Exploiting ColdFusion 8

HacktheBox(Arctic)

Contents

Nmap

The results of the nmap scan shows RPC ports and fmtp. The interesting port here is 8500. By navigating to this port in the browser, we can enumerate more.

Nmap 7.80 scan initiated Thu Jan 14 07:26:41 2021 as: nmap -sV -v -p- -oN allports.nmap 10.10.10.11

Nmap scan report for 10.10.10.11

Host is up (0.052s latency).

Not shown: 65532 filtered ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

8500/tcp open fmtp?

49154/tcp open msrpc Microsoft Windows RPC

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

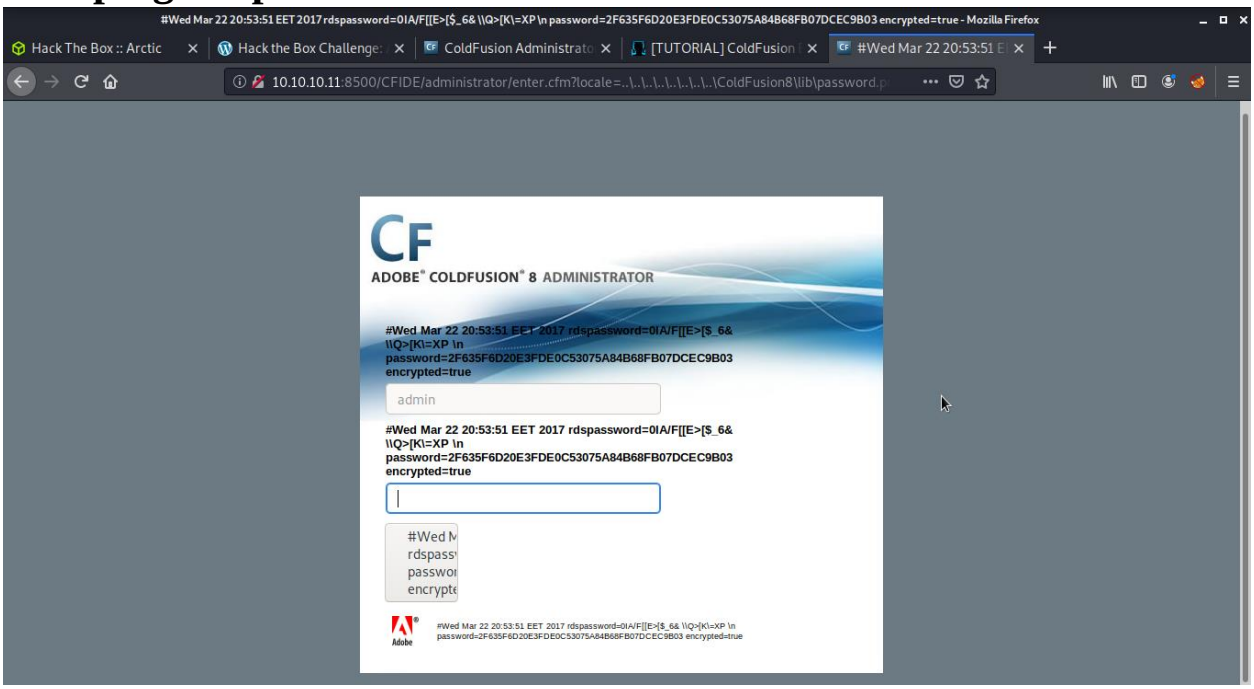
Read data files from: /usr/bin/../share/nmap

