03-Scanning Networks

PLEASE use prebuilt labs

Victim Data: direct interaction Need 2-6 computers online

Scope & Contract:
You may not go past the scanning stage.
You may only do this as a class member after you state you agree in the chat.
You may not publish the results ever.
You may only transmit the results to secure.dbushmiller@gmail.com using PDF password encrypted files.
IN SCOPE 18.144.18.3 and 52.53.152.100 these server will only be open until last day of class.
OUT OF SCOPE mail servers.

If the above is unacceptable, then you are your own scope: do not send any files to anyone.
If you need a website you may use http://certifiedhacker.com/ a real website with no instructions (from ec council)

Advanced: Build a data file / artifact that is actionable by the contract holder. There are no instructions for this task. You must figure everything out.

Attacker Data: Kali/ Parrot

Objective

The objective of this lab is to conduct network scanning, port scanning, analyzing the network vulnerabilities, etc.

Network scans are needed to:

- Check live systems and open ports
- Identify services running in live systems
- Perform banner grabbing/OS fingerprinting
- Identify network vulnerabilities
- Draw network diagrams of vulnerable hosts

Overview of Scanning Networks

Network scanning is the process of gathering additional detailed information about the target by using highly complex and aggressive reconnaissance techniques. The purpose

of scanning is to discover exploitable communication channels, probe as many listeners as possible, and keep track of the responsive ones.

Types of scanning:

- **Port Scanning**: Lists open ports and services
- **Network Scanning**: Lists the active hosts and IP addresses
- **Vulnerability Scanning**: Shows the presence of known weaknesses

Lab Tasks

Ethical hackers and pen testers use numerous tools and techniques to scan the target network. Recommended labs that will assist you in learning various network scanning techniques include:

1. Perform host discovery
    - Perform host discovery using Nmap
    - Perform host discovery using Angry IP Scanner
2. Perform port and service discovery
    - ~~Perform port and service discovery using MegaPing~~
    - ~~Perform port and service discovery using NetScanTools Pro~~
    - Explore various network scanning techniques using Nmap
    - Explore various network scanning techniques using Hping3
3. Perform OS discovery
    - Identify the target system's OS with Time-to-Live (TTL) and TCP window sizes using Wireshark
    - Perform OS discovery using Nmap Script Engine (NSE)
    - ~~Perform OS discovery using Unicornscan~~
4. Scan beyond IDS and Firewall
    - Scan beyond IDS/firewall using various evasion techniques
    - ~~Create custom packets using Colasoft Packet Builder to scan beyond IDS/firewall~~
    - Create custom UDP and TCP packets using Hping3 to scan beyond IDS/firewall
    - Create custom packets using Nmap to scan beyond IDS/firewall
5. Draw network diagrams
    - Draw network diagrams using Network Topology Mapper
6. Perform network scanning using various scanning tools
    - Scan a target network using Metasploit