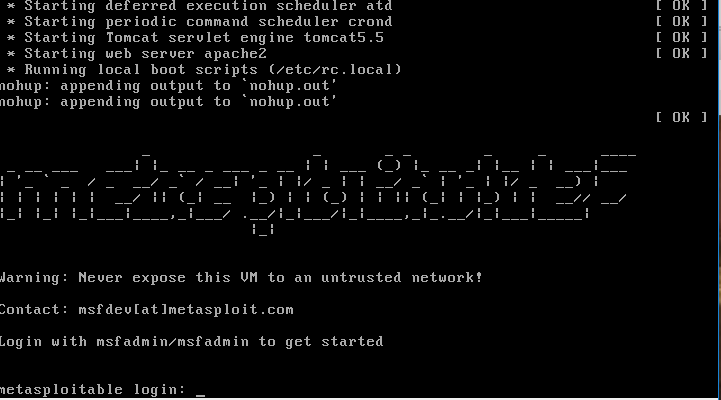
Alexander Cannell

CSIA 6210

Week 5 - Scanning/Mapping

**Setting up my Meta:**



**My IP Address of my kali box:**

﻿

**root@kali**:**~**# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
 inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255  
 inet6 fe80::a00:27ff:fe27:6d4 prefixlen 64 scopeid 0x20<link>  
 ether 08:00:27:27:06:d4 txqueuelen 1000 (Ethernet)  
 RX packets 10 bytes 2350 (2.2 KiB)  
 RX errors 0 dropped 0 overruns 0 frame 0  
 TX packets 534 bytes 33360 (32.5 KiB)  
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
 inet 127.0.0.1 netmask 255.0.0.0  
 inet6 ::1 prefixlen 128 scopeid 0x10<host>  
 loop txqueuelen 1 (Local Loopback)  
 RX packets 18 bytes 1058 (1.0 KiB)  
 RX errors 0 dropped 0 overruns 0 frame 0  
 TX packets 18 bytes 1058 (1.0 KiB)  
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

**Scanning a domain to get all the active addresses in the domain:**

**root@kali**:**~**# nmap -n -sP 10.0.2.15/24  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-05 15:08 EST  
Nmap scan report for 10.0.2.2  
Host is up (0.00019s latency).  
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)  
Nmap scan report for 10.0.2.3  
Host is up (0.00019s latency).  
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)  
Nmap scan report for 10.0.2.4  
Host is up (0.00018s latency).  
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)  
Nmap scan report for 10.0.2.15  
Host is up.  
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.00 seconds

**A default Syn Scan:**

﻿

**root@kali**:**~**# nmap -sS 10.0.2.0/24  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-06 22:29 EST  
Nmap scan report for 10.0.2.2  
Host is up (1.0s latency).  
Not shown: 997 closed ports  
PORT STATE SERVICE  
135/tcp open msrpc  
445/tcp open microsoft-ds  
65000/tcp filtered unknown  
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)  
  
Nmap scan report for 10.0.2.3  
Host is up (1.0s latency).  
Not shown: 997 closed ports  
PORT STATE SERVICE  
135/tcp open msrpc  
445/tcp open microsoft-ds  
65000/tcp filtered unknown  
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)  
  
Nmap scan report for 10.0.2.4  
Host is up (1.0s latency).  
Not shown: 997 closed ports  
PORT STATE SERVICE  
135/tcp open msrpc  
445/tcp open microsoft-ds  
65000/tcp filtered unknown  
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)  
  
Nmap scan report for 10.0.2.15  
Host is up (0.0000020s latency).  
All 1000 scanned ports on 10.0.2.15 are closed  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 68.62 seconds

﻿**OS detection nmap scan on ports 0-65535 with a metasploitable scan for vulnerabilities also saving those scans to xml, grep, and txt files. Like you did in your example:**

**root@kali**:**~**# nmap -A -p 0-65535 -n -oA nmap metasploitable\_scan2 10.0.2.2  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-05 15:10 EST  
Stats: 0:16:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 96.49% done; ETC: 15:27 (0:00:37 remaining)  
Nmap scan report for metasploitable (198.105.244.23)  
Host is up (0.033s latency).  
Other addresses for metasploitable (not scanned): 198.105.254.23  
Not shown: 65535 filtered ports  
PORT STATE SERVICE VERSION  
80/tcp open http nginx  
| http-robots.txt: 1 disallowed entry   
|\_/  
|\_http-server-header: nginx  
|\_http-title: Site doesn't have a title (text/html).  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: bridge  
Running: Oracle Virtualbox  
OS CPE: cpe:/o:oracle:virtualbox  
OS details: Oracle Virtualbox  
Network Distance: 2 hops  
  