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

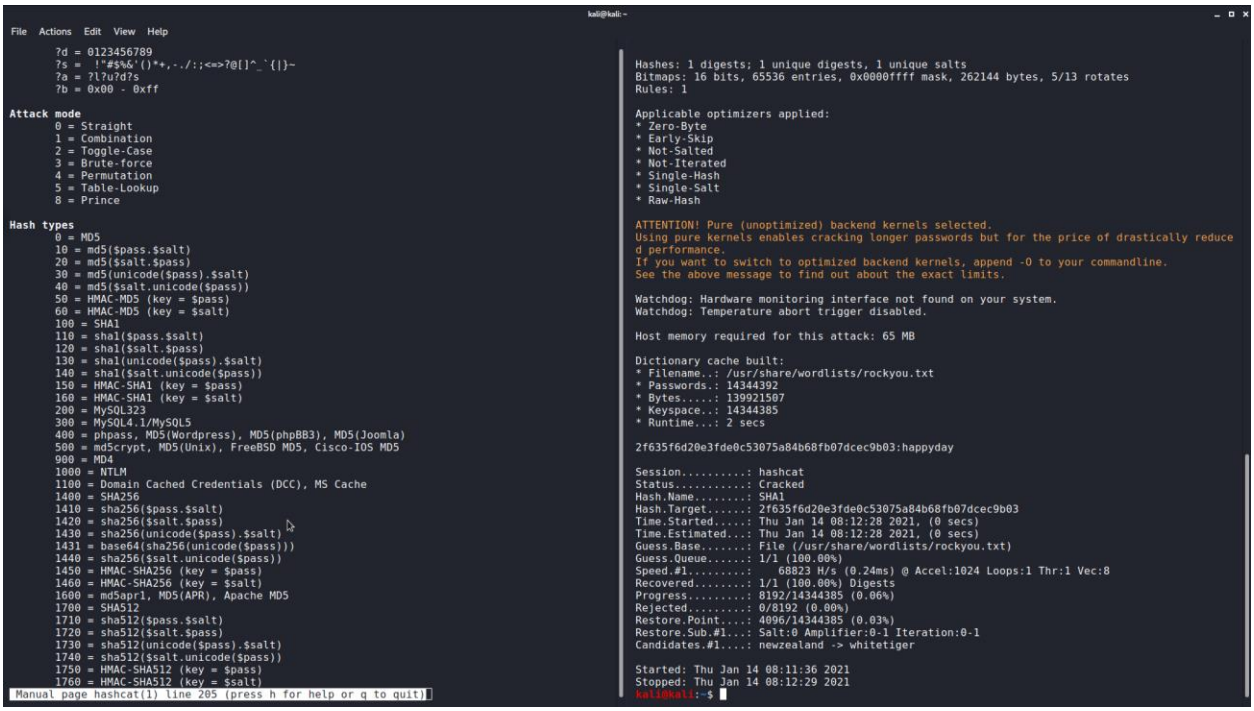
Nmap done at Thu Jan 14 07:30:38 2021 -- 1 IP address (1 host up) scanned in 237.02 seconds

After some dirbusting I came to an administrator login page. Some google searching led to a string that can be pasted into the url. This causes the login page to leak the hashed credentials for the login.

