"db_import" → to import external results into the database

"hosts" → command to list all the hosts in the database

"services" → command to show all available open port and services on the identified hosts.

4a lezione 02-03-2021

ENUMERATION 3° CAPITOLO

↳ involves active connections to systems and directed queries.

INFO: - user name account;
- opt - misconfigured shared resource;
- older version of software with known security vulnerabilities.

- Service fingerprinting: is more thorough and provides more valuable info than scanning, but it's also more time consuming and noticeable because it generates considerably more traffic.

Nmap:

Nmap lists service names along with ports, this info is obtained from a file named nmap-services.

-sV Option: switch goes a step further and interrogates the ports, soliciting feedback and matching what it receives with known protocols and specific protocol version info using a different file called: nmap-service-probe (info about services responses).

amap:

Uses its own network service pattern-matching techniques to fingerprint network services, and Nmap's functionality is typically more accurate and up-to-date. (NMAP > AMAP).

Vulnerability Scanners:

Employing the battering-ram approach of directing an automated vulnerability scanner against a target or entire network can be an effective and time efficient means of gathering vulnerability info.

PRODOTTI A PAGAMENTO: McAfree, nCircle, Qualys, Tenable

PRODOTTI Open Source: OpenVAS

Nessus:

Nessus, by Tendle Network Security. It's easy to use graphical interface, frequently updated database of vulnerabilities, support for all major platforms and optimized performance make it well suited for a good scaning a target or network of targets in short order.

Users can develop plugins using NASL (NESSUS - ATTACK - SCRIPTING LANGUAGE) to expand capabilities.

has a web interface

COUNTERMEASURES:

You should implement effective patch and configuration management processes to try to prevent such vulnerabilities from being introduced in the first place. Use IDS and IPS.

Nmap NSE Scripting: is an interface that allows users to extend Nmap's capabilities through scripts written in the LUA interpreted programming language to send, receive and report on arbitrary data. Nmap comes bundled with a library of useful NSE scripts capable of performing activities such as network discovery, version detection, backdoor detection, and even exploitation of vulnerabilities.

-Basic Banner Grabbing: can be simply defined as connecting to remote services and observing the output, as it can be surprisingly informative to remote attackers. They may identify the make and model of the running service, which in many cases is enough to set the vulnerability research process in motion.

Telnet and netcat → for a slightly more surgical probing tool rely on netcat, the "TCP/IP Swiss Army knife"

↳ use telnet to grab banners is as easy as opening a telnet connection to known port on the target server, pressing ENTER a few times and seeing what comes back.

nc -v www.example.com 80

The best defense against banner grabbing is to shut down unnecessary services, restrict access to services using network access control.

-ENUMERATING FTP (TCP/21)

Many such sites are configured for anonymous access.

We can use anonymous and a spurious email address to authenticate to this anonymous service:

ftp ftp.example.com

GRAPHICAL FTP clients → FileZilla

COUNTERMEASURES:

Should just turned off. Use secure FTP (SFTP) ssh encryption or FTP SECURE (FTPS, with SSL) protected by strong PSW or CA.

-ENUMERATING TELNET (TCP/23)

REMOTE ACCESS → transmit data in cleartext.

Telnet often display a system banner prior to login. This banner

contains the host OS and version (system enumeration).
Many times the system displays a unique prompt from which you can easily deduce what type of device it is through prior knowledge or a google search.
EXAMPLE:
Telnet. If valid username + invalid password → "CPE 1107 Password not correct for user profile"

Else, system respond with "CPE 1120 → User don't exit".

COUNTERMEASURES:
SSH is a widely deployed alternative that should be used as a replacement in all possible cases. In situation where telnet must be used, mitigation controls to restrict the access.

-Enumerative SMTP (TCP/25)
SMT provides two built-commands that allow for the enumeration of the users:

- vrfy <mail>
  - confirm names of valid users.
- expn <mail>
  - reveals the actual delivery addresses of aliases and mailing list.

A tool called vrfy.pl can speed up this process.

COUNTERMEASURES:
Should just be turned off. Popular SMT server can disable these commands through the file mail.cf (SMTP version ≥ 8). If they don't, consider switching vendors.

-Enumerating DNS (TCP/UDP 53):

match host IP add
with human friendly names.

→ UDP/53 (normally)

→ TCP/53 transfert zone.

Dump the entire contents
of a given domains zone files,
enumerating info like hostname-
to-IP address mappings and
HINFO data.

nslookup
ls -d <domain_name>

-Bind Enumeration: Bind comes with a record within the "CHAOS" class wich contains the version of the BIND installation. To request this record:

dig @192.168.56.101 version.bind txt chaos

-DNS Cache Snooping: Attacker can abuse of this functionality by requesting the DNS server to query only it's cache and, by doing so, deduce if the DNS server's client have or not visited a particular site:

dig @192.168.56.101 www.foodstore.com A +norecurse

-Automated DNS enumeration: dnsenum (tool) does a variety of different task such as Google Scraping, brute forcing subdomains performing reverse lookups, performing WHOIS queries on the ranges identified and so on. The tool can be run on a domain name.