TRACEROUTE (using port 80/tcp)  
HOP RTT ADDRESS  
1 4.43 ms 10.0.2.2  
2 4.45 ms 198.105.244.23  
  
Nmap scan report for 10.0.2.2  
Host is up (0.044s latency).  
Not shown: 65508 closed ports  
PORT STATE SERVICE VERSION  
0/tcp filtered unknown  
135/tcp open msrpc Microsoft Windows RPC  
137/tcp filtered netbios-ns  
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds  
1120/tcp open unknown  
1241/tcp open ssl/nessus Nessus Daemon (NTP v1.2)  
| ssl-cert: Subject: commonName=DESKTOP-JKTTIDP/organizationName=Nessus Users United/stateOrProvinceName=NY/countryName=US  
| Not valid before: 2016-09-10T19:43:17  
|\_Not valid after: 2020-09-09T19:43:17  
|\_ssl-date: TLS randomness does not represent time  
3648/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|\_http-server-header: Microsoft-HTTPAPI/2.0  
|\_http-title: Not Found  
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|\_http-server-header: Microsoft-HTTPAPI/2.0  
|\_http-title: Service Unavailable  
7779/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|\_http-server-header: Microsoft-HTTPAPI/2.0  
|\_http-title: Not Found  
8834/tcp open ssl/unknown  
| ssl-cert: Subject: commonName=DESKTOP-JKTTIDP/organizationName=Nessus Users United/stateOrProvinceName=NY/countryName=US  
| Not valid before: 2016-09-10T19:43:17  
|\_Not valid after: 2020-09-09T19:43:17  
|\_ssl-date: TLS randomness does not represent time  
9990/tcp open osm-appsrvr?  
27036/tcp open ssl/steam Valve Steam In-Home Streaming service (TLSv1.2 PSK)  
47984/tcp open unknown  
47989/tcp open http Mongoose httpd  
|\_http-title: Site doesn't have a title.  
48010/tcp open rtsp?  
|\_rtsp-methods: ERROR: Script execution failed (use -d to debug)  
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  
49670/tcp open msrpc Microsoft Windows RPC  
49672/tcp open ssl/unknown  
| ssl-cert: Subject: commonName=DESKTOP-JKTTIDP/organizationName=Nessus Users United/stateOrProvinceName=NY/countryName=US  
| Not valid before: 2016-09-10T19:43:17  
|\_Not valid after: 2020-09-09T19:43:17  
|\_ssl-date: TLS randomness does not represent time  
49678/tcp open msrpc Microsoft Windows RPC  
49822/tcp open ssl/unknown  
| ssl-cert: Subject: commonName=localbattle.net  
| Not valid before: 2016-06-17T14:29:38  
|\_Not valid after: 2017-06-17T14:29:38  
|\_ssl-date: TLS randomness does not represent time  
54767/tcp open tcpwrapped  
59879/tcp open unknown  
62522/tcp open unknown  
65000/tcp filtered unknown  
65001/tcp open tcpwrapped  
7 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-Port1120-TCP:V=7.25BETA2%I=7%D=2/5%Time=589794D7%P=x86\_64-pc-linux-gnu%  
SF:r(GetRequest,32,"HTTP/1\.0\x20401\x20Unauthorized\r\nContent-Length:\x2  
SF:02\r\n\r\n{}")%r(FourOhFourRequest,32,"HTTP/1\.0\x20401\x20Unauthorized  
SF:\r\nContent-Length:\x202\r\n\r\n{}");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port8834-TCP:V=7.25BETA2%T=SSL%I=7%D=2/5%Time=589794FE%P=x86\_64-pc-linu  
SF:x-gnu%r(GetRequest,2F93,"HTTP/1\.1\x20200\x20OK\r\nCache-Control:\x20\r  
SF:\nX-Frame-Options:\x20DENY\r\nEtag:\x202e4d643a7bcd8715c25971121312c559  
SF:\r\nContent-Type:\x20text/html\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x2020  
SF:17\x2021:11:26\x20GMT\r\nConnection:\x20close\r\nServer:\x20NessusWWW\r  
SF:\nContent-Length:\x2011933\r\nExpires:\x200\r\nPragma:\x20\r\n\r\n<!doc  
SF:type\x20html>\n<html\x20lang=\"en\">\n\x20\x20\x20\x20<head>\n\x20\x20\  
SF:x20\x20\x20\x20\x20\x20<meta\x20http-equiv=\"X-UA-Compatible\"\x20conte  