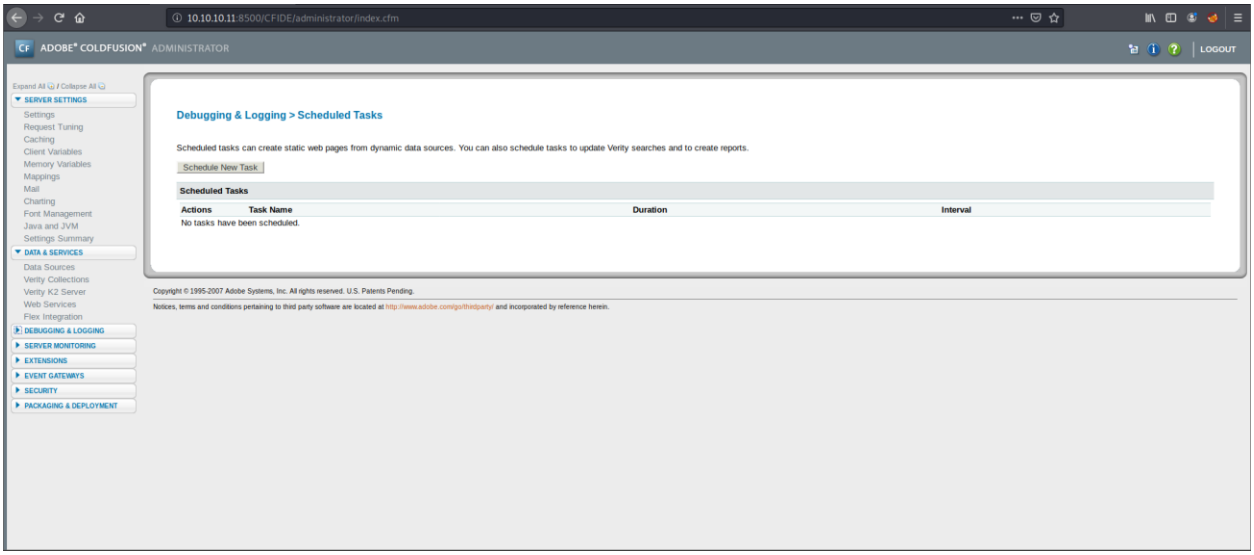
Dumping the password hash



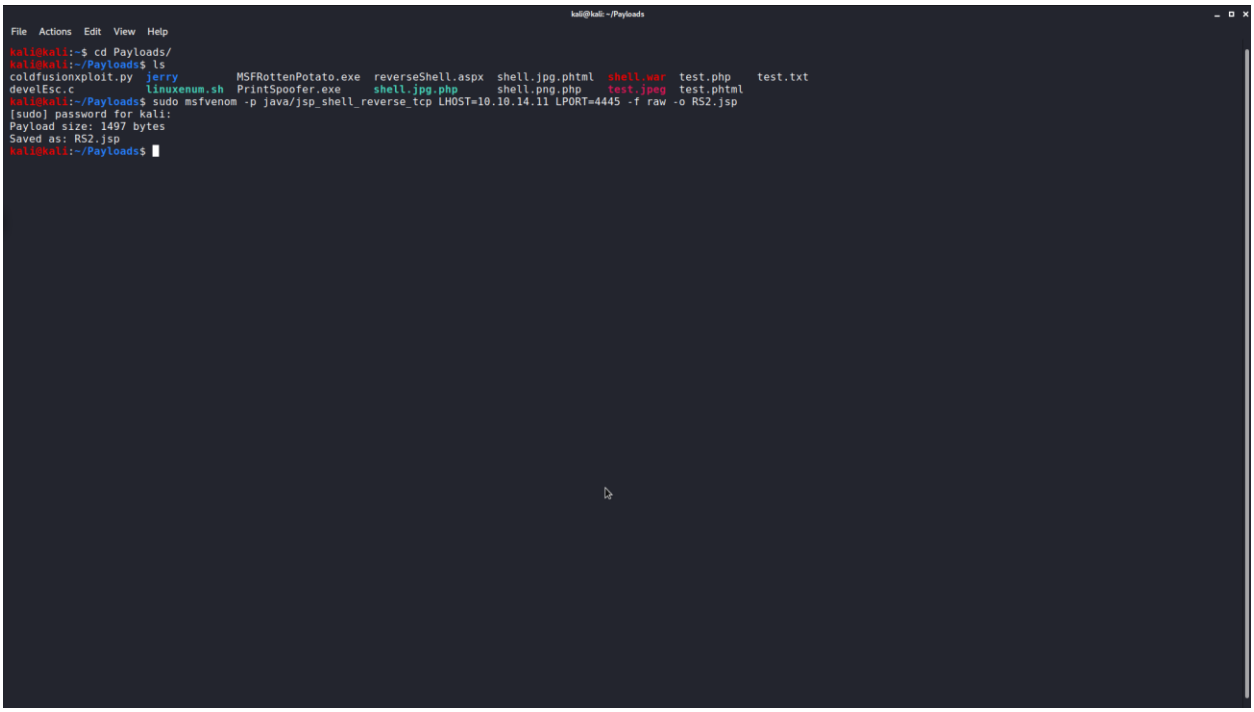
Cracking the hash:


