October 21, 2022

Security Audit Report for

ABC Company

ATTENTION: This document contains information from Aaron Yeap Chun Keat. that is confidential and privileged. The information is intended for private use of the client. By accepting this document you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from Aaron Yeap Chun Keat. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited.

Document Details

|  |  |
| --- | --- |
| Title | Details |
|  |  |
| COMPLETED ON: | OCTOBER 21, 2022 |
|  |  |
| REPORT TYPE: | MANUAL SCAN |
|  |  |
| PREPARED BY: | AARON YEAP CHUN KEAT |
|  |  |
| CONTACT: | ckyeap9310@gmail.com |

Table of Contents

1. Executive Summary
2. Methodology/ Approach
3. Results
4. Conclusion and Suggestions
5. Appendix
6. Executive Summary

This document contains the initial security assessment report for :

{a small network containing 2 ubuntu machines}

ABC company suspects that they could be vulnerable and be potential hacking target. The purpose of this assessment was to point out security loopholes and missing best security practices. The tests were carried out assuming the identity of an attacker or a malicious user but no harm was made to the functionality or working of the network.

1.1 Scope of Testing

Security assessment includes testing for potential open ports which might be vulnerable and can be exploited for attacker to gain access and even privilege escalation, leads to full control of the machines.

1.2 Overall findings

Machine ID: 192.168.142.139

|  |  |  |  |
| --- | --- | --- | --- |
| Ports | Status | Services | Severity |
| 21 | open | Vsftpd 2.3.4 | High |
| 139 | open | Samba smbd | High |
| 1099 | open | Java RMI | High |
| 512 | open | Netkit-rsh rexecd | High |
| 2121 | open | ProFTPD 1.3.1 | High |

Total open ports: 14

Out of 14 open ports, 5 of the ports listed above are critically vulnerable as attacker might eventually gain access as root.

* Through enumeration and obtain the combination of user and weak password such as root:root under rexec-brute force using port 512.
* Exploit using known vulnerability and gain meterpreter access as root (full control of system).

Machine ID: 192.168.142.142

|  |  |  |  |
| --- | --- | --- | --- |
| Ports | Status | Services | Severity |
| 23 | open | telnet | Medium |
| 80 | open | HTTP | Medium |
| 1099 | open | Java RMI | High |
| 2121 | open | ProFTPD 1.3.1 | Medium |

Total open ports: 9

Out of 9 open ports,4 of the ports listed above are labelled as high and medium risk.

* List of users are leaked on company website through port 80. This provides attacker convenient to brute force against popular weak passwords. It can be done through port 23 telnet service. If there is matching combination, attacker will gain access to system with or without root privilege depending on user account setting. The leak users are not having root privilege, but attacker is able to perform post exploitation to eventually obtain root access through privilege escalation.
* Attacker is able to exploit on know vulnerability to gain root access using Java RMI service.

1. Methodology / Approach

In this assessment, I will be testing on some of those common open ports that are critically vulnerable and have known exploits scripts available online. I will run my own script which involves tools listed below.

Tools involved in this assessment:

* Nmap (including NSE scripts)
* Searchsploit
* Metasploit

1. Result

Machine: 192.168.142.139

Nmap result

Script command (IP refers to Machine’s IP Address)



Scan result for all open ports

|  |  |  |  |
| --- | --- | --- | --- |
| PORT | STATE | SERVICE | VERSION |
| 21/tcp | open | ftp | vsftpd 2.3.4 |
| 25/tcp | open | smtp | Postfix smtpd |
| 53/tcp | open | domain | ISC BIND 9.4.2 |
| 111/tcp | open | rpcbind | 2 (RPC #100000) |
| 139/tcp | open | netbios-ssn | Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 512/tcp | open | exec | netkit-rsh rexecd |
| 513/tcp | open | login | OpenBSD or Solaris rlogind |
| 1099/tcp | open | java-rmi | GNU Classpath grmiregistry |
| 2121/tcp | open | ftp | ProFTPD 1.3.1 |
| 3632/tcp | open | distccd | distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)) |
| 8180/tcp | open | http | Apache Tomcat/Coyote JSP engine 1.1 |
| 8787/tcp | open | drb | Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb) |
| 36516/tcp | open | java-rmi | GNU Classpath grmiregistry |
| 39173/tcp | open | nlockmgr | 1-4 (RPC #100021) |
| 53386/tcp | open | mountd | 1-3 (RPC #100005) |
| 56491/tcp | open | status | 1 (RPC #100024) |

Nmap result using brute category scripts.