SF:nt=\"IE=edge,chrome=1\"\x20/>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x2  
SF:0charset=\"utf-8\"\x20/>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20name  
SF:=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=1\.0,\x  
SF:20maximum-scale=1\.0,\x20user-scalable=0\"\x20/>\n\x20\x20\x20\x20\x20\  
SF:x20\x20\x20<meta\x20name=\"apple-mobile-web-app-capable\"\x20content=\"  
SF:yes\"\x20/>\n\x20\x20\x20\x20\x20\x20\x20\x20<link\x20rel=\"apple-touch  
SF:-icon\"\x20href=\"data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAJgAAAC  
SF:YCAIAAACXoLd2AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAAAyNpVF  
SF:h0WE1MOmNvbS5hZG9iZS54bXAAAAAAADw/eHBhY2tldCBiZWdpbj0i77u/IiBpZD0iVzVNM  
SF:E1wQ2VoaUh6cmVTek5UY3prYzlkIj8\+IDx4OnhtcG1ldGEgeG1sbnM6eD0iYWRvYmU6bnM  
SF:6bWV0YS8iIHg")%r(HTTPOptions,83,"HTTP/1\.1\x20405\x20Method\x20not\x20A  
SF:llowed\r\nConnection:\x20close\r\nContent-Length:\x200\r\nServer:\x20Ne  
SF:ssusWWW\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2021:11:26\x20GMT\r  
SF:\n\r\n")%r(RTSPRequest,7C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnec  
SF:tion:\x20close\r\nContent-Length:\x200\r\nServer:\x20NessusWWW\r\nDate:  
SF:\x20:\x20Sun,\x2005\x20Feb\x202017\x2021:11:26\x20GMT\r\n\r\n")%r(Help,  
SF:7C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\nConte  
SF:nt-Length:\x200\r\nServer:\x20NessusWWW\r\nDate:\x20:\x20Sun,\x2005\x20  
SF:Feb\x202017\x2021:11:41\x20GMT\r\n\r\n")%r(FourOhFourRequest,10A,"HTTP/  
SF:1\.1\x20404\x20File\x20not\x20found\r\nCache-Control:\x20\r\nX-Frame-Op  
SF:tions:\x20DENY\r\nContent-Type:\x20application/json\r\nDate:\x20:\x20Su  
SF:n,\x2005\x20Feb\x202017\x2021:12:06\x20GMT\r\nConnection:\x20close\r\nS  
SF:erver:\x20NessusWWW\r\nContent-Length:\x2044\r\nExpires:\x200\r\nPragma  
SF::\x20\r\n\r\n{\"error\":\"The\x20requested\x20file\x20was\x20not\x20fou  
SF:nd\"}");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port9990-TCP:V=7.25BETA2%I=7%D=2/5%Time=589794DC%P=x86\_64-pc-linux-gnu%  
SF:r(GenericLines,24,"\x20\0\0\0\xc2>\x1d\n\x1bReceived\x20an\x20unknown\x  
SF:20request")%r(GetRequest,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20pars  
SF:e\x20the\x20request\.")%r(HTTPOptions,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\  
SF:x20to\x20parse\x20the\x20request\.")%r(RTSPRequest,25,"!\0\0\0\xc2>\x1e  
SF:\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(RPCCheck,25,"!\0\0\  
SF:0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(DNSVersio  
SF:nBindReq,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20requ  
SF:est\.")%r(DNSStatusRequest,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20pa  
SF:rse\x20the\x20request\.")%r(Help,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to  
SF:\x20parse\x20the\x20request\.")%r(SSLSessionReq,25,"!\0\0\0\xc2>\x1e\n\  
SF:x1cFailed\x20to\x20parse\x20the\x20request\.")%r(TLSSessionReq,25,"!\0\  
SF:0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(Kerbero  
SF:s,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")  
SF:%r(SMBProgNeg,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x2  
SF:0request\.")%r(X11Probe,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse  
SF:\x20the\x20request\.")%r(FourOhFourRequest,25,"!\0\0\0\xc2>\x1e\n\x1cFa  
SF:iled\x20to\x20parse\x20the\x20request\.")%r(LPDString,25,"!\0\0\0\xc2>\  
SF:x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(LDAPSearchReq,25  