kali@kali: ~
File Actions Edit View Help
?d = 0123456789
?s = !"#$%&'()*+,-./:;<=>?@[]^_`{|}~
?a = ?l?u?d?s
?b = 0x00 - 0xff
Attack mode
0 = Straight
1 = Combination
2 = Toggle-Case
3 = Brute-force
4 = Permutation
5 = Table-Lookup
8 = Prince
Hash types
0 = MD5
10 = md5($pass.$salt)
20 = md5($salt.$pass)
30 = md5(unicode($pass).$salt)
40 = md5($salt.unicode($pass))
50 = HMAC-MD5 (key = $pass)
60 = HMAC-MD5 (key = $salt)
100 = SHA1
110 = sha1($pass.$salt)
120 = sha1($salt.$pass)
130 = sha1(unicode($pass).$salt)
140 = sha1($salt.unicode($pass))
150 = HMAC-SHA1 (key = $pass)
160 = HMAC-SHA1 (key = $salt)
200 = MySQL323
300 = MySQL4.1/MySQL5
400 = phpass, MD5(Wordpress), MD5(phpBB3), MD5(Joomla)
500 = md5crypt, MD5(Unix), FreeBSD MD5, Cisco-IOS MD5
900 = MD4
1000 = NTLM
1100 = Domain Cached Credentials (DCC), MS Cache
1400 = SHA256
1410 = sha256($pass.$salt)
1420 = sha256($salt.$pass)
1430 = sha256(unicode($pass).$salt)
1431 = base64(sha256(unicode($pass)))
1440 = sha256($salt.unicode($pass))
1450 = HMAC-SHA256 (key = $pass)
1460 = HMAC-SHA256 (key = $salt)
1600 = md5apr1, MD5(APR), Apache MD5
1700 = SHA512
1710 = sha512($pass.$salt)
1720 = sha512($salt.$pass)
1730 = sha512(unicode($pass).$salt)
1740 = sha512($salt.unicode($pass))
1750 = HMAC-SHA512 (key = $pass)
1760 = HMAC-SHA512 (key = $salt)
Manual page hashcat(1) line 205 (press h for help or q to quit)
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
Applicable optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash
ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduce
d performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.
Host memory required for this attack: 65 MB
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 2 secs
2f635f6d20e3fde0c53075a84b68fb07dcec9b03:happyday
Session.........: hashcat
Status..........: Cracked
Hash.Name.......: SHA1
Hash.Target.....: 2f635f6d20e3fde0c53075a84b68fb07dcec9b03
Time.Started.....: Thu Jan 14 08:12:28 2021, (0 secs)
Time.Estimated...: Thu Jan 14 08:12:28 2021, (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 68823 H/s (0.24ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 8192/14344385 (0.06%)
Rejected.........: 0/8192 (0.00%)
Restore.Point....: 4096/14344385 (0.03%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: newzealand -> whitetiger
Started: Thu Jan 14 08:11:36 2021
Stopped: Thu Jan 14 08:12:29 2021
kali@kali:~$

ColdFusion Admin Portal

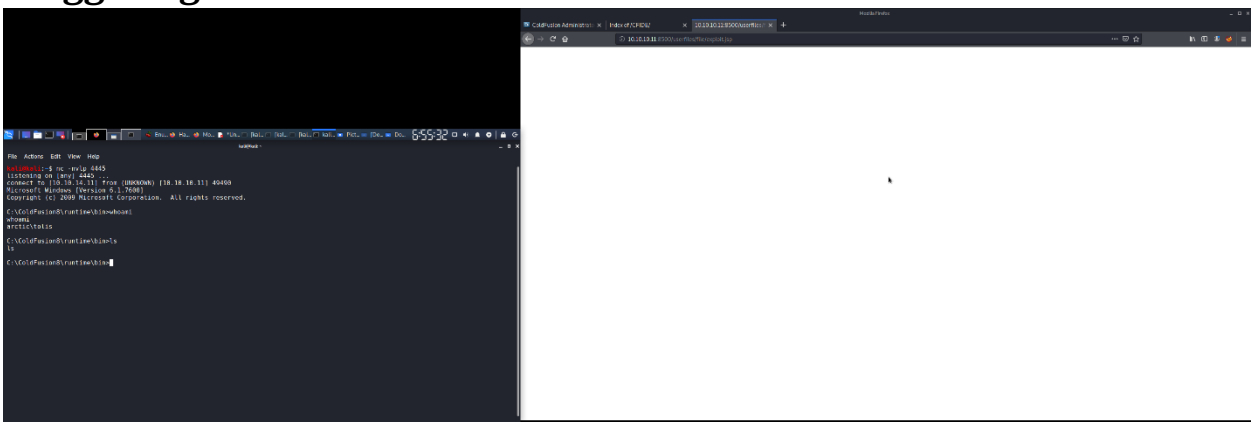


After logging in, navigate to debugging and logging. Here we can schedule a new task and upload our malicious file.