Script command



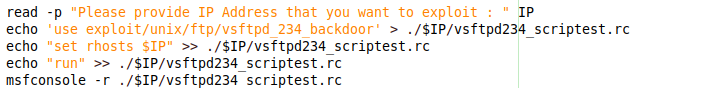
Result

|  |  |  |  |
| --- | --- | --- | --- |
| PORT | STATE | SERVICE | VERSION |
| 21/tcp | open | ftp | vsftpd 2.3.4 |
| | ftp-brute:  | Accounts:  | user:user - Valid credentials | | | |
| 111/tcp | open | rpcbind | 2 (RPC #100000) |
| | 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 51259/udp mountd  | 100005 1,2,3 54137/tcp mountd  | 100021 1,3,4 33314/udp nlockmgr  | 100021 1,3,4 47315/tcp nlockmgr  | 100024 1 47856/udp status  |\_ 100024 1 60363/tcp status | | | |
| 512/tcp | open | exec | netkit-rsh rexecd |
| rexec-brute:  | Accounts:  | root:root - Valid credentials  | netadmin:netadmin - Valid credentials  | guest:guest - Valid credentials  | user:user - Valid credentials  | web:web - Valid credentials  | sysadmin:sysadmin - Valid credentials  | administrator:administrator - Valid credentials  | webadmin:webadmin - Valid credentials  | admin:admin - Valid credentials  | test:test - Valid credentials | | | |
| 2121/tcp | open | ftp | ProFTPD 1.3.1 |
| | ftp-brute:  | Accounts:  | user:user - Valid credentials | | | |
| 8180/tcp | open | http | Apache Tomcat/Coyote JSP engine 1.1 |
| |\_http-server-header: Apache-Coyote/1.1  | http-brute:  |\_ Path "/" does not require authentication | | | |
| Host script results:  | smb-brute:  | msfadmin:msfadmin => Valid credentials  |\_ user:user => Valid credentials | | | |

