03-Scanning Networks

PLEASE use prebuilt labs

Victim Data: direct interaction Need 2-6 computers online

Scope & Contract:
AWS lab setup give you 2 Victims
You may not publish the results ever.
You may only transmit the results to the POC using PDF password encrypted files.
IN SCOPE 10.0.0.21 &10.0.0.4 these are your AWS servers
OUT OF SCOPE expsec.us webserver or mail server
You will use only a browser and the scope given in class
Collect data from external sources
Document using your copy (check https://github.com/deanbushmiller/CEH-bootcamp/wiki/4-day-Series#02 for current update)
Generate a password list + a user list = make txt files, install seclist into kali
Brute force using Instructor password list against 2 AWS host for each service in enumeration
Capture new account logins and test standard interfaces

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.

Advanced: capture encrypted packets, using decryption process from capture discussion

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

Lab Tasks

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

*Indicates capture