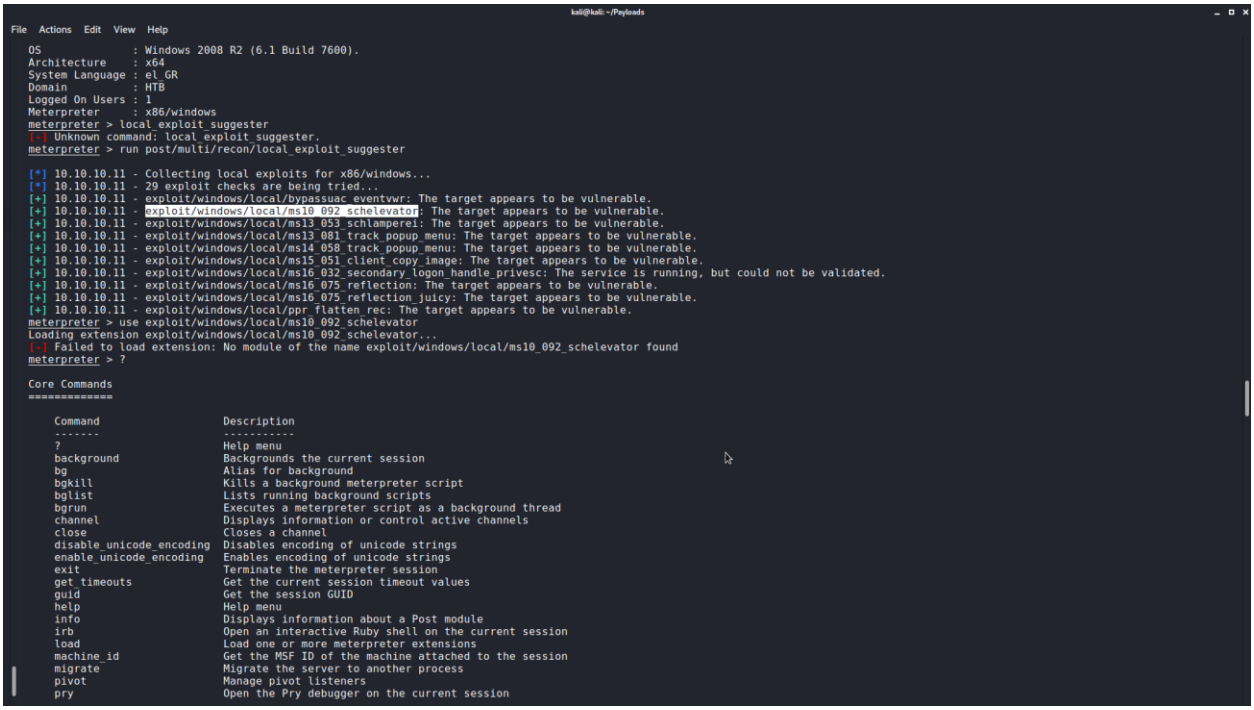
Generating shell code

Triggering a reverse shell

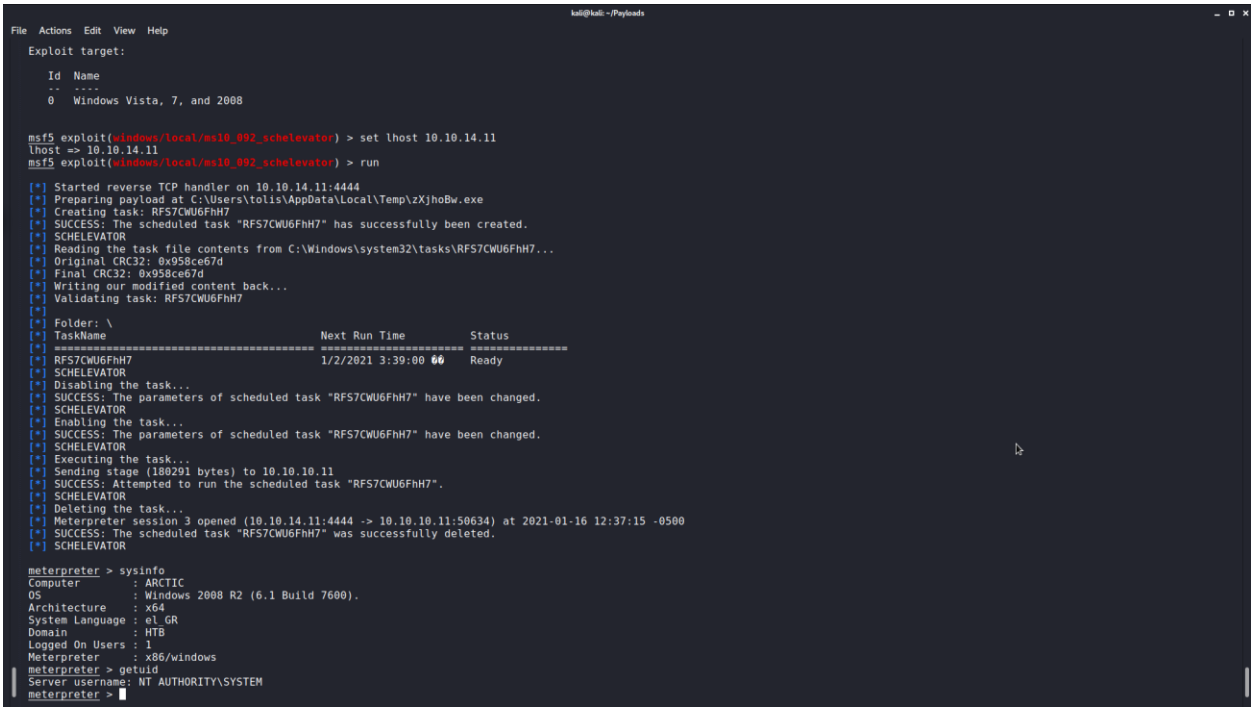


From here we can further enumerate the machine outlined in recon.txt. The output of this file will be shown in the appendix.

