You have been asked to conduct a quantitative risk analysis. Which of the following might you use?

Surveys

SLE

Focus groups

Previous experience

Answer: B

Explanation: Quantitative risk analysis uses methods to calculate the specific risk in terms of numerical data, such as cost, downtime, etc. While surveys, focus groups, and your previous experience can be good sources of information to help determine the qualitative risk, they are not useful for calculating the quantitative risk. Instead, formulas like the Single Loss Expectancy are better suited for quantitative risk analysis.

You have recently been hired as a security analyst. During your initial port scans of your network, you determine that the company is still using telnet to configure its switches and routers. You bring the issue up to your boss who believes it isn’t a “big deal”. You disagree and ask his permission to prove how insecure telnet can be. He agrees and lets you set up one tool to prove how insecure telnet is on the network. Which tool will you use to prove how insecure telnet is as he logs into the switch from his workstation?

John the Ripper

Wireshark

Nmap

Netcat

Answer: B

Explanation: Wireshark is a protocol analyzer. By sniffing the network traffic using Wireshark, you will be able to see the username and password your boss uses to login to telnet because telnet doesn’t use any encryption during its communication. This will allow you to see everything he sends and receives to the telnet server, including his username and password. There is no need to crack his password with John the Ripper since it will be displayed as plain text in a protocol analyzer like Wireshark.

Which piece of software can be used to test the network for weak passwords?

Norton Antivirus software

Wireshark

John the Ripper

Nmap

Answer: C

Explanation: John the Ripper is a cross-platform password cracking tool. It is used to crack passwords locally and across the network.