```
# Nmap 7.92 scan initiated Sun Jul 16 18:04:06 2023 as: nmap -sS -A -oN 20230701Scan.txt
10.0.0.10-21
Nmap scan report for ip-10-0-0-10.us-east-2.compute.internal (10.0.0.10)
Host is up (0.00033s latency).
Not shown: 990 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.5
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open  http        Apache httpd 2.4.7
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
111/tcp  open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          34557/udp   status
|   100024  1          40170/tcp6  status
|   100024  1          40639/udp6  status
|_  100024  1          53386/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open  ipp         CUPS 1.7
|_http-server-header: CUPS/1.7 IPP/2.1
|_http-title: Bad Request - CUPS v1.7.2
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
```

| lusers: 1
| lservers: 0
|_ server: irc.TestIRC.net
8080/tcp open http   Jetty 8.1.7.v20120910
|_http-server-header: Jetty(8.1.7.v20120910)
|_http-title: Error 404 - Not Found
MAC Address: 02:3E:89:EE:41:99 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=7/16%OT=21%CT=1%CU=39217%PV=Y%DS=1%DC=D%G=Y%
M=023E89%T
OS:M=64B431A9%P=x86_64-pc-linux-
gnu)SEQ(SP=100%GCD=1%ISR=106%TI=Z%II=I%TS=8
OS:)OPS(O1=M2301ST11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M2301S
T11NW7%O5
OS:=M2301ST11NW7%O6=M2301ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%
W5=68DF%W
OS:6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%D
F=Y%T=40%S
OS:=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S
=Z%A=S+%
OS:F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=
G%RID=G
OS:%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix,
Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
| date: 2023-07-16T18:06:15
|_ start_date: N/A
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE3, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
| Computer name: metasploitable3-ub1404

```
|   NetBIOS computer name: METASPLOITABLE3-UB1404\x00
|   Domain name: \x00
|   FQDN: metasploitable3-ub1404
|_  System time: 2023-07-16T18:06:06+00:00
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required

TRACEROUTE
HOP RTT     ADDRESS
1   0.33 ms ip-10-0-0-10.us-east-2.compute.internal (10.0.0.10)

Nmap scan report for ip-10-0-0-21.us-east-2.compute.internal (10.0.0.21)
Host is up (0.00018s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE             VERSION
21/tcp    open  ftp                 Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
22/tcp    open  ssh                 OpenSSH 7.1 (protocol 2.0)
| ssh-hostkey:
|   2048 e4:77:93:34:2c:4f:fd:5d:7e:d7:d3:c3:89:a3:8b:0c (RSA)
|_  521 bb:88:a5:31:1b:46:9b:39:19:08:5b:77:cf:38:8e:1a (ECDSA)
80/tcp    open  http                Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc               Microsoft Windows RPC
139/tcp   open  netbios-ssn         Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds        Windows Server 2008 R2 Standard 7601 Service Pack 1
microsoft-ds
3306/tcp  open  mysql               MySQL 5.5.20-log
| mysql-info:
|   Protocol: 10
|   Version: 5.5.20-log
|   Thread ID: 6
|   Capabilities flags: 63487
|   Some Capabilities: Speaks41ProtocolOld, InteractiveClient, SupportsTransactions,
SupportsCompression, IgnoreSpaceBeforeParenthesis, DontAllowDatabaseTableColumn,
LongPassword, ConnectWithDatabase, IgnoreSigpipes, ODBCClient, Support41Auth,
Speaks41ProtocolNew, FoundRows, SupportsLoadDataLocal, LongColumnFlag,
SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatments
|   Status: Autocommit
```

