**Module 04 : Enumeration**

**Concept**

* Enumeration: An attacker **creates avtive connections** with a target system and perform **directed queries** to gain more info about the target
* Identify points for a system attack and perform password attacks to…
* Conducted in an **intranet environment**
* Enumerated information:
  + Network resources
  + Network shares
  + Routing tables
  + Audit and service settings
  + SNMP and FQDN (Fully Qualified Domain) details
  + Machine names
  + Users and groups
  + Applications and banners
* Techniques:
  + Extract usernames using **email IDS**
  + Extract info using **default passwords**
  + Brute force **AD**
  + Extract info using **DNS Zone Transfer**
    - Replicate DNS datra across several DNS servers or back up DNS files
    - using **nslookup** and **dig** commands
  + Extract **user groups** from Windows
  + Extract usernames using **SNMP**

**Services and Ports to Enumerate**

* TCP/UDP 53: DNS Zone Transfer
* TCP/UDP 135: MS RPC Endpoint Mapper
* UDP 137: NBNS (NetBIOS Name Service)
* TCP 139: NetBIOS Session Service (SMB over NetBIOS)
* TCP 445: SMB over TCP (Direct Host)
* UDP 161: SNMP
* TCP/UDP 390: LDAP
* TCP 2049: NFS (Network File System)
* TCP 25: SMTP
* TCP/UDP 162: SNMP Trap
* UDP 500: ISAKMP (Internet Security Association and Key Management Protocol) /IKE (Internet Key Exchange)
* TCP 22: SSH
* TCP 23: Telnet
* TCP 20/21: FTP
* TCP/UDP 5060,5061: SIP (Session Initation Protocol)
* TCP/UDP 3268: Global Catalog Service
* UDP 69: TFTP (Tricial File Transfer Protocol)
* TCP 179: BGP (Border Gateway Protocol)

**NetBIOS Enumeration**

* A NetBIOS name is a unique 16 ASCII char string used to identify the network devices over TCP/IP
* Attackers use it to obtain the **list of computers belongs to a domain**, the **list of shares on the individual hosts in the network**, **policies and passwords**
* command: **nbtstat -a <target>**  -> obtain the NetBIOS name table of a remote computer
* command: **nbtstat -c** -> obtain the contents of the NetBIOS name cache, table of NetBIOS names, and their resolved IP address
* Tools:
  + **NetBIOS Enumerator:** Help to enumerate details such as NetBIOS names, usernames, domain names, Mac address…
  + **Nmap:** **nbstat NSE script** allow attackers to retrieve target’s NetBIOS names and MAC address
  + NMAP**: nmap -sV-v –script nbstat.nse <target>**

**Enumerating User Accounts**

* Use **PsTools** suite helps to control and manage remote systems from the command line

**Enumerating Shared Resources Using Net View**

* It is used to obtain a list of all the **shared resources of a remote host or workgroup**
* command: **net view \\<computername>** **net view /domain: <domain name>**

**SNMP Enumeration**

* The process of enumerating user accounts and devices on a target system using SNMP
* Agents are embedded on each network device, manager is on a separate computer
* SNMP holds **two passwords**. **Read community string**, it is public by default and allows for the veiwing of the device configuration. **Read/Write community string**: It is private by default and allows remote editing of configuration
* Attacker extract info about **network resources** (hosts, routers, devices, shares), **network info** (ARP tables, routing tables, traffic)

**Management Info Base (MIB)**

* A virtual database containing **a formal description of all the network objects** that can be managed using SNMP
* It is hierarchical, each managed object in a MIB is addressed through **OIDs (Object Identifiers)**

**SNMP Enumeration Tools**

* **Snmpcheck:** Allow one to enumerate the SNMP devices and place the output…
* **SoftPerfectNetworkScanner:** Discover shared folders and retrieve practically any info about the network device via WMI (Windows Management Instrumentation), SNMP, HTTP, and PowerShell

**LDAP Enumeration**

* **An internet protocol** for accessing distributed directory services
* A client starts a LDAP session by connecting to a **directory system agent (DSA)** on **TCP 389** and then sends an operation request to the DSA
* Transmitted info using **BER (Basic Encoding Rules)**
* Attacker query the LDAP service to gather info, such as **valid usernames, addresses, and departmental details**
* Tools: Softerra LDAP Administrator, LDAP Admin Tool…

**NTP and NFS Enumeration**

* NTP is designed to **synchronize the clocks** of networked computer, using **UDP 123**
* Attackers query the NTP server to obtain info such as list of connected hosts, clients IP address in a network, their system name, and OS
* Internal IPs can be obtained if the NTP server is in the DMZ
* NTP Enumeration Commands:
  + **ntptrace:** Trace a chain of NTP server back to the primary source
  + **ntpdc:** Monitors operation of the NTP daemon, ntpd
  + **ntpd:** Monitor NTP daemon (ntpd) operations and determines performance
  + **ntpdate:** Collect the number of time samples from several time sources
* NTP Enumeration Tools: PRTG Network Monitor, NMAP, Wireshark, NTP Server Scanner
* NFS enumeration enables attackers to identify the **exported directories, list of clients and their IP address, and the shared data**.
* command: **showmount -e <Target Address>** -> view the list of shared files and dirs
* command: **rpcinfo -p <Target Address> ->** scan the target address for an open NFS port and the NFS services running on it
* NFS Enumeration Tools: RPCScan, SuperEnum