-Fierce.pl (Perl script)

COUNTERMEASURES:

Restrict zone transfers to authorized machine. Blocking bind version.bind request. Disabling DNS cache snooping.

-ENUMERATING TFTP (TCP/UDP 69):

Unauthenticated file transfer commonly run on UDP port 69. You have to know the file name in order to pull it from the server.

tftp <ip>

Exit from connection: quit

Enumeration tricks is getting the /etc/passwd file (password grabbing) and copy it in a tmp file:

get /etc/passwd /tmp/passwd.crackeater

Contain the encrypted password hashes for each users.

Accessing Router/Switch configuration via TFTP:

Attackers can leverage the possibility to configure router device through configuration file in order to obtain the device's configuration.

- names of configuration files: running-config
  startup-config
  config
  .config
  r.n

COUNTERMEASURES:

Don't run TFTP and if you do, wrap it to restrict access and make sure it's blocked at the border firewall.

-ENUMERATING FINGER (TCP/UDP 79) (info about users)

Assume that a valid host (username) running the finger services has been identified in previous scans. To obtain info about that user: (social engineering attack)

finger -l @target.example.com

COUNTERMEASURES:

Don't run finger and block port 879 at the firewall.

Use TCP wrappers to restrict and log host access.

-Enumerating HTTP (TCP 80):

Basic banner grabbing with a connection to a web server on the HTTP port using netcat.

```
nc -v www.example.com 80
```

-Banner grabbing with SSL: If you encounter a website that uses SSL you can negotiate SSL connections.

```
openssl <s_client> -quiet -connect www.pippo.com:443
```

-quiet: to limit the output.

COUNTERMEASURES:

Change the banner on your web servers.

-Enumerating Microsoft RPC Endpoint Mapper (MSRPC, TCP/135)

Endpoint Mapper: Run on the port TCP/135.

Querying this service can yield info about applications & services available.

```
epdump mail.example.com
```

FOR LINUX we have rpcdump.py in order to permits queries over different ports/protocols besides TCP/135.

COUNTERMEASURES:

Restric access to TCP port 135.

Require users to establish a VPN connection between their system and the internal network. You can restrict access to your RPC applications.

-Enumerating NetBios Name Service (NBNS, UDP 137)

Distributed naming system for Microsoft Windows-based networks. Replaced by the standard DNS. However, is still enabled by default in all Windows distributions.

Enumerate windows workgroups and domains:

The "net view" command is a great example of a built-in enumeration tool.

Example to enumerate the domains:

```
net view /domain
```

Example to enumerate computers in a particular domain

```
net view /domain:corleone
```

5) -Enumerate windows domain controllers: Tool "nltest" to identify the domain controllers in the domain we just enumerated using "net view".

```
nltest /dclist:corleone
```

-Enumerate network services:

We often use "net view" to probe for the Remote Access Service (RAS) to get an idea of the number of dial-in servers that exist in the network EXAMPLE:

```
netview -D CORLEONE -T DIALIN dialin_server
```

-T: Specify the type of machine/service to look for.

Dumping the netBios name table:

-"nbtstat" connects to discrete machines rather than enumerating. It calls up the NetBios name table from a remote system:

```
Nbtstat -A 192.168.56.101
```

We can specify an entire network like 192.168.56.0/24.

Extract the system name, the domain it's in, any logged-on users, any services running and network interface hardware media Access Control.

-Linux NetBios:

Tool: NMBscan that provides the ability to enumerate NetBios by specify different levels of verbosity. Specify the -a option to obtain a complete view of the NetBios network around us.

COUNTERMEASURES:

Restrict the access to UDP 137, blocking the protocol or ACL. To prevent user data from appearing in NetBios name table dumps, disable the Alerter and Messenger services on individual hosts (service control panel on Windows 2000 and later)

5ª Sessione 03/03/2021

-NetBios Session Enumeration, TCP/139 & TCP/445

Windows null session/anonimous connection attack. If you've ever accessed a file or printed to a printer, chances are good that you've used Microsoft Server Message Block (SMB) protocole. SMB is accessible via API even to unauthenticated users (biggest Achilles' heels for Windows). In computer networking, SMB is mainly used for providing shared access to files, printers, and serial ports and miscellaneous communication among nodes on a network. First step in Enumerating SMB is to connect to the service using the null session command:

```
net use
\\192.168.56.101\IPC$ "" /u:""
```

connect to interprocess communication share (IPC$) at ip address

192.168.56.101 as the target-ip anonymous user (/u:"") with a null ("") psw. Open a channel to get info as users, groups, registry keys and so on. The IPC$ share is also known as a null session connection.