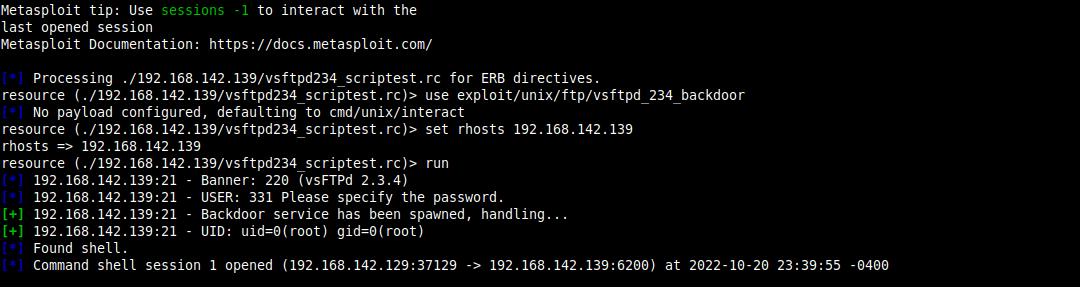
Successful Exploit

1. Using msfconsole via port 21 - vsftpd

Script command



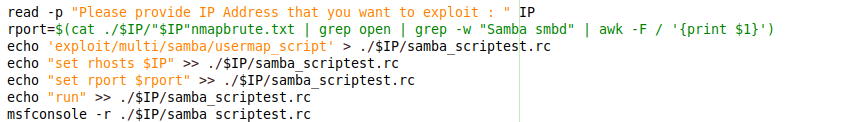
Result



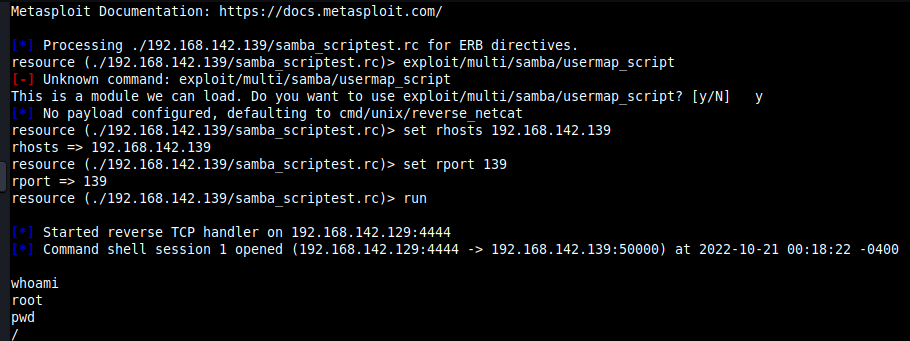
The access granted: root

1. Using msfconsole via port 139 - Samba smbd

Script command



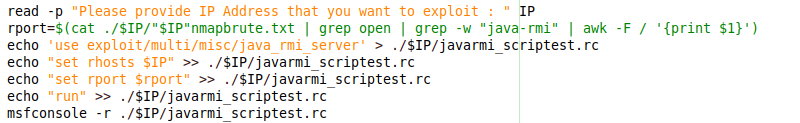
Result



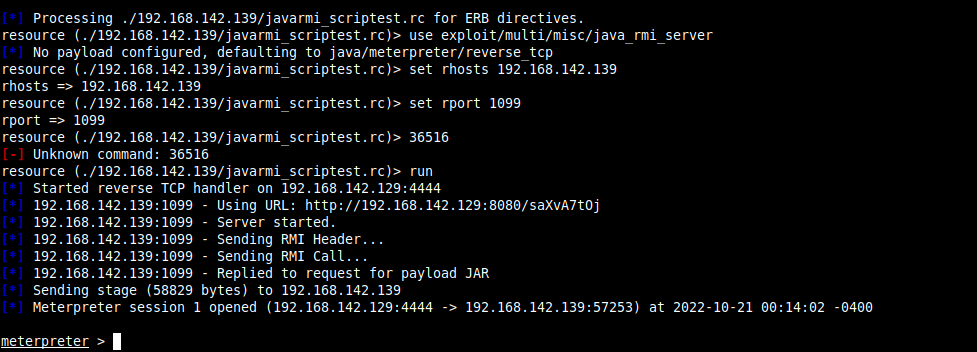
The access granted: root

1. Using msfconsole via port 1099 or 36516 - Java RMI

Script



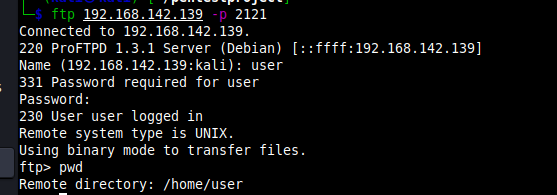
Result



The access granted: root

1. Login using credential of ‘user’ for user and password via port 2121 - Proftpd or 21 – ftp

Result



Access granted: user

Machine: 192.168.142.142

Nmap result

Scan result for all open ports

|  |  |  |  |
| --- | --- | --- | --- |
| PORT | STATE | SERVICE | VERSION |
| 23/tcp | open | telnet | Linux telnetd |
| 25/tcp | open | smtp | Postfix smtpd |
| 80/tcp | open | http | Apache httpd 2.2.8 ((Ubuntu) DAV/2) |
| 2121/tcp | open | ftp | ProFTPD 1.3.1 |
| 8180/tcp | open | http | Apache Tomcat/Coyote JSP engine 1.1 |
| 36157/tcp | open | mountd | 1-3 (RPC #100005) |
| 48679/tcp | open | java-rmi | GNU Classpath grmiregistry |
| 51615/tcp | open | status | 1 (RPC #100024) |
| 59036/tcp | open | nlockmgr | 1-4 (RPC #100021 |

Nmap result using brute category scripts.