SF:,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(L  
SF:DAPBindReq,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20re  
SF:quest\.")%r(SIPOptions,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\  
SF:x20the\x20request\.")%r(LANDesk-RC,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20  
SF:to\x20parse\x20the\x20request\.")%r(TerminalServer,25,"!\0\0\0\xc2>\x1e  
SF:\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(NCP,25,"!\0\0\0\xc2  
SF:>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(NotesRPC,25,"!  
SF:\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(WMSR  
SF:equest,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20reques  
SF:t\.")%r(oracle-tns,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20t  
SF:he\x20request\.")%r(afp,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse  
SF:\x20the\x20request\.");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port48010-TCP:V=7.25BETA2%I=7%D=2/5%Time=589794D7%P=x86\_64-pc-linux-gnu  
SF:%r(GenericLines,6E,"RTSP/1\.0\x20500\x20Server\x20Error\r\nContent-Leng  
SF:th:\x2042\r\nConnection:\x20close\r\n\r\nError\x20500:\x20Server\x20Err  
SF:or\nBad\x20request:\x20\[\r\n\r\]")%r(GetRequest,6E,"RTSP/1\.0\x20500\x  
SF:20Server\x20Error\r\nContent-Length:\x2042\r\nConnection:\x20close\r\n\  
SF:r\nError\x20500:\x20Server\x20Error\nBad\x20request:\x20\[GET\]")%r(HTT  
SF:POptions,72,"RTSP/1\.0\x20500\x20Server\x20Error\r\nContent-Length:\x20  
SF:46\r\nConnection:\x20close\r\n\r\nError\x20500:\x20Server\x20Error\nBad  
SF:\x20request:\x20\[OPTIONS\]");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port49672-TCP:V=7.25BETA2%T=SSL%I=7%D=2/5%Time=589794FE%P=x86\_64-pc-lin  
SF:ux-gnu%r(GetRequest,10A,"HTTP/1\.1\x20404\x20File\x20not\x20found\r\nCa  
SF:che-Control:\x20\r\nX-Frame-Options:\x20DENY\r\nContent-Type:\x20applic  
SF:ation/json\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2021:11:26\x20GM  
SF:T\r\nConnection:\x20close\r\nServer:\x20NessusWWW\r\nContent-Length:\x2  
SF:044\r\nExpires:\x200\r\nPragma:\x20\r\n\r\n{\"error\":\"The\x20requeste  
SF:d\x20file\x20was\x20not\x20found\"}")%r(HTTPOptions,83,"HTTP/1\.1\x2040  
SF:5\x20Method\x20not\x20Allowed\r\nConnection:\x20close\r\nContent-Length  
SF::\x200\r\nServer:\x20NessusWWW\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x2020  
SF:17\x2021:11:26\x20GMT\r\n\r\n")%r(RTSPRequest,7C,"HTTP/1\.1\x20400\x20B  
SF:ad\x20Request\r\nConnection:\x20close\r\nContent-Length:\x200\r\nServer  
SF::\x20NessusWWW\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2021:11:26\x  
SF:20GMT\r\n\r\n")%r(Help,7C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnec  
SF:tion:\x20close\r\nContent-Length:\x200\r\nServer:\x20NessusWWW\r\nDate:  
SF:\x20:\x20Sun,\x2005\x20Feb\x202017\x2021:11:41\x20GMT\r\n\r\n")%r(FourO  
SF:hFourRequest,10A,"HTTP/1\.1\x20404\x20File\x20not\x20found\r\nCache-Con  
SF:trol:\x20\r\nX-Frame-Options:\x20DENY\r\nContent-Type:\x20application/j  
SF:son\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2021:12:06\x20GMT\r\nCo  
SF:nnection:\x20close\r\nServer:\x20NessusWWW\r\nContent-Length:\x2044\r\n  
SF:Expires:\x200\r\nPragma:\x20\r\n\r\n{\"error\":\"The\x20requested\x20fi  
SF:le\x20was\x20not\x20found\"}")%r(SIPOptions,7C,"HTTP/1\.1\x20400\x20Bad  
SF:\x20Request\r\nConnection:\x20close\r\nContent-Length:\x200\r\nServer:\  
SF:x20NessusWWW\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2021:12:21\x20  
