Scanning and Enumeration Laboratory – Module 7 Prelude to a Hack

Background: This lab allows students to use a number of tools discussed in class to learn information about the lab network as well as some information about networks on the Internet.

Requirements/assumptions

- 1 system with Windows 2000 and LanGuard Network Scanner and other network enumeration tools installed
- 1 system with Red Hat Linux and NMAP Network Scanner and other network enumeration tools installed
- Internet access and a web browser
- Local administrative/root privileges

Before attempting to compromise systems in a target network, an intruder may first want to try to gain valuable information about the network (systems, and protocols) which he is going to attack. This gathering of information will allow the attacker to increase the chance of success of the attacks he will run, because the attacks will be much more targeted to the given network environment.

Students should divide into teams of 3-4 to answer the following questions about the lab networks (192.168.30.0/24, 192.168.40.0/24).

Q1 – List all of the operating systems seen on the two networks.
Q2 – How many web servers are operating on the two networks? What OS are these servers running? What type of web servers are these systems running?
Q3 – What are the network layer protocols (aside from IP) observed on the network?
Q4 – What are the IP addresses of systems running FTP and TFTP,?
Q5 – What TCP and UDP ports are open on the Windows 2000 Server (192.168.30.240)
Q6 – Who is the administrative contact for the cmu.edu domain? What is the IP address of one of CMU's external mail servers? What are the hostnames of CMU's public DNS servers?
Q7 – How many systems are alive (reachable) on both networks?

Bonus questions:

B1 – What are the MAC addresses of both interfaces on the router which is routing between the .30 and .40 network?
B2 – Find a file called 'treasure.txt' and encrypt it with the isftsinstructor@192.168.30.19 key and e-mail it to that address. Hint: this file may be available through weak/no authentication protocols. Use what you know about the network to find it.
B3 – Are there any hosts which do not seem to be real hosts? If so, which ones?