After upgrading to a meterpreter shell, I ran exploit suggester and received the output pictured.



Root



Successful exploitation leads to root privileges.

Appendix

###Nmap###

Nmap 7.80 scan initiated Thu Jan 14 07:26:41 2021 as: nmap -sV -v -p- -oN allports.nmap 10.10.10.11

Nmap scan report for 10.10.10.11

Host is up (0.052s latency).

Not shown: 65532 filtered ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

8500/tcp open fmtp?

49154/tcp open msrpc Microsoft Windows RPC

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

Read data files from: /usr/bin/../share/nmap

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

###Interesting Finds###

http://10.10.10.11:8500/CFIDE

###System Enumeration###

C:\ColdFusion8\runtime\bin>systeminfo

systeminfo

Host Name: ARCTIC

OS Name: Microsoft Windows Server 2008 R2 Standard

OS Version: 6.1.7600 N/A Build 7600

OS Manufacturer: Microsoft Corporation

OS Configuration: Standalone Server

OS Build Type: Multiprocessor Free

Registered Owner: Windows User

Registered Organization:

Product ID: 55041-507-9857321-84451

Original Install Date: 22/3/2017, 11:09:45 ��

System Boot Time: 17/1/2021, 9:37:38 ��

System Manufacturer: VMware, Inc.

System Model: VMware Virtual Platform

System Type: x64-based PC

Processor(s): 2 Processor(s) Installed.

[01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz

[02]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz

BIOS Version: Phoenix Technologies LTD 6.00, 12/12/2018

Windows Directory: C:\Windows

System Directory: C:\Windows\system32

Boot Device: \Device\HarddiskVolume1

System Locale: el;Greek

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

Time Zone: (UTC+02:00) Athens, Bucharest, Istanbul

Total Physical Memory: 1.023 MB

Available Physical Memory: 280 MB

Virtual Memory: Max Size: 2.047 MB

Virtual Memory: Available: 1.190 MB

Virtual Memory: In Use: 857 MB

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

Domain: HTB

Logon Server: N/A

Hotfix(s): N/A

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

[01]: Intel(R) PRO/1000 MT Network Connection

Connection Name: Local Area Connection

DHCP Enabled: No

IP address(es)

[01]: 10.10.10.11

###User enumeration###

C:\ColdFusion8\runtime\bin>whoami /priv

whoami /priv

PRIVILEGES INFORMATION

Privilege Name Description State

============================= === ========

SeChangeNotifyPrivilege Bypass traverse checking Enabled

SeImpersonatePrivilege Impersonate a client after authentication Enabled

SeCreateGlobalPrivilege Create global objects Enabled

SeIncreaseWorkingSetPrivilege Increase a process working set Disabled

C:\ColdFusion8\runtime\bin>whoami /groups

whoami /groups

GROUP INFORMATION

Group Name Type SID Attributes

=================================== ================ ============
==

Everyone Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group

BUILTIN\Users Alias S-1-5-32-545 Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\SERVICE Well-known group S-1-5-6 Mandatory group, Enabled by default, Enabled group

CONSOLE LOGON Well-known group S-1-2-1 Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\Authenticated Users Well-known group S-1-5-11 Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\This Organization Well-known group S-1-5-15 Mandatory group, Enabled by default, Enabled group

LOCAL Well-known group S-1-2-0 Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10 Mandatory group, Enabled by default, Enabled group

Mandatory Label\High Mandatory Level Label S-1-16-12288 Mandatory group, Enabled by default, Enabled group

C:\ColdFusion8\runtime\bin>net user

net user

User accounts for \\ARCTIC

Administrator Guest tolis

The command completed successfully.