SF:GMT\r\n\r\n");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port49822-TCP:V=7.25BETA2%T=SSL%I=7%D=2/5%Time=589794F0%P=x86\_64-pc-lin  
SF:ux-gnu%r(GenericLines,69,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nConnect  
SF:ion:\x20close\r\nContent-Type:\x20text/plain\r\nContent-Length:\x2012\r  
SF:\n\r\nBad\x20Request\.")%r(GetRequest,71,"HTTP/1\.1\x20404\x20Not\x20Fo  
SF:und\r\nConnection:\x20close\r\nContent-Length:\x209\r\nContent-Type:\x2  
SF:0text/html;\x20charset=UTF-8\r\n\r\nNot\x20found")%r(HTTPOptions,7E,"HT  
SF:TP/1\.1\x20501\x20Not\x20Implemented\r\nConnection:\x20close\r\nContent  
SF:-Length:\x2015\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\n\r\nN  
SF:ot\x20implemented")%r(RTSPRequest,69,"HTTP/1\.0\x20400\x20Bad\x20Reques  
SF:t\r\nConnection:\x20close\r\nContent-Type:\x20text/plain\r\nContent-Len  
SF:gth:\x2012\r\n\r\nBad\x20Request\.")%r(RPCCheck,69,"HTTP/1\.0\x20400\x2  
SF:0Bad\x20Request\r\nConnection:\x20close\r\nContent-Type:\x20text/plain\  
SF:r\nContent-Length:\x2012\r\n\r\nBad\x20Request\.")%r(DNSVersionBindReq,  
SF:69,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\nConte  
SF:nt-Type:\x20text/plain\r\nContent-Length:\x2012\r\n\r\nBad\x20Request\.  
SF:")%r(DNSStatusRequest,69,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nConnect  
SF:ion:\x20close\r\nContent-Type:\x20text/plain\r\nContent-Length:\x2012\r  
SF:\n\r\nBad\x20Request\.")%r(Help,69,"HTTP/1\.0\x20400\x20Bad\x20Request\  
SF:r\nConnection:\x20close\r\nContent-Type:\x20text/plain\r\nContent-Lengt  
SF:h:\x2012\r\n\r\nBad\x20Request\.")%r(SSLSessionReq,69,"HTTP/1\.0\x20400  
SF:\x20Bad\x20Request\r\nConnection:\x20close\r\nContent-Type:\x20text/pla  
SF:in\r\nContent-Length:\x2012\r\n\r\nBad\x20Request\.")%r(Kerberos,69,"HT  
SF:TP/1\.0\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\nContent-Typ  
SF:e:\x20text/plain\r\nContent-Length:\x2012\r\n\r\nBad\x20Request\.")%r(S  
SF:MBProgNeg,69,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nConnection:\x20clos  
SF:e\r\nContent-Type:\x20text/plain\r\nContent-Length:\x2012\r\n\r\nBad\x2  
SF:0Request\.")%r(FourOhFourRequest,71,"HTTP/1\.1\x20404\x20Not\x20Found\r  
SF:\nConnection:\x20close\r\nContent-Length:\x209\r\nContent-Type:\x20text  
SF:/html;\x20charset=UTF-8\r\n\r\nNot\x20found")%r(LPDString,69,"HTTP/1\.0  
SF:\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\nContent-Type:\x20t  
SF:ext/plain\r\nContent-Length:\x2012\r\n\r\nBad\x20Request\.");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port59879-TCP:V=7.25BETA2%I=7%D=2/5%Time=589794E2%P=x86\_64-pc-linux-gnu  
SF:%r(GetRequest,4B,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Length:\x  
SF:203\r\nContent-Type:\x20text/html\r\n\r\n404\r\n")%r(FourOhFourRequest,  
SF:4B,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Length:\x203\r\nContent  
SF:-Type:\x20text/html\r\n\r\n404\r\n");  
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)  
Device type: general purpose  
Running: QEMU  
OS CPE: cpe:/a:qemu:qemu  
OS details: QEMU user mode network gateway  
Network Distance: 1 hop  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|\_clock-skew: mean: -0s, deviation: 0s, median: -0s  
| smb-security-mode:   
| account\_used: guest  
| authentication\_level: user  
| challenge\_response: supported  
|\_ message\_signing: disabled (dangerous, but default)  
|\_smbv2-enabled: Server supports SMBv2 protocol  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 44.44 ms 10.0.2.2  
  