-Enumerate file shares:
We can enumerate the names of the file shares using a number of techniques:
net view \\ip
Best tool: DumpSec

-Registry enumeration:
Dumping the contents of the windows registry from the target. Fortunately, Windows default configuration is to allow only administrators access to registry. If you want to check whether a remote registry is locked down, the best tool is "reg".
reg query
\\192.168.56.101\HKLM\SOFTWARE\MICROSOFT\Windows\CurrentVersion\Run

-Enumerate trusted domains: Once a null session is set up to one of the machines, the nltest tool can be used to learn about further Windows domains:
nltest /server:<server_name>
nltest /trusted_domains <server_name>

-Enumerate users: DumpSec=Best tool.
It can be pull a list of users, groups and the NT systems policies and users rights.
dumpsec /computer=\\192.168.56.101 /rpt=usersonly /saveas=tsv /outfile=c:\temp\users.txt
c:\temp\users.txt is the file of output.

The other two extremely powerful windows enumeration tools are sid2user and user2sid (SID = security identifier)

↓
a variable length numeric value issued to an NT family system at installation.

user2sid // 192.168.56.101 "domain users"

or

sid2users // 192.168.56.101 21 8915387 16458 22062 8198288005 500

-All-In-One null session tools:

Top tool: Winfingerprint.

↳ win for dee overde functionality, as it has nearly everything you could hope for in a Windows enumeration tool. It can target a single host, list or ranges of host or just all visible host on a segment. It's also capable of enumerating Windows system via Active Directory.

ANOTHER TOOL: NBTENUM (command "enum").

Portcullis security has developed a linux clone of enum named "enum4linux" which is a wrapper for common commands available within the Samba (SMB) suite.

-Miscellaneous null session tools:

Using a null session, "getmac" displays the MAC addresses and device names of network interface cards on remote machine. Can yield useful network info to an attacker dealing a system with multiple network interfaces

COUNTERMEASURES:

Filter TCP/UDP port 139/445 at the permeter network access devices. You could also disable SMB services on individual NT hosts by unbinding WINS client from the appropriate interface. Following NT4, Microsoft provided a facility to prevent enumeration of sensitive info over a null session. Ensure the registry is locked down and is not accessible remotely.

Beating RestrictAnonymous=1: Can be bypassed. NBTENum and the UserInfo tool enumerate user info over a null session even if RestrictAnonymous is set to 1.

Setting RestrictAnonymous=2 prevents even users from even connecting to the ipc$ share. This setting has the deleterious effect of preventing down-level client access and trusted domain enumeration.

-Enumerating SNMP (UDP 161)
é um protocolo

is designed to provide intimate info about network devices, software and systems. Dowered it the colloquial name "Security Not My Problem". EXAMPLE: the commonly implemented psw for accessing an SNMP agent in read-only mode is "public".

Enumerating Windows users via SNMP is a cakewalk using the RK snmputil. You need to specify the Object Identifier (OID) in the snmputil.

UNIX/LINUX → tool snmpget within the net-snmp suite to query SNMP.

·Scanners: Query SNMP is a simple task that makes it an ideal service for automated scanning. An easy-to-use Windows-based tool that performs this well is FoundStone's SNScan. For each host

successfully queried and the results can be exported to CSV.
UNIX → "onesixtyone".

COUNTERMEASURES:
Remove/Disable SNMP agents on individual machines.
If you're using SNMP to manage your network, block access to TCP/UDP port 161 (SNMP get/set) at the perimeter net work access device.
Windows NT family systems: you can edit the Registry to permit only approved access devices to the SNMP community name and to prevent Microsoft MIB info from being sent.

-Enumerating BGP (TCP/179)
By looking at BGP routing tables, you can determine the network associated with a particular corporation to add to your target host matrix. Steps to perform enumeration:
- Determine the ASN (autonomous system number) of the target organization.
-Execute a query on the routers to identify the networks where the AS Path terminates with the organization's ASN.

Enumeration from Internet: 1) Determine the ASN for an organization:
- If you have the company name, is to perform WHOIS search on ARIN with the ASN keyword.
- If you have an IP addr for the company, you can query a router and use the last entry in the AS Path as the ASN.

Then, to query the router using the last ASN to determine the network addresses associated with the ASN, do the following:
show ip bgp regexp _16394$. COUNTERMEASURES: No exist a

good countermeasures for BGP enumeration. For packets to be routed to your network, BGP must be used.

-Enumerating Windows LDAP (TCP/UDP ports 389/3268)

AD is designed to contain a unified, logical representation of all the objects relevant to the corporate technology infrastructure. An attacker can point ldp.exe against a Windows 2000 or later host and all of the existing users and groups can be enumerated with a simple LDAP query. You need to create an authenticated session with LDAP.

COUNTERMEASURES:

You should filter access to ports 389/3268 at the network border. To prevent this info from leaking out to unauthorized parties on internet semi trusted networks, permissions on AD need to be restricted.