ZROC102

Module 2 – Scanning and Enumeration

What is Enumeration?

- Enumeration is one of the of the most important methodologies in cybersecurity - especially for offensive security
- it's all about information gathering
- Not only automated scanning, but manual exploration of
  - Webpages
  - Networks
  - File Systems
- Enumeration is recursive, too!
  - You might find a new service and have to enumerate that
  - You might find some credentials and want to see what new things you can access

Why do we do it?

- To figure out the kind of system we're dealing with
  - Whether it's networked (outgoing and incoming connections, protocols)
  - What the OS is (Any known exploits? Vulnerable kernel versions?)
  - What its purpose is (web server? Domain controller?)
- To figure out a way in
  - Vulnerable software versions or exposed ports
  - Users and credentials left lying around
- To spot anything out of the ordinary
  - Interesting files and unusual processes
  - Remote connections to other services/machines

What are we looking for?

- Open ports
  - Useful services like SMB, SSH, NFS and Windows Services like LDAP & Kerberos
- Config info, users & credentials
  - Default creds for common services
  - Passwords lying around in public documents, config files & exposed databases
  - Version numbers, package info etc
- Running services and other processes
  - Machines communicating with each other
  - Processes downloading things from a server
  - Stuff running as root
  - Anything that runs periodically is a possible path to a foothold/privesc

Nmap

- Nmap is one of the first steps in a security assessment - it scans the most common ports (or a specific list of ports), checks if they are open, and tries to discover services on each of them. It comes preinstalled on Kali Linux

- A standard command to run nmap on the most common ports is: nmap -sC -sV [ip]

  - sC is use safe scripts
  - sV is enumerate versions/services
  - oA [file directory] can be used to output the data in all formats to a directory

- You can also specify ports with the -p flag (use -p- to scan all 65535 ports) and control the speed of the scan with the -Tx flag where x is the intensity from 0 to 5 (0 is highest!)

- The -O flag discovers the operating system. You can even disable host discovery with the -Pn flag, which can be useful if your packets get dropped!

- Another tip is to run an all ports scan in the background while you test (use nmap -p- [ip])

Nmap Scripting Engine (NSE)

- Used to launch user-created scripts in order to automate various scanning tasks.
- These scripts perform a broad range of functions including DNS enumeration, brute force attacks, and even vulnerability identification.
- For example, the smb-os-discovery script attempts to connect to the SMB service on a target system and determine its operating system:
    - $ nmap IP --script=smb-os-discover

HTTP Enumeration: Gobuster

- Gobuster is a tool that is used for enumerating multiple services, most notably HTTP/S services. However it also supports DNS and vhost enumeration.

- After an nmap scan it's always worth having some form of enumeration running in the background while you actively search for other exploitation paths. An example of this would be to run gobuster file/directory enumeration against the server you're exploiting.

    - gobuster dir -w [file/directory wordlist] -u [http:// + ip]
        - -x can be used to specify extensions, e.g. -x php,html,txt
        - -s & -b can be used to add or remove response codes from the filter list

- Gobuster can also be used for DNS enumeration for subdomains as well as virtual host enumeration.

HTTP Enumeration: Wfuzz

- Allows injection of payloads into HTTP requests (similar to the Burp Intruder module)

- Payload positions are marked by the FUZZ word - for example:

  - wfuzz -u http://example.com/FUZZ -w wordlist/general/common.txt will replace FUZZ with all words in the specified wordlist (useful for URL discovery)
  - wfuzz -u http://example.com/login.php -d 'email=FUZZ&password=testpass' -w /path/to/email-list -p 127.0.0.1:8080:HTTP will use the -d parameter to pass data to a POST request and enumerate possible emails that we can login with - it also passes the request through a proxy, so we can see what it's doing
  - wfuzz -u http://example.com/search.php?search=FUZZ -w /path/to/search-terms -b 'PHPSESSID=123456789123456789123456789' performs a search, passing a cookie with -b

- Remember to add box URLs to your /etc/hosts folder if wfuzz is struggling to connect!

SMB Enumeration

- What is SMB?
    - SMB - Server Message Block Protocol - is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network.
- **Enum4Linux**
    - Enum4linux is a tool used to enumerate SMB shares on both Windows and Linux systems. It is basically a wrapper around the tools in the Samba package and makes it easy to quickly extract information from the target pertaining to SMB.
- Other tools: smbclient, smbmap

NFS Enumeration

- NFS stands for “Network File System” and allows a system to share directories and files with others over a network.
- By using NFS, users and programs can access files on remote systems almost as if they were local files. It does this by “mounting” all, or a portion of a file system on a server.
- Show available share:
    - $ showmount -e [IP]
- Mount share
    - First, use “mkdir /tmp/mount” to create a directory on your machine to mount the share to.
    - $mount –t nfs ip:/sharename ~/tmp/mount -nolock

FTP Enumeration

- File Transfer Protocol (FTP) is, as the name suggests , a protocol used to allow remote transfer of files over a network. It uses a client-server model to do this, and- as we'll come on to later- relays commands and data in a very efficient way.

Active	Passive
In an Active FTP connection, the client opens a port and listens. The server is required to actively connect to it.	In a Passive FTP connection, the server opens a port and listens (passively) and the client connects to it.

SMTP Enumeration

SMTP stands for “Simple Mail Transfer Protocol“.

We will be making use of msfconsole:

- Smtp_version – find system mail name
- Smtp_enum – enumerate usernames

John/Hashcat

- Both John and Hashcat are tools for password cracking. Often used once you have a foothold on a machine to allow for further exploitation.

- A hash is the output once a password has been put through a one way function. This one way function means that you can turn a password into a hash easily, however turning the hash back into the password is very time and computationally expensive.

- John typically uses CPU to crack hashes, however has support for GPU. Hashcat has full support for GPU.

Using John

- Once you know the type of hash that you want to crack, you want to find the location of a password list file. These can commonly be found in kali linux under /user/share/wordlists or /usr/share/seclists/

  - john --list=formats
  - john [hash file] --wordlist=[wordlist file] --format=[hash format]
  - john [hash file] --show --format=[hash format]

  - Eg: $ john -format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash1_1.txt

Using HashCat

- Hashcat can crack a variety of different password hash formats using the GPU.

- The following commands will help find the ID of the hash you want to crack

  - hashcat --help
  - hashcat -m [hash id] [hash file] [wordlist file]

  - $ e.g. hashcat -m 0 hash1_1.txt /usr/share/wordlists/rockyou.txt

Hydra

- Hydra is a tool for brute forcing usernames and passwords for different services. It has support for 50 different protocols.

- Unlike John, this uses a network connection in order to find the password - each username and password combination is sent to the server and used for authentication. If the combination fails then another different attempt is made.

- This means that there is a larger overhead when connecting

- Brute forcing is also very ‘loud’ - it can be easy to see the system is under attack.