Post-scan script results:  
| clock-skew:   
|\_ -0s: Majority of systems scanned  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 2 IP addresses (2 hosts up) scanned in 3793.16 seconds

**root@kali**:**~**# nmap -A -p 0-65535 -n -oA nmap metasploitable\_scan3 10.0.2.3  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-05 16:17 EST  
Nmap scan report for metasploitable (198.105.244.23)  
Host is up (0.0096s latency).  
Other addresses for metasploitable (not scanned): 198.105.254.23  
Not shown: 65535 filtered ports  
PORT STATE SERVICE VERSION  
80/tcp open http nginx  
| http-robots.txt: 1 disallowed entry   
|\_/  
|\_http-server-header: nginx  
|\_http-title: Site doesn't have a title (text/html).  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: bridge  
Running: Oracle Virtualbox  
OS CPE: cpe:/o:oracle:virtualbox  
OS details: Oracle Virtualbox  
Network Distance: 2 hops  
  
TRACEROUTE (using port 80/tcp)  
HOP RTT ADDRESS  
1 1.28 ms 10.0.2.2  
2 1.33 ms 198.105.244.23  
  
Nmap scan report for 10.0.2.3  
Host is up (0.26s latency).  
Not shown: 65508 closed ports  
PORT STATE SERVICE VERSION  
0/tcp filtered unknown  
135/tcp open msrpc Microsoft Windows RPC  
137/tcp filtered netbios-ns  
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds  
1120/tcp open unknown  
1241/tcp open ssl/nessus Nessus Daemon (NTP v1.2)  
| ssl-cert: Subject: commonName=DESKTOP-JKTTIDP/organizationName=Nessus Users United/stateOrProvinceName=NY/countryName=US  
| Not valid before: 2016-09-10T19:43:17  
|\_Not valid after: 2020-09-09T19:43:17  
|\_ssl-date: TLS randomness does not represent time  
3648/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|\_http-server-header: Microsoft-HTTPAPI/2.0  
|\_http-title: Not Found  
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|\_http-server-header: Microsoft-HTTPAPI/2.0  
|\_http-title: Service Unavailable  
7779/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|\_http-server-header: Microsoft-HTTPAPI/2.0  
|\_http-title: Not Found  
8834/tcp open ssl/unknown  
| ssl-cert: Subject: commonName=DESKTOP-JKTTIDP/organizationName=Nessus Users United/stateOrProvinceName=NY/countryName=US  
| Not valid before: 2016-09-10T19:43:17  
|\_Not valid after: 2020-09-09T19:43:17  
|\_ssl-date: TLS randomness does not represent time  
9990/tcp open osm-appsrvr?  
27036/tcp open ssl/steam Valve Steam In-Home Streaming service (TLSv1.2 PSK)  
47984/tcp open unknown  
47989/tcp open http Mongoose httpd  
|\_http-title: Site doesn't have a title.  
48010/tcp open rtsp?  
|\_rtsp-methods: ERROR: Script execution failed (use -d to debug)  
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  
49670/tcp open msrpc Microsoft Windows RPC  
49678/tcp open msrpc Microsoft Windows RPC  
49822/tcp open ssl/unknown  
| ssl-cert: Subject: commonName=localbattle.net  
| Not valid before: 2016-06-17T14:29:38  
|\_Not valid after: 2017-06-17T14:29:38  
|\_ssl-date: TLS randomness does not represent time  
59879/tcp open unknown  
62110/tcp open tcpwrapped  
62522/tcp open unknown  
64040/tcp open ssl/unknown  
| ssl-cert: Subject: commonName=DESKTOP-JKTTIDP/organizationName=Nessus Users United/stateOrProvinceName=NY/countryName=US  
| Not valid before: 2016-09-10T19:43:17  
|\_Not valid after: 2020-09-09T19:43:17  
|\_ssl-date: TLS randomness does not represent time  
65000/tcp filtered unknown  
65001/tcp open tcpwrapped  
7 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-Port1120-TCP:V=7.25BETA2%I=7%D=2/5%Time=5897A331%P=x86\_64-pc-linux-gnu%  
SF:r(GetRequest,32,"HTTP/1\.0\x20401\x20Unauthorized\r\nContent-Length:\x2  
SF:02\r\n\r\n{}")%r(FourOhFourRequest,32,"HTTP/1\.0\x20401\x20Unauthorized  