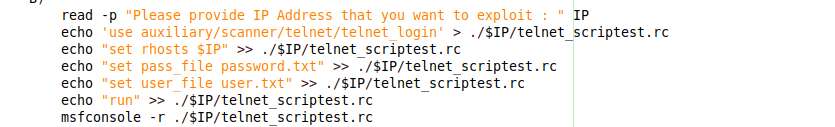
Result

|  |  |  |  |
| --- | --- | --- | --- |
| PORT | STATE | SERVICE | VERSION |
| 23/tcp | open | telnet | Linux telnetd |
| | telnet-brute:  | Accounts: No valid accounts found  | Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0  |\_ ERROR: The service seems to have failed or is heavily firewalled...  |\_tso-enum: ERROR: Script execution failed (use -d to debug)  |\_vtam-enum: Not VTAM or 'logon applid' command not accepted. Try with script arg 'vtam-enum.macros=true' | | | |
| 80/tcp | open | http | Apache httpd 2.2.8 ((Ubuntu) DAV/2) |
| |\_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)  | http-brute:  |\_ Path "/" does not require authentication  |\_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2 | | | |
| 2121/tcp | open | ftp | ProFTPD 1.3.1 |
| | ftp-brute:  | Accounts: No valid accounts found  | Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0  |\_ ERROR: The service seems to have failed or is heavily firewalled... | | | |
| 8180/tcp | open | http | Apache Tomcat/Coyote JSP engine 1.1 |
| | http-brute:  |\_ Path "/" does not require authentication  |\_http-server-header: Apache-Coyote/1.1 | | | |

