Assignment: Security Testing Tools

Professor Deepa Kundur

Please note that this is an *individual* assignment and each person can talk to others, but must ultimately provide their own answers and write their own assignment report.

In this assignment you will be exposed to tools used in *penetration testing*. A penetration test (often called a pen test) is the process of assessing the security of computing assets by taking the perspective of a potential threat. Pen test analysis occurs by observing how a computing environment behaves in the presence of simulated attacks on the system.

Questions

Consider the following Internet downloadable tools:

- Kismet, www.kismetwireless.net
- Tcpdump, www.tcpdump.org
- Aircrack, www.aircrack-ng.org
- Nmap, www.nmap.org
- Nessus, www.tenablesecurity.com/nessus

1. For each tool, please:
    a. Describe in general what the tool does and if possible why it has been developed.
    b. Describe what resources (hardware, software, specific knowledge) are required to use the tool.
    c. List and describe the types of vulnerabilities the tool addresses.
    d. Describe how the tool could be used to hack into a future smart grid and what impacts it could have. Be creative.
2. Based on your answers in Question 1, do you believe that it is easy for an opponent to hack into a future smart grid? Please explain.