MODULE - 3
Enumeration

Enumeration :
- This Technique is usually conducted internaly
- Require an active connection
- Attacker then directly queries the target
  - Look for remote IPC$ share
  - Look for services tha offer up data
  - Create a NULL Scan
- Looking at a target expose :
  - Usernames
  - Groups
  - Machines names
  - Network Resources
  - Service Running
  - Routing Tables
  - Auditing Services
  - Applications
  - DNS & SNMP info

Techiques of Enumeration :

What are Possible Weakness :
1. Email/Business cards
2. Windows Groups
3. DNS Zone Transfers
4. Brute Force Active Directory
5. Default Passwords
6. SNMP

Know you ports and services :
1. DNS Zone Transfers [**TCP 53**]
2. SMTP [**TCP 25**]
3. Microsoft RPC Endpoint [**TCP 135**]
4. Global Catalog Service [**TCP 3268**]
5. NetBIOS Naming Service [**TCP/UDP 137**]
6. LDAP [**TCP/UDP 389**]
7. SMB over NetBIOS [**TCP 139**]
8. SNMP [**UDP 161**]
9. SMB Over TCP [**TCP 445**]
10. Network File System [**TCP 2049**]
11. SMTP [**TCP 25**]
12. SNMP Trap [**TCP/UDP 162**]
13. SSH [TCP 22]
14. Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key exchange (IKE) [**UDP 500**]
15. FTP [TCP 20/21] :
    FTP is controlled on port 21
    FTP Data Transmission Port 20
16. Telnet [**TCP 23**]
17. Trivial File Transfer Protocol [**UDP 69**]
18. Border Gateway Protocol [**TCP 179**]

#1. Enumerating via Defaults & NetBIOS :

What is NetBIOS ??
- Network Basic input / output system
- A program that allows the application on different systems to talk to each other on the LAN
- used by “clients for Microsoft network”
- Included in most operating system
- NetBIOS name resolution doesn't work on IPv6

Command ;

`nbtstat -a` list the remote machine's name table given its **name**
`nbtstat -A` - list the remote machine's name table given its **IP address**
`nbtstat -n` gives local table
`nbtstat -c` gives cache information / content

- IPC$: Interprocess communication
- Using winfo
  - Winfo [ip address] -n -v

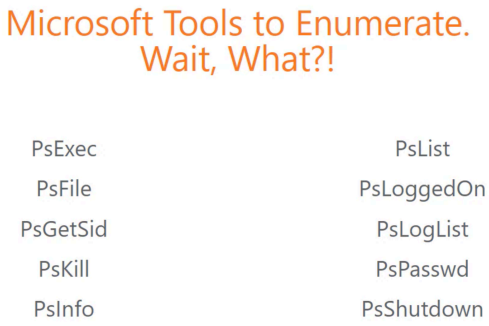
Code	Type	Meaning
<1B>	UNIQUE	Domain master browser
<1C>	UNIQUE	Domain controller
<1D>	GROUP	Master browser for subnet
<00>	UNIQUE	Hostname
<00>	GROUP	Domain name
<03>	UNIQUE	Service running on system
<20>	UNIQUE	Server service running

 # Pulling SID's and User Account :

Tools :
1. **user2sid**
2. **sid2user**

Administrator sid ends with 500

 # Microsoft tools to enumerate :



 # NetBIOS Enumeration Tools :
1. **NetBIOS Enumerator**
2. **Nmap**
3. Global Network Inventory
4. Advanced IP Scanner
5. **Hyena**
6. Nsauditor Network Security Auditor
7. **Superscan**

#2 Enumerating SNMP :

SNMP enumeration is the process of enumerating the users accounts and devices on a SNMP enabled computer.