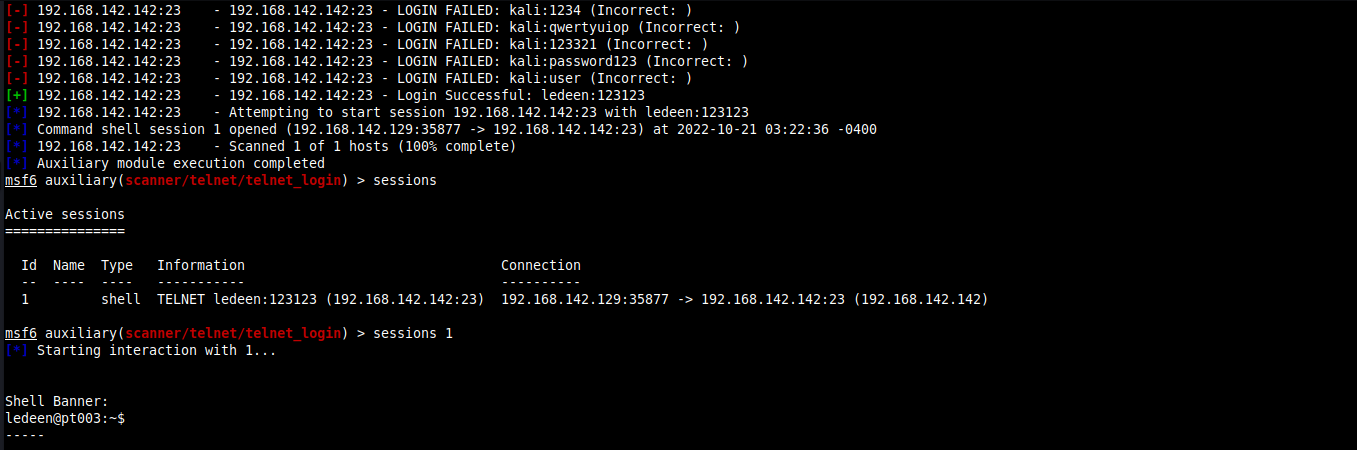
Successful exploit

1. Using msfconsole via port 23 - telnet

Script command

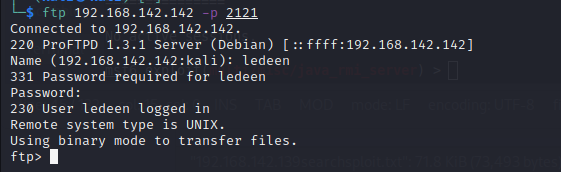


Result



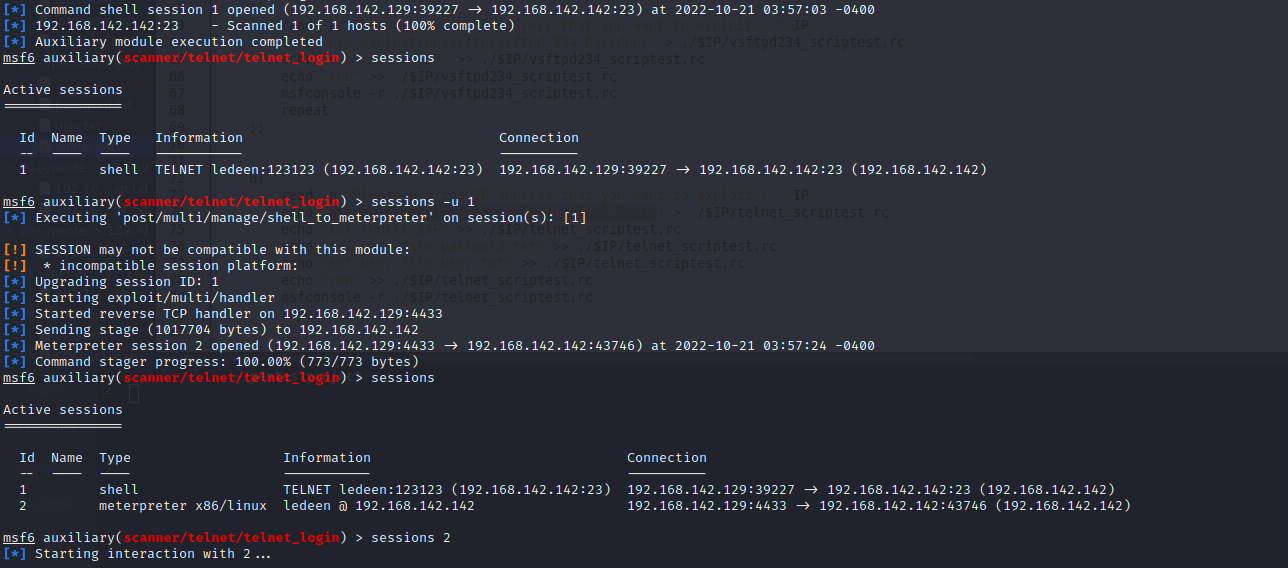
The access granted: ledeen

1. Login using ID, “ledeen” (leaked on company