**SMTP Enumeration**

* Provide **3 built-in-commands**:
  + **VRFY**: Validate users
  + **EXPN**: Show the actual delivery addresses of ailiases and mailling lists
  + **RCPT TP**: Define the recipients of a message
* Attackers can directly interact with SMTP via the **telnet** prompt and collect **a list of valid users** on the SMTP server
* Tools: NetScan Tools Pro, smtp-user-enum

**DNS Enumeration Using Zone Transfer**

* If the target DNS serverr allow zone transfer, attackers can use this technique to obtain **DNS server names, hostnames, machine names, usernames, IP address, aliases,** etc…
* Tools: **nslookup, dig, and DNSRecon**
* dig command: **dig ns <target domain>**
* nslookup command: **nslookup set querytype=soa (Start of Authority) <target domain>**
* DNSRecon command: **dnsrecon -t axfr -d <target domain>**
* DNS Cache Snooping: A DNS enumeration technique whereby an attacker queries the DNS server for a specific cached DNS record.
* **Non-recursive Method** and **Recursive Method**
* **DNSSEC Zone Walking: A DNS enumeration technique** where an attacker attempts to obtain internal records of the DNS server if the DNS zone is not properly configured.
* **LDNS** and **DNSRecon,** to exploiot this vulnerability and obtain the network info

**IPSec Enumeration**

* IPSec uses **ESP (Encapsulation Security Payload), AH (Authentication Header), and IKE (Internet Key Exchange)** to secure communication between VPN end points
* NMAP: **nmap -sU -p 500 <target address>** ->perform an Nmap scan for checking the status of ISAKMP over port 500
* **ike-scan -M <target gateway address>**

**VoIP Enumeration**

* VoIP uses **SIP (Session Initation Protocol)** to enable voice and..
* UDP/TCP ports 2000, 2001, 5000, 5061
* Provide sensitive info such as **VoIP gateway/servers, IP-PBX system, client software, user extensions, IP…**
* This info can be sued to launch VoIP attacks such as **DoS, Session Hijacking, Caller ID spoofing, Evaesdropping, SPIT (Spamming over the Internet Telephone), and VoIP phishing (Vishing)**
* Tool command: **svmap <target network range>**

**RPC Enumeration**

* Allow clients and servers to communicate in distributed client/server programs
* Enumerating RPC endpoints enables attackers to identify any vulnerable services on these service ports.
* NMAP: **nmap -sR <Target address>** / **nmap -T4 -A <Target address>**

**Unix/Linux User Enumeration**

* **rusers:** Display a list of users who are logged on to remote machines or local network machines
* **rwho:** Display a list of users who are logged on to hosts on the local network
* **finger:** Display info about system users, such as login name, real name, terminal name, idle time…

**Telnet and SMB Enumeration**

* Attackers can access shared info, including the hardware and software info of the target it the Telnet port is found open
* Enable attackers to **exploit identifid vulnerabilities** and perform **brute-force attacks** to gain unauthorized…
* Attacks use SMB enumeration tools, such as **Nmap, SMBMap, enum4linux**, and nullinux, to perform a directed scan on the SMB service running on port 445
* Help attacks to perform **OS banner grabbing** on the garget

**FTP and TFTP Enumeration**

* FTP transfers data in plain text
* Attacker use Nmap to scan and enumerate open port 21
* Attackers perform TFTP enumeration using **PortQry** and **Nmap**, to extract info such as running TFTP services and files stored on the remote server

**BGP Enumeration**

* Using Nmap and BGP Toolkit to discover the IPv4 prefixes announced by the **AS (Autonomous System)** number and routing path followed by the target

**Enumeration Countermeasures**

* **SNMP**
  + Remove the SNMP agent or turn off the SNMP service
  + Change the default community string names
  + Upgrade to SNMP3, which encrypts passwords and meesages
* **DNS**
  + Disable the DNS zone transfer to the untrusted hosts
  + Use premium DNS registration servies
  + Use standard network admin contacts for DNS registrations
  + Ensure the private hosts and their IP are not published in DNS zone files of public DNS servers
* **SMTP**
  + Ignore email messages to unknown recipents
  + Exclude sensitive mail server and local host info in mail responses
  + Disable open relay feature
  + Limit the number of accepted connections from a source to prevent brute-force attacks
* **LDAP**
  + Use SSL or STARTTLS technology to encrypt the traffic
  + Select a username different from your email address and enable account lockout
  + Use NTLM or any basic authentication mechanism to limit access to legitimate users only
* **SMB**
  + Disable SMB procotol on Web and DNS servers
  + Disable SMB protocol on Internet facing servers
  + Disable ports TCP 139 and TCP 445
  + Restrict anomymous access
* **NFS**
  + Implement proper permissions on exported files systems
  + Implement firewall rules to block NFS port 2049
  + Proper configuration of files
  + Log requests to access system files on the NFS server
* **FTP**
  + Implement secure FTP (SFTP, which uses SSH) or FTP secure (FTPS, which use SSL)
  + Strong password or a certification-based authentication policy
  + Ensure that unrestricted uploading of files on the FTP server is not allowed
  + Disabled anomyous FTP accounts
  + Restrict access by IP or domain name to the FTP server