Allow us to manage different devices,

 # Security of SNMP :

Depends on the version
1. Version 1 : Simple / basic
2. Version 2 : Same as V1 but Enhancement

Both uses community Strings
public - public
private - private

Version 3 :
i) Restrict User Access
ii) Data Encryption in transit
iii) more complex to configure

 # MIB's : Management Information Base :

MIB is a database that contain official explaination of all the network objects

 # OID's : Object identifier :

OID's Include the type of object,counter, string or address, access levels

 # MIB Hierarchical :

Each managed object in a MIB is addressed via OID's

Used by SNMP to convert OID number into plain human language

 # Tools :

 # command Line tool :

1. snmp-check
2. metasploit Module : snmp_enum
3. snmpwalk

 # GUI :

1. SNMPScanner
2. Softperfect Network Scanner
3. Network Performance Monitor
4. OpUtils
5. Engineer's Toolkit

#2 Enumerating LDAP :

Q. What is LDAP ??

Runs on TCP ports 389 and 636 (over SSL)
Connects on 389 to a Directory System Agent (DSA)
Returns information such as valid user names, domain information, addresses, telephone numbers, system data, organization structure and other items

1. DSA Ports : Directory Service Attendent : Client uses it to start a session an LDAP Session by connecting it to LDAP Server.

Global Catalog : It is simply a smaller or a stripped down version of the full database

Q. What can we learn from LDAP ??

Group Names
Username
Account Information

 # Tools :

1. Softerra
2. JXplorer
3. Lex
4. LDAP admin tool
5. Hyena

 # Enumerating SMTP :

- The Protocol used for emails
- Uses "MX" records via DNS
- Uses MTA for routing : Mail Transfer Agents
- POP, IMAP , MAPI to delivery mail internally
- 25, 587 (Submission)

 # Enumerating DNS :

- Record Lookup
- Cache Snooping
- Google Loop
- Reverse Lookup
- Zone Walking
- Zone Transfers

Port : UDP (53) : Lookup
Port : TCP (53) : Zone Transfers

 # Records :

1. A Records : Maps to IPv4 Address
2. AAAA Records : Maps to IPv6 Address
3. Cname : alias for A records
4. MX : Mail Exchange
5. NS : Name Server : DNS Servers
6. SOA : Start of Authority : Primary DNS Server
7. PTR : Reverse Lookup : IP -> Name
8. SRV : Service Records : What Service are running on a machine
9. SPF : This Record tells which server actually sends emails

 # Tools :

1. Nslookup
2. DNSRecon
    1. dnsrecon -d **hackthissite.org**
    2. dnsrecon -r **hackthissite.org** : reverse Domain lookup
    3. dnsrecon -t snoop -n **hackthissite.org** : cache snooping
    4. dnsrecon -d **hackthissite.org** -t zonewalk : Zone Walking

 # IPSec Enumeration :

- Most of the Ipsec based VPNs uses ISAKMP (Internet Security Association key management Protocol)
- It is a Part of IKE (Internet Key Exchange)
- UDP Port 500
- Nmap -p 500 -sU <target_ip_address>
- Ike-scan -M <target_ip_address>

 # VOIP Enumeration :

- SIP : Session Initiation Protocol -> Used by VOIP
- UDP/TCP : 2000,2001,5050,5061

Tools :

1. SIPVicious
2. Svmap

 # RPC Enumeration :

It Is technology basically used to create a distributed client server client/server program, Allows the client and server to communicate via these programs.

nmap -sR <target_ip_address>
nmap -sR 192.168.0.1-254

 # Countermeasures for Enumeration :

1. Defaults & NetBIOS :

- Change the Default User name and passwords
- change the default Port numbers
- Turn off SMB (Server Message Block)

2. SNMP :

- If not needed turn if off
- use version 3
- Group Policy “additional Restriction for anonymous connections”
- Block port 161 on TCP/UDP
- IPsec Filtering : Encrypt the data going back and forth between the agent and the server
- Limited access to the null session

3. LDAP :

- Separate email address and logon names
- LDAP traffic is not encrypted so use SSL to encrypt the traffic
- Encrypt the drivers that stores LDAP Databases

4. NTP :

- Watch your ports (Default Port is : 123)

- Understand what software is installed
- check your master NTP

5. SMTP (Simple Mail Transfer Protocol) :

- Disable Open Relay
- Drop Unknown Recepients
- Never include email Server info in your mail Header and Posts

6. DNS (Domain Name System) :

- Configure DNS Zone transfer to a specific or explicit server
- Ensure that nonpublic hostnames are not referenced to IP within the DNS Zone Files or publicly accessible DNS Server.
- Check Both External and Internal DNS Server.
- Ensure that HINFO and other records do not appear in DNS Zone Files.