website, port 80) and password (123123 found through telnet exploit).

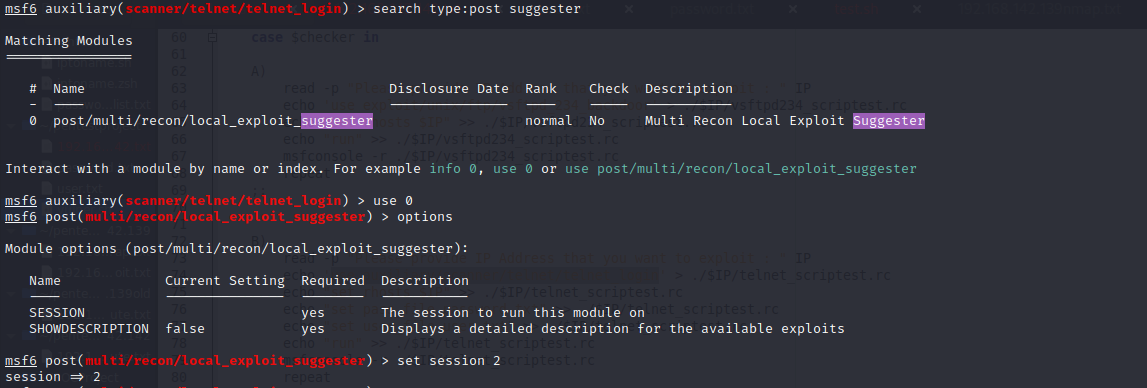


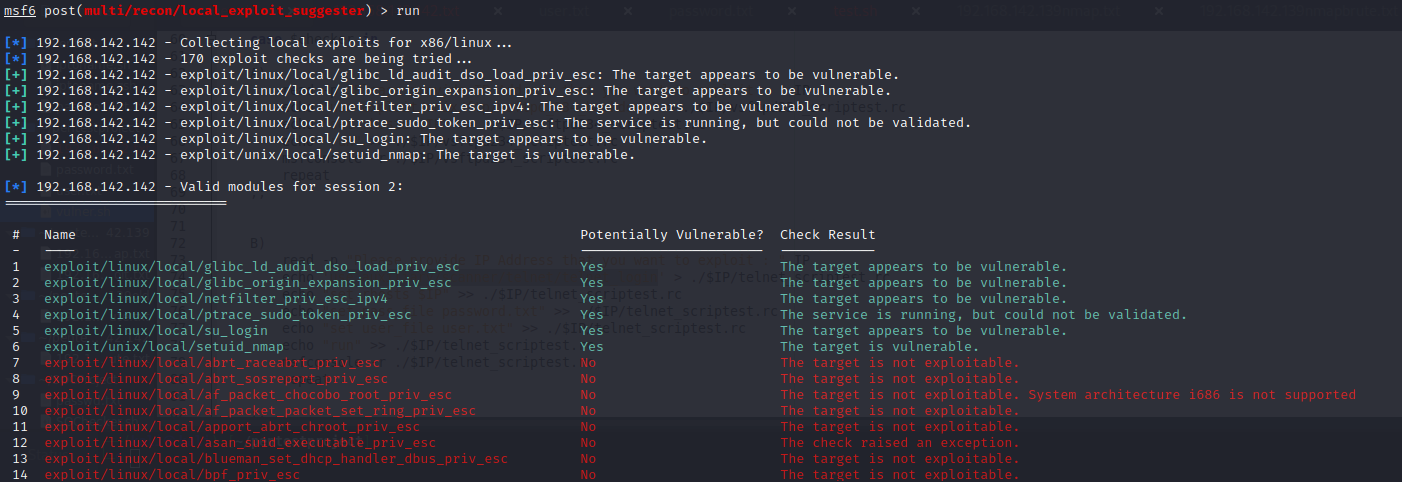
Post Exploitation

In order to escalate the privilege to become root access, I upgrade the session from shell to meterpreter.



