

Question 10
Marks: 1
Approximately how long did the port scan take to complete?
Choose one answer.
- 27.1 seconds
- 4.0 seconds
- 3.5 seconds
- 17.1 seconds

Section 3: SCADA Protocols

Artifacts
Packet capture: HMI2PLC.pcap
Question 11
Marks: 1
Which of the following best describes the nature of the communications between .20 and .130?
Choose one answer.

Each device sends data as needed based on operational events.
Each device sends data at regular intervals
The .130 device sends data at regular intervals
The .20 device requests data at regular intervals
Both devices exchange data at regular intervals

Question 12
Marks: 1
A number of packets from .20 to .130 appear to have a counter. Which of the following represents the packet offset location of the counter?
Choose one answer.
0x73
0x26
0x42
0x2a

Question 13
Marks: 1
Which of the following protocols appears to be in use between the two devices?
Choose one answer.
Ethernet over IP
Common Instrumentation Protocol
Modbus
Ethernet Industrial Protocol

Section 4: PLC web recon

Artifacts
Packet Capture: web_recon.pcap

Question 14
Marks: 1
What username was successfully used to access pages on the webserver on .130?
Choose one answer.
admin
ml1100
root
guest

Question 15
Marks: 1
What was the URI that returned an embedded reference to an ActiveX control?
Choose one answer.
/navtree.htm
/dataview.htm
/control.htm
/newdata.htm

Question 16
Marks: 1
Which URL request first resulted in an authentication request?
Choose one answer.
/dataview.htm
/redirect.htm
/navtree.htm
/home.htm

Question 17
Marks: 1
What webserver appears to be running on the .130 device?
Choose one answer.
Apache 2.2.19
A-B WWW/0.1
Firefox/3.6.24
1763-L16BWA B/9.00

Question 18
Marks: 1
What tool do the attackers appear to be using to probe the webserver on .130?

Choose one answer.
- Firefox
- wget
- Nessus
- OpenVAS

Section 5: HMI web recon

Artifact
Packet Capture: hmi_web_recon.pcap

Question 19
Marks: 1
What browser did the attackers use to access the HMI?
Choose one answer.
- Safari
- Chrome
- Firefox
- Internet Explorer

Question 20
Marks: 1
The operating system that appears to be running on the attacker's machine appears to differ from the OS running on 10.1.10.33. Based on the information in the packet capture, what is the most likely explanation?
Choose one answer.
- The attackers are tunneling X11 over an SSH connection
- The attackers are spoofing their source address.
- The attackers set up a tunnel for port 80 over an SSH connection
- The attackers set up a PPTP server on the 10.1.10.33 box

Question 21
Marks: 1
Which of the following passwords was most likely used to authenticate to the HMI webserver?
Choose one answer.
- L3tmein
- password
- fm3y3r-hmi
- hmiviewonly

Question 22
Marks: 1
One of the pages viewed by the attackers contains logs showing logon times. This log appears to have captured their activity on the HMI webserver. Based on this, which U.S. timezone does the HMI appear to be in? [Note: assume the packet capture timestamps were stored in UTC, and are adjusted by Wireshark to reflect your local timezone]
Choose one answer.
- Pacific
- Mountain
- Eastern
- Central

Question 23
Marks: 1
Based on the times from the logfile in the previous question, which of the following most closely represents the time differential between the HMI webserver and the device performing the packet captures?
Choose one answer.
- 3 seconds
- 9 seconds
- 13 seconds
- 51 seconds

Section 6: Attempted Man-in-the-Middle attack on PLC and HMI

Artifact
Packet Capture: ettercap.pcap

Question 24
Marks: 1
The previously mentioned page that showed logon times also contained logs of other events. Based on this page, what event occurred on the HMI on Feb 1 at 3:24:50PM?
Choose one answer.
- A log file rotation
- A user login
- An HMI restart
- A watchdog timer event

Question 25
Marks: 1
Assume that a watchdog timer event indicates a loss of communication between the HMI and the PLC. Based on the packet captures, what is the most likely cause of the communications loss?
Choose one answer.
- The switch began dropping packets due to a MAC table overflow
- A port scan caused the PLC to reboot
- A forged bootp reply changed the PLC’s IP address
- ARP spoofing disrupted communications

Question 26
Marks: 1
Assume that a watchdog timer event indicates a loss of communication between the HMI and the PLC. Which packet most likely first caused the communications failure?
Choose one answer.
- 2922
- 2878
- 2920
- 2879

Question 27
Marks: 1
What appears to be the MAC address of the device which performed the ARP spoofing?
Choose one answer.
- 00:0f:73:02:52:51
- 54:52:55:53:54:1f
- 08:00:27:fb:b8:10
- 14:fe:b5:ab:23:be

Question 28
Marks: 1
What event allowed the PLC and HMI connection to be restored?
Choose one answer.
- The HMI sent an ARP request and the response overwrote the spoofed ARP
- The spoofed ARP timed out
- The PLC sent a gratuitous ARP that overwrote the spoofed ARP
- The attackers spoofed an ARP packet with the correct settings

Question 29
Marks: 1
Which packet allowed communications between the HMI and PLC to be restored?
Choose one answer.
- 21222
- 20796
- 20795
- 20784