C:\ColdFusion8\runtime\bin>net localgroup

net localgroup

Aliases for \\ARCTIC

---

*Administrators

*Backup Operators

*Certificate Service DCOM Access

*Cryptographic Operators

*Distributed COM Users

*Event Log Readers

*Guests

*IIS_IUSRS

*Network Configuration Operators

*Performance Log Users

*Performance Monitor Users

*Power Users

*Print Operators

*Remote Desktop Users

*Replicator

*Users

The command completed successfully

###Network Enumeration###

C:\ColdFusion8\runtime\bin>ipconfig /all

ipconfig /all

Windows IP Configuration

Host Name . . . . . : arctic

Primary Dns Suffix . . . . . :

Node Type . . . . . : Hybrid

IP Routing Enabled. . . . . : No

WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-50-56-B9-ED-06
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 10.10.10.11(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.10.2
DNS Servers . . . . . : 10.10.10.2
8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{79F1B374-AC3C-416C-8812-BF482D048A22}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Local Area Connection* 9:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Description . . . . . : Teredo Tunneling Pseudo-Interface

Physical Address. . . . . : 00-00-00-00-00-00-00-E0

DHCP Enabled. . . . . : No

Autoconfiguration Enabled . . . . : Yes

C:\ColdFusion8\runtime\bin>arp -a

arp -a

Interface: 10.10.10.11 --- 0xb

Internet Address Physical Address Type

10.10.10.2 00-50-56-b9-f9-ab dynamic

10.10.10.255 ff-ff-ff-ff-ff-ff static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.252 01-00-5e-00-00-fc static

C:\ColdFusion8\runtime\bin>route print

route print

===

Interface List

11...00 50 56 b9 ed 06 ......Intel(R) PRO/1000 MT Network Connection

1...........................Software Loopback Interface 1

12...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter

13...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface

===

IPv4 Route Table

===

Active Routes:

Network Destination Netmask Gateway Interface Metric

```
          0.0.0.0          0.0.0.0      10.10.10.2      10.10.10.11    266
       10.10.10.0    255.255.255.0        On-link      10.10.10.11    266
      10.10.10.11  255.255.255.255        On-link      10.10.10.11    266
     10.10.10.255  255.255.255.255        On-link      10.10.10.11    266
        127.0.0.0        255.0.0.0        On-link        127.0.0.1    306
        127.0.0.1  255.255.255.255        On-link        127.0.0.1    306
  127.255.255.255  255.255.255.255        On-link        127.0.0.1    306
        224.0.0.0        240.0.0.0        On-link        127.0.0.1    306
        224.0.0.0        240.0.0.0        On-link      10.10.10.11    266
  255.255.255.255  255.255.255.255        On-link        127.0.0.1    306
  255.255.255.255  255.255.255.255        On-link      10.10.10.11    266
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      10.10.10.2  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
  1    306 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\ColdFusion8\runtime\bin>netstat -ano
netstat -ano
```

