1. You notice that the indicator light near the robot’s antenna begins to blink. Perhaps the robot is connecting to a network? Using a wireless card and the network protocol analyzer Wireshark, you are able to create a PCAP file containing the packets sent over the network. You suspect that the robot is communicating with the crashed ship. Your goal is to find the location of the ship by inspecting the network traffic. [ First-contact.pcap ]
2. Ann Dercover is after SaucyCorp’s Secret Sauce recipe. She’s been trailing the lead developer, Vick Timmes, to figure out how she can remotely access SaucyCorp’s servers. One night, while conducting reconnaissance, she sees him log into his laptop (10.10.10.70) and VPN into SaucyCorp’s headquarters.

Leveraging her connections with international hacking organizations, Ann obtains a 0-day exploit for Internet Explorer and launches a client-side spear phishing attack against Vick Timmes. Ann carefully crafts an email to Vick containing tips on how to improve secret sauce recipes and sends it. Seeing an opportunity that could get him that Vice President of Product Development title (and corner office) that he’s been coveting, Vick clicks on the link. Ann is ready to strike…

You are the forensic investigator. Your mission is to analyze the packet capture containing Ann’s exploit, build a timeline, and submit your evidence including… [evidence06.pcap]

1. What was the full URI of Vick Timmes’ original web request? (Please include the port in your URI.)
2. In response, the malicious web server sent back obfuscated JavaScript. Near the beginning of this code, the attacker created an array with 1300 elements labeled “COMMENT”, then filled their data element with a string. What was the value of this string?
3. Vick’s computer made a second HTTP request for an object.
   1. What was the filename of the object that was requested?
   2. What is the MD5sum of the object that was returned?
4. When was the TCP session on port 4444 opened? (Provide the number of seconds since the beginning of the packet capture, rounded to tenths of a second. ie, 49.5 seconds)
5. When was the TCP session on port 4444 closed? (Provide the number of seconds since the beginning of the packet capture, rounded to tenths of a second. ie, 49.5 seconds)
6. In packet 17, the malicious server sent a file to the client.
7. What type of file was it? Choose one:

Windows executable

GIF image

PHP script

Zip file

Encrypted data

1. What was the MD5sum of the file?
2. Vick’s computer repeatedly tried to connect back to the malicious server on port 4445, even after the original connection on port 4444 was closed. With respect to these repeated failed connection attempts:
   1. How often does the TCP initial sequence number (ISN) change? (Choose one.)

Every packet

Every third packet

Every 10-15 seconds

Every 30-35 seconds

Every 60 seconds

* 1. How often does the IP ID change? (Choose one.)

Every packet

Every third packet

Every 10-15 seconds

Every 30-35 seconds

Every 60 seconds

* 1. How often does the source port change? (Choose one.)

Every packet

Every third packet

Every 10-15 seconds

Every 30-35 seconds

Every 60 seconds

1. Eventually, the malicious server responded and opened a new connection. When was the TCP connection on port 4445 first successfully completed? (Provide the number of seconds since the beginning of the packet capture, rounded to tenths of a second. ie, 49.5 seconds)
2. Subsequently, the malicious server sent an executable file to the client on port 4445. What was the MD5 sum of this executable file?
3. When was the TCP connection on port 4445 closed? (Provide the number of seconds since the beginning of the packet capture, rounded to tenths of a second. ie, 49.5 seconds)