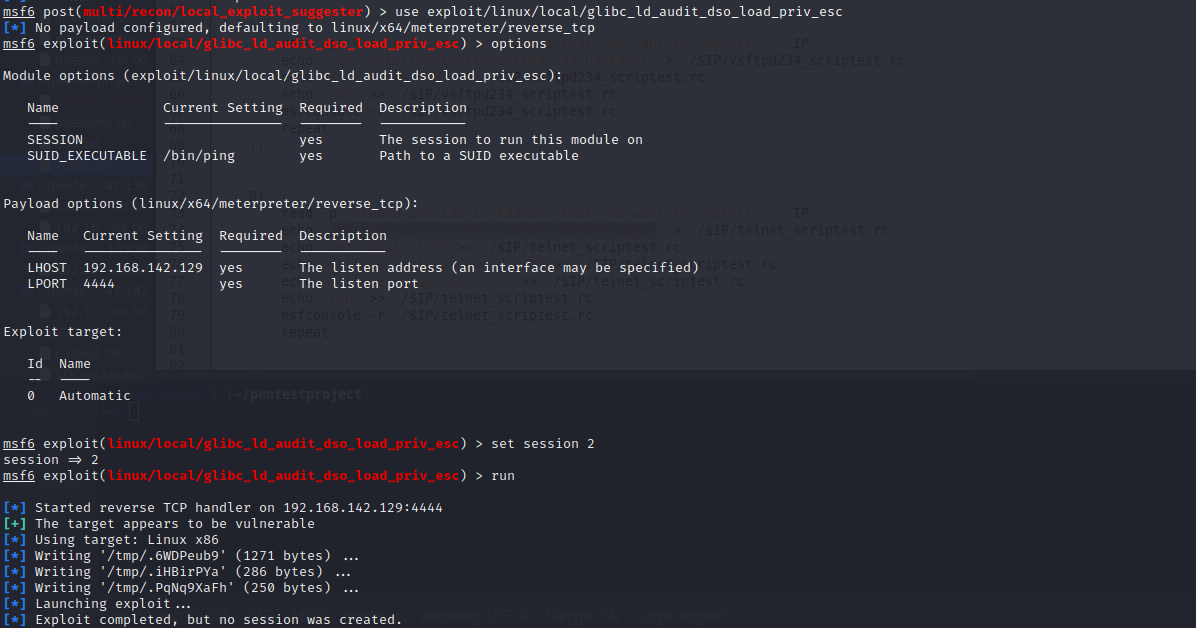
Then, I proceed to use msfconsole post suggester to look for possible way to gain root access.



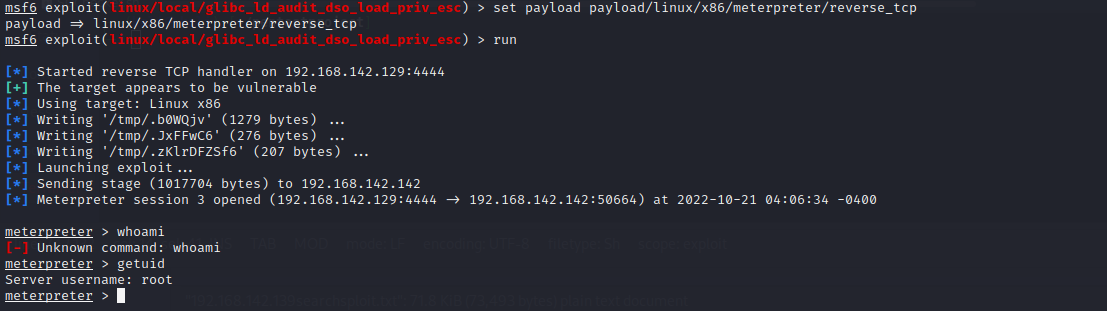


I try to test the first suggestion: exploit/linux/local/glibc\_ld\_audit\_dso\_load\_priv\_esc.

In first attempt, the exploit completed but no session was created.



I try to change the payload to x86 (32 bits) and I manage to gain access into meterpreter with root access.



1. Conclusion / Suggestions

As shown from Section 3- Results, attacker is able to gain root access for both machines. Thus, it is imperative to fix or mitigate those vulnerable ports by closing the unused ports.

Another loophole is using weak passwords. System admin can cross reference existing user’s password with popular weak password listed online. A general rule is using at least 12 digits passwords with combination of number, alphabet, upper, lower and special characters.

Please update the service’s version to latest version (if can) or applying the available patches (if any) as those patches have already address those vulnerabilities.

Last but not least, please look out for leaked credentials online be it on own company website or in site like [www.pastebin.com](http://www.pastebin.com). If the user ID and password can be found online, please proceed to change the ID and password.

1. Appendix

Searchsploit output for potential vulnerability



Script used in assessment



Hash password copy and download from target machine



Leaked users in company website (192.168.142.142)

