04-Enumeration

PLEASE use prebuilt labs

Victim Data: direct interaction Need 2-6 computers online that have the services running and vulnerable

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

extract information about the target organization:

- Machine names, their OSes, services, and ports
- Network resources
- Usernames and user groups
- Lists of shares on individual hosts on the network
- Policies and passwords
- Routing tables
- Audit and service settings
- SNMP and FQDN details

Overview of Enumeration

Enumeration creates an active connection with the system and performs directed queries to list information about the target.

Lab Tasks

Ethical hackers or penetration testers use several tools and techniques to enumerate the target network. Recommended labs that will assist you in learning various enumeration techniques include:

1. Perform NetBIOS enumeration

    - Perform NetBIOS enumeration using Windows command-line utilities
    - ~~Perform NetBIOS enumeration using~~ NetBIOS Enumerator
    - Perform NetBIOS enumeration using an NSE Script*

2. Perform SNMP enumeration
    - Perform SNMP enumeration using snmp-check*
    - ~~Perform SNMP enumeration using SoftPerfect Network Scanner~~
3. Perform LDAP enumeration
    - Perform LDAP enumeration using Active Directory Explorer (AD Explorer)
4. Perform NFS enumeration
    - Perform NFS enumeration using RPCScan and SuperEnum
5. Perform DNS enumeration
    - Perform DNS enumeration using zone transfer
    - Perform DNS enumeration using DNSSEC zone walking
6. Perform RPC, SMB, and FTP enumeration
    - Perform RPC and SMB enumeration using NetScanTools Pro
    - Perform RPC, SMB, and FTP enumeration using Nmap*
7. Perform enumeration using various enumeration tools
    - ~~Enumerate information using Global Network Inventory~~
    - ~~Enumerate network resources using Advanced IP Scanner~~
    - Enumerate information from Windows and Samba host using Enum4linux

*Indicates capture