Nax_THM

Enumuration

On main page we see some letters which seem to be periodic table .We see the numbers of that element and then convert the ascii to text
and we get a /PI3T.PNg

We go to that directory and see the image

we see that artist of the picture is
Piet Mondrian

 # default username is nagiosadmin

 # The password was embedded in the picture and we found it from a website
   n3p3UQ&9BjLp4$7uhWdY

 # nagiosadmin:n3p3UQ&9BjLp4$7uhWdY

Nmap

```
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 62:1d:d9:88:01:77:0a:52:bb:59:f9:da:c1:a6:e3:cd (RSA)
|   256 af:67:7d:24:e5:95:f4:44:72:d1:0c:39:8d:cc:21:15 (ECDSA)
|_  256 20:28:15:ef:13:c8:9f:b8:a7:0f:50:e6:2f:3b:1e:57 (ED25519)
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: ubuntu.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=ubuntu
| Not valid before: 2020-03-23T23:42:04
|_Not valid after:  2030-03-21T23:42:04
|_ssl-date: TLS randomness does not represent time
80/tcp    open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
389/tcp   open  ldap        OpenLDAP 2.2.X - 2.3.X
443/tcp   open  ssl/http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=192.168.85.153/organizationName=Nagios Enterprises/stateOrProvinceName=Minnesota/-
countryName=US
| Not valid before: 2020-03-24T00:14:58
|_Not valid after:  2030-03-22T00:14:58
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
5667/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.1 (95%), Linux 3.16
(95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Android 4.1.1 (92%), Sony Android TV (Android 5.0)
(92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: Host:  ubuntu.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   204.17 ms 10.4.0.1
2   ... 3
4   458.95 ms 10.10.42.212

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.61 seconds
```

SSH:22

SMTP:25

HTTP:80:443

Gobuster

/cgi-bin/ (Status: 403)
/cgi-bin/.php (Status: 403)
/index.html (Status: 200)
/index.php (Status: 200)
/index.php (Status: 200)
/javascript (Status: 301)
/nagios (Status: 401)
/server-status (Status: 403)

LDAP:389

TCPWRAPPED:5667

Exploitation

We see that nagiosxi is running version 5.5.6

We found a msf module linux/http/nagios_xi_authenticated_rce

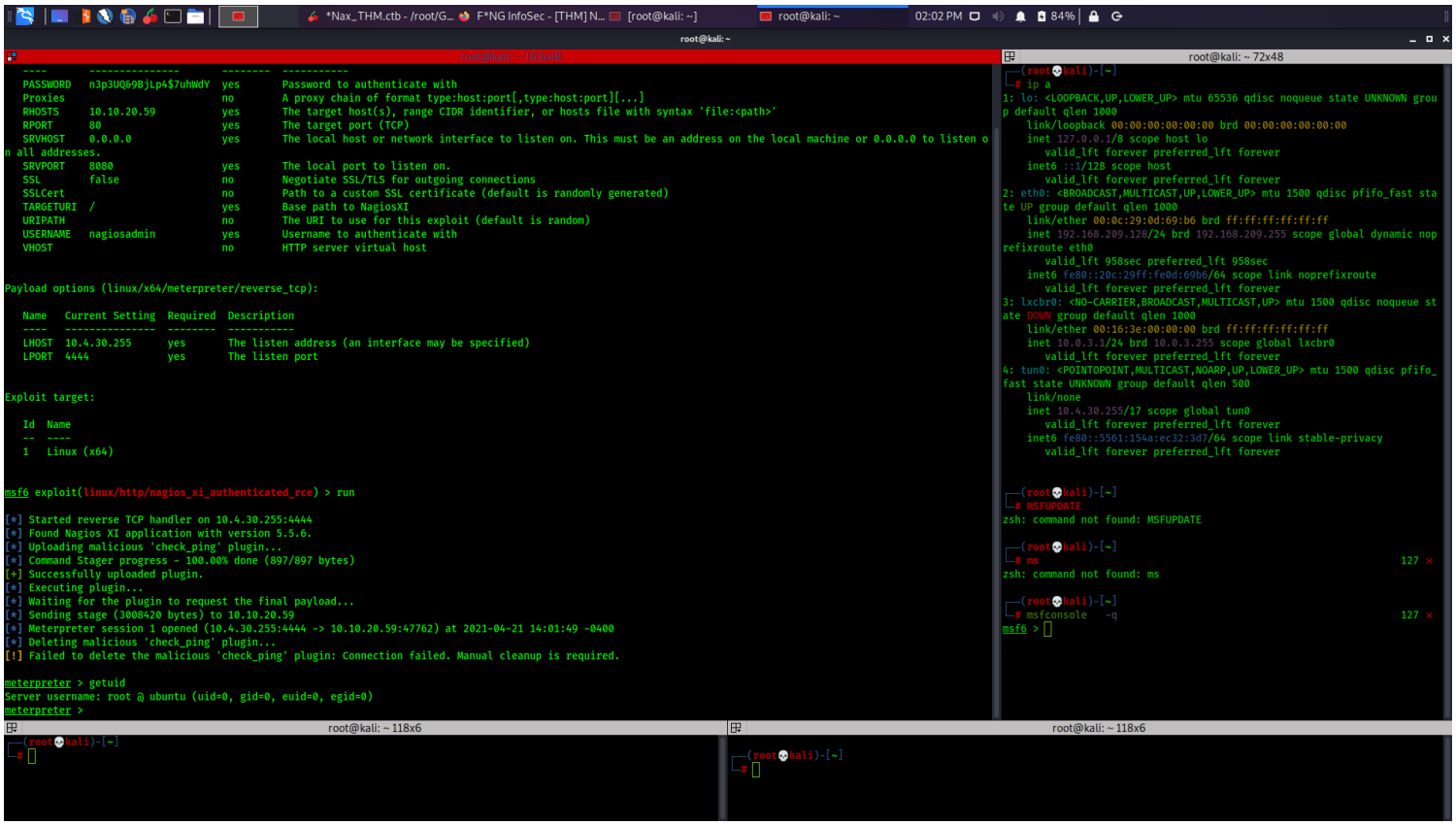
Exploit gave us a shell after many tries :(

CVE-2019-15949

RCE

msf module: linux/http/nagios_xi_authenticated_rce

Got a meterpreter



#

Post Exploitation

Directoly root

got user and root flags

Loot

Credentials

Web Login

nagiosadmin:n3p3UQ&9BjLp4$7uhWdY

Flag

User Flag

THM{84b17add1d72a9f2e99c33bc568ae0f1}

Root Flag

THM{c89b2e39c83067503a6508b21ed6e962}