| Salt: CyW(_)JyD(7{(QC:8JJs
|_ Auth Plugin Name: mysql_native_password
3389/tcp open tcpwrapped
| ssl-cert: Subject: commonName=metasploitable3-win2k8
| Not valid before: 2023-06-26T15:04:33
|_Not valid after: 2023-12-26T15:04:33
| rdp-ntlm-info:
| Target_Name: METASPLOITABLE3
| NetBIOS_Domain_Name: METASPLOITABLE3
| NetBIOS_Computer_Name: METASPLOITABLE3
| DNS_Domain_Name: metasploitable3-win2k8
| DNS_Computer_Name: metasploitable3-win2k8
| Product_Version: 6.1.7601
|_ System_Time: 2023-07-16T18:06:15+00:00
|_ssl-date: 2023-07-16T18:06:32+00:00; 0s from scanner time.
4848/tcp open ssl/http   Oracle Glassfish Application Server
|_ssl-date: 2023-07-16T18:06:32+00:00; 0s from scanner time.
|_http-title: Login
|_http-server-header: GlassFish Server Open Source Edition 4.0
| ssl-cert: Subject: commonName=localhost/organizationName=Oracle
Corporation/stateOrProvinceName=California/countryName=US
| Not valid before: 2013-05-15T05:33:38
|_Not valid after: 2023-05-13T05:33:38
7676/tcp open java-message-service Java Message Service 301
8080/tcp open http   Sun GlassFish Open Source Edition 4.0
|_http-title: GlassFish Server - Server Running
| http-methods:
|_ Potentially risky methods: PUT DELETE TRACE
|_http-server-header: GlassFish Server Open Source Edition 4.0
8181/tcp open ssl/http   Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
|_ssl-date: 2023-07-16T18:06:32+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=localhost/organizationName=Oracle
Corporation/stateOrProvinceName=California/countryName=US
| Not valid before: 2013-05-15T05:33:38
|_Not valid after: 2023-05-13T05:33:38
|_http-server-header: GlassFish Server Open Source Edition 4.0
|_http-title: GlassFish Server - Server Running
| http-methods:
|_ Potentially risky methods: PUT DELETE TRACE
8383/tcp open http   Apache httpd
|_http-title: 400 Bad Request
|_http-server-header: Apache
9200/tcp open wap-wsp?
| fingerprint-strings:

```
|   FourOhFourRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/plain; charset=UTF-8
|     Content-Length: 80
|     handler found for uri [/nice%20ports%2C/Tri%6Eity.txt%2ebak] and method [GET]
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: application/json; charset=UTF-8
|     Content-Length: 332
|     "status" : 200,
|     "name" : "Lilith, the Daughter of Dracula ",
|     "version" : {
|     "number" : "1.1.1",
|     "build_hash" : "f1585f096d3f3985e73456debdc1a0745f512bbc",
|     "build_timestamp" : "2014-04-16T14:27:12Z",
|     "build_snapshot" : false,
|     "lucene_version" : "4.7"
|     "tagline" : "You Know, for Search"
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Content-Type: text/plain; charset=UTF-8
|     Content-Length: 0
|   RTSPRequest, SIPOptions:
|     HTTP/1.1 200 OK
|     Content-Type: text/plain; charset=UTF-8
|_    Content-Length: 0
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49167/tcp open  java-rmi       Java RMI
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9200-TCP:V=7.92%I=7%D=7/16%Time=64B43125%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,1A3,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20application/js
SF:on;\x20charset=UTF-8\r\nContent-Length:\x20332\r\n\r\n{\r\n\x20\x20\"st
SF:atus\"\x20:\x20200,\r\n\x20\x20\"name\"\x20:\x20\"Lilith,\x20the\x20Dau
SF:ghter\x20of\x20Dracula\x20\",\r\n\x20\x20\"version\"\x20:\x20{\r\n\x20\
SF:x20\x20\x20\"number\"\x20:\x20\"1\.1\.1\",\r\n\x20\x20\x20\x20\"build_h
SF:ash\"\x20:\x20\"f1585f096d3f3985e73456debdc1a0745f512bbc\",\r\n\x20\x20
SF:\x20\x20\"build_timestamp\"\x20:\x20\"2014-04-16T14:27:12Z\",\r\n\x20\x
SF:20\x20\x20\"build_snapshot\"\x20:\x20false,\r\n\x20\x20\x20\x20\"lucene
SF:_version\"\x20:\x20\"4\.7\"\r\n\x20\x20},\r\n\x20\x20\"tagline\"\x20:\x
SF:20\"You\x20Know,\x20for\x20Search\"\r\n}\n")%r(HTTPOptions,4F,"HTTP/1\.
SF:0\x20200\x20OK\r\nContent-Type:\x20text/plain;\x20charset=UTF-8\r\nCont
```

SF:ent-Length:\x200\r\n\r\n")%r(RTSPRequest,4F,"HTTP/1\.1\x20200\x20OK\r\n
SF:Content-Type:\x20text/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r
SF:\n\r\n")%r(FourOhFourRequest,A9,"HTTP/1\.0\x20400\x20Bad\x20Request\r\n
SF:Content-Type:\x20text/plain;\x20charset=UTF-8\r\nContent-Length:\x2080\
SF:r\n\r\nNo\x20handler\x20found\x20for\x20uri\x20\[/nice%20ports%2C/Tri%6
SF:Eity\.txt%2ebak\]\x20and\x20method\x20\[GET\]")%r(SIPOptions,4F,"HTTP/1
SF:\.1\x20200\x20OK\r\nContent-Type:\x20text/plain;\x20charset=UTF-8\r\nCo
SF:ntent-Length:\x200\r\n\r\n");
MAC Address: 02:2C:DA:8E:81:53 (Unknown)
Device type: general purpose
Running: Microsoft Windows 2008|Vista|7
OS CPE: cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008
cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h00m01s, deviation: 2h38m47s, median: 0s
|_nbstat: NetBIOS name: METASPLOITABLE3, NetBIOS user: <unknown>, NetBIOS MAC: 02:2c:da:8e:81:53 (unknown)
| smb-os-discovery:
| OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
| OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
| Computer name: metasploitable3-win2k8
| NetBIOS computer name: METASPLOITABLE3\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2023-07-16T11:06:14-07:00
| smb2-time:
| date: 2023-07-16T18:06:12
|_ start_date: 2023-07-16T17:35:53
| smb2-security-mode:
| 2.1:
|_   Message signing enabled but not required
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT ADDRESS
1 0.18 ms ip-10-0-0-21.us-east-2.compute.internal (10.0.0.21)

Post-scan script results:
| clock-skew:
| 0s:
| 10.0.0.10 (ip-10-0-0-10.us-east-2.compute.internal)
|_ 10.0.0.21 (ip-10-0-0-21.us-east-2.compute.internal)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Sun Jul 16 18:06:33 2023 -- 12 IP addresses (2 hosts up) scanned in 147.37 seconds