SF:\r\nContent-Length:\x202\r\n\r\n{}");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port8834-TCP:V=7.25BETA2%T=SSL%I=7%D=2/5%Time=5897A358%P=x86\_64-pc-linu  
SF:x-gnu%r(GetRequest,2F93,"HTTP/1\.1\x20200\x20OK\r\nCache-Control:\x20\r  
SF:\nX-Frame-Options:\x20DENY\r\nEtag:\x202e4d643a7bcd8715c25971121312c559  
SF:\r\nContent-Type:\x20text/html\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x2020  
SF:17\x2022:12:40\x20GMT\r\nConnection:\x20close\r\nServer:\x20NessusWWW\r  
SF:\nContent-Length:\x2011933\r\nExpires:\x200\r\nPragma:\x20\r\n\r\n<!doc  
SF:type\x20html>\n<html\x20lang=\"en\">\n\x20\x20\x20\x20<head>\n\x20\x20\  
SF:x20\x20\x20\x20\x20\x20<meta\x20http-equiv=\"X-UA-Compatible\"\x20conte  
SF:nt=\"IE=edge,chrome=1\"\x20/>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x2  
SF:0charset=\"utf-8\"\x20/>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20name  
SF:=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=1\.0,\x  
SF:20maximum-scale=1\.0,\x20user-scalable=0\"\x20/>\n\x20\x20\x20\x20\x20\  
SF:x20\x20\x20<meta\x20name=\"apple-mobile-web-app-capable\"\x20content=\"  
SF:yes\"\x20/>\n\x20\x20\x20\x20\x20\x20\x20\x20<link\x20rel=\"apple-touch  
SF:-icon\"\x20href=\"data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAJgAAAC  
SF:YCAIAAACXoLd2AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAAAyNpVF  
SF:h0WE1MOmNvbS5hZG9iZS54bXAAAAAAADw/eHBhY2tldCBiZWdpbj0i77u/IiBpZD0iVzVNM  
SF:E1wQ2VoaUh6cmVTek5UY3prYzlkIj8\+IDx4OnhtcG1ldGEgeG1sbnM6eD0iYWRvYmU6bnM  
SF:6bWV0YS8iIHg")%r(HTTPOptions,83,"HTTP/1\.1\x20405\x20Method\x20not\x20A  
SF:llowed\r\nConnection:\x20close\r\nContent-Length:\x200\r\nServer:\x20Ne  
SF:ssusWWW\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2022:12:40\x20GMT\r  
SF:\n\r\n")%r(RTSPRequest,7C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnec  
SF:tion:\x20close\r\nContent-Length:\x200\r\nServer:\x20NessusWWW\r\nDate:  
SF:\x20:\x20Sun,\x2005\x20Feb\x202017\x2022:12:40\x20GMT\r\n\r\n")%r(Help,  
SF:7C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\nConte  
SF:nt-Length:\x200\r\nServer:\x20NessusWWW\r\nDate:\x20:\x20Sun,\x2005\x20  
SF:Feb\x202017\x2022:12:55\x20GMT\r\n\r\n")%r(FourOhFourRequest,10A,"HTTP/  
SF:1\.1\x20404\x20File\x20not\x20found\r\nCache-Control:\x20\r\nX-Frame-Op  
SF:tions:\x20DENY\r\nContent-Type:\x20application/json\r\nDate:\x20:\x20Su  
SF:n,\x2005\x20Feb\x202017\x2022:13:20\x20GMT\r\nConnection:\x20close\r\nS  
SF:erver:\x20NessusWWW\r\nContent-Length:\x2044\r\nExpires:\x200\r\nPragma  
SF::\x20\r\n\r\n{\"error\":\"The\x20requested\x20file\x20was\x20not\x20fou  
SF:nd\"}");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port9990-TCP:V=7.25BETA2%I=7%D=2/5%Time=5897A336%P=x86\_64-pc-linux-gnu%  
SF:r(GenericLines,24,"\x20\0\0\0\xc2>\x1d\n\x1bReceived\x20an\x20unknown\x  
SF:20request")%r(GetRequest,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20pars  
SF:e\x20the\x20request\.")%r(HTTPOptions,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\  
SF:x20to\x20parse\x20the\x20request\.")%r(RTSPRequest,25,"!\0\0\0\xc2>\x1e  
SF:\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(RPCCheck,25,"!\0\0\  
SF:0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(DNSVersio  
SF:nBindReq,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20requ  
SF:est\.")%r(DNSStatusRequest,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20pa  
SF:rse\x20the\x20request\.")%r(Help,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to  
SF:\x20parse\x20the\x20request\.")%r(SSLSessionReq,25,"!\0\0\0\xc2>\x1e\n\  
SF:x1cFailed\x20to\x20parse\x20the\x20request\.")%r(TLSSessionReq,25,"!\0\  
SF:0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(Kerbero  