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	668
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:2522	0.0.0.0:0	LISTENING	1172
TCP	0.0.0.0:2930	0.0.0.0:0	LISTENING	1172
TCP	0.0.0.0:6085	0.0.0.0:0	LISTENING	1172
TCP	0.0.0.0:6086	0.0.0.0:0	LISTENING	1088
TCP	0.0.0.0:7999	0.0.0.0:0	LISTENING	1172
TCP	0.0.0.0:8500	0.0.0.0:0	LISTENING	1172
TCP	0.0.0.0:9921	0.0.0.0:0	LISTENING	2196
TCP	0.0.0.0:9951	0.0.0.0:0	LISTENING	1308
TCP	0.0.0.0:9961	0.0.0.0:0	LISTENING	2412
TCP	0.0.0.0:19997	0.0.0.0:0	LISTENING	1180
TCP	0.0.0.0:19998	0.0.0.0:0	LISTENING	1232
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	368
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	756
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	796
TCP	0.0.0.0:49159	0.0.0.0:0	LISTENING	1172
TCP	0.0.0.0:49171	0.0.0.0:0	LISTENING	492
TCP	0.0.0.0:49175	0.0.0.0:0	LISTENING	476
TCP	10.10.10.11:139	0.0.0.0:0	LISTENING	4
TCP	10.10.10.11:8500	10.10.14.11:39418	TIME_WAIT	0
TCP	10.10.10.11:49606	10.10.14.11:4445	ESTABLISHED	1172
TCP	127.0.0.1:9951	127.0.0.1:49169	ESTABLISHED	1308
TCP	127.0.0.1:49169	127.0.0.1:9951	ESTABLISHED	2412

```
TCP    127.0.0.1:49605        127.0.0.1:9921         TIME_WAIT       0
TCP    127.0.0.1:49607        127.0.0.1:9961         TIME_WAIT       0
TCP    127.0.0.1:49608        127.0.0.1:9921         TIME_WAIT       0
TCP    127.0.0.1:49609        127.0.0.1:9961         TIME_WAIT       0
TCP    127.0.0.1:49610        127.0.0.1:9921         TIME_WAIT       0
TCP    127.0.0.1:49611        127.0.0.1:9961         TIME_WAIT       0
TCP    127.0.0.1:49612        127.0.0.1:9921         TIME_WAIT       0
TCP    127.0.0.1:49613        127.0.0.1:9961         TIME_WAIT       0
TCP    [::]:135               [::]:0                 LISTENING       668
TCP    [::]:445               [::]:0                 LISTENING       4
TCP    [::]:2522              [::]:0                 LISTENING       1172
TCP    [::]:2930              [::]:0                 LISTENING       1172
TCP    [::]:6085              [::]:0                 LISTENING       1172
TCP    [::]:7999              [::]:0                 LISTENING       1172
TCP    [::]:8500              [::]:0                 LISTENING       1172
TCP    [::]:47001             [::]:0                 LISTENING       4
TCP    [::]:49152             [::]:0                 LISTENING       368
TCP    [::]:49153             [::]:0                 LISTENING       756
TCP    [::]:49154             [::]:0                 LISTENING       796
TCP    [::]:49159             [::]:0                 LISTENING       1172
TCP    [::]:49171             [::]:0                 LISTENING       492
TCP    [::]:49175             [::]:0                 LISTENING       476
UDP    0.0.0.0:123            *:*                                    852
UDP    0.0.0.0:5355           *:*                                    936
UDP    0.0.0.0:58423          *:*                                    1180
UDP    0.0.0.0:58425          *:*                                    1180
UDP    0.0.0.0:58427          *:*                                    1232
UDP    0.0.0.0:58429          *:*                                    1232
UDP    10.10.10.11:137        *:*                                    4
```

```
  UDP    10.10.10.11:138        *:*                    4
  UDP    127.0.0.1:58422        *:*                    1180
  UDP    127.0.0.1:58424        *:*                    1180
  UDP    127.0.0.1:58426        *:*                    1232
  UDP    127.0.0.1:58428        *:*                    1232
  UDP    [::]:123               *:*                    852
```

###Firewall and Antivirus###

C:\ColdFusion8\runtime\bin>netsh firewall show state

netsh firewall show state

Firewall status:

Profile = Standard

Operational mode = Enable

Exception mode = Enable

Multicast/broadcast response mode = Enable

Notification mode = Disable

Group policy version = Windows Firewall

Remote admin mode = Disable

Ports currently open on all network interfaces:

Port Protocol Version Program

8500 TCP Any (null)

IMPORTANT: Command executed successfully.

However, "netsh firewall" is deprecated;

use "netsh advfirewall firewall" instead.

For more information on using "netsh advfirewall firewall" commands

instead of "netsh firewall", see KB article 947709

at http://go.microsoft.com/fwlink/?linkid=121488 .

C:\ColdFusion8\runtime\bin>netsh firewall show config

netsh firewall show config

Domain profile configuration:

Operational mode = Enable

Exception mode = Enable

Multicast/broadcast response mode = Enable

Notification mode = Disable

Allowed programs configuration for Domain profile:

Mode Traffic direction Name / Program

Port configuration for Domain profile:

Port Protocol Mode Traffic direction Name

8500 TCP Enable Inbound CF

ICMP configuration for Domain profile:

Mode Type Description

Enable 2 Allow outbound packet too big

Standard profile configuration (current):

Operational mode = Enable

Exception mode = Enable

Multicast/broadcast response mode = Enable

Notification mode = Disable

Allowed programs configuration for Standard profile:

Mode Traffic direction Name / Program

Port configuration for Standard profile:

Port Protocol Mode Traffic direction Name

8500 TCP Enable Inbound CF

ICMP configuration for Standard profile:

Mode Type Description

Enable 2 Allow outbound packet too big

Log configuration:

File location = C:\Windows\system32\LogFiles\Firewall\pfirewall.log

Max file size = 4096 KB

Dropped packets = Disable

Connections = Disable

IMPORTANT: Command executed successfully.

However, "netsh firewall" is deprecated;

use "netsh advfirewall firewall" instead.

For more information on using "netsh advfirewall firewall" commands

instead of "netsh firewall", see KB article 947709

at http://go.microsoft.com/fwlink/?linkid=121488 .