SF:s,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")  
SF:%r(SMBProgNeg,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x2  
SF:0request\.")%r(X11Probe,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse  
SF:\x20the\x20request\.")%r(FourOhFourRequest,25,"!\0\0\0\xc2>\x1e\n\x1cFa  
SF:iled\x20to\x20parse\x20the\x20request\.")%r(LPDString,25,"!\0\0\0\xc2>\  
SF:x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(LDAPSearchReq,25  
SF:,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(L  
SF:DAPBindReq,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20re  
SF:quest\.")%r(SIPOptions,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\  
SF:x20the\x20request\.")%r(LANDesk-RC,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20  
SF:to\x20parse\x20the\x20request\.")%r(TerminalServer,25,"!\0\0\0\xc2>\x1e  
SF:\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(NCP,25,"!\0\0\0\xc2  
SF:>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(NotesRPC,25,"!  
SF:\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(WMSR  
SF:equest,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20reques  
SF:t\.")%r(oracle-tns,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20t  
SF:he\x20request\.")%r(afp,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse  
SF:\x20the\x20request\.");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port48010-TCP:V=7.25BETA2%I=7%D=2/5%Time=5897A331%P=x86\_64-pc-linux-gnu  
SF:%r(GenericLines,6E,"RTSP/1\.0\x20500\x20Server\x20Error\r\nContent-Leng  
SF:th:\x2042\r\nConnection:\x20close\r\n\r\nError\x20500:\x20Server\x20Err  
SF:or\nBad\x20request:\x20\[\r\n\r\]")%r(GetRequest,6E,"RTSP/1\.0\x20500\x  
SF:20Server\x20Error\r\nContent-Length:\x2042\r\nConnection:\x20close\r\n\  
SF:r\nError\x20500:\x20Server\x20Error\nBad\x20request:\x20\[GET\]")%r(HTT  
SF:POptions,72,"RTSP/1\.0\x20500\x20Server\x20Error\r\nContent-Length:\x20  
SF:46\r\nConnection:\x20close\r\n\r\nError\x20500:\x20Server\x20Error\nBad  
SF:\x20request:\x20\[OPTIONS\]");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port49822-TCP:V=7.25BETA2%T=SSL%I=7%D=2/5%Time=5897A344%P=x86\_64-pc-lin  
SF:ux-gnu%r(GenericLines,69,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nConnect  
SF:ion:\x20close\r\nContent-Type:\x20text/plain\r\nContent-Length:\x2012\r  
SF:\n\r\nBad\x20Request\.")%r(GetRequest,71,"HTTP/1\.1\x20404\x20Not\x20Fo  
SF:und\r\nConnection:\x20close\r\nContent-Length:\x209\r\nContent-Type:\x2  
SF:0text/html;\x20charset=UTF-8\r\n\r\nNot\x20found")%r(HTTPOptions,7E,"HT  
SF:TP/1\.1\x20501\x20Not\x20Implemented\r\nConnection:\x20close\r\nContent  
SF:-Length:\x2015\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\n\r\nN  
SF:ot\x20implemented")%r(RTSPRequest,69,"HTTP/1\.0\x20400\x20Bad\x20Reques  
SF:t\r\nConnection:\x20close\r\nContent-Type:\x20text/plain\r\nContent-Len  
SF:gth:\x2012\r\n\r\nBad\x20Request\.")%r(DNSStatusRequest,69,"HTTP/1\.0\x  
SF:20400\x20Bad\x20Request\r\nConnection:\x20close\r\nContent-Type:\x20tex  
SF:t/plain\r\nContent-Length:\x2012\r\n\r\nBad\x20Request\.")%r(Help,69,"H  
SF:TTP/1\.0\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\nContent-Ty  
SF:pe:\x20text/plain\r\nContent-Length:\x2012\r\n\r\nBad\x20Request\.")%r(  
SF:SSLSessionReq,69,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nConnection:\x20  
SF:close\r\nContent-Type:\x20text/plain\r\nContent-Length:\x2012\r\n\r\nBa  
SF:d\x20Request\.")%r(TLSSessionReq,69,"HTTP/1\.0\x20400\x20Bad\x20Request  
SF:\r\nConnection:\x20close\r\nContent-Type:\x20text/plain\r\nContent-Leng  
SF:th:\x2012\r\n\r\nBad\x20Request\.")%r(SMBProgNeg,69,"HTTP/1\.0\x20400\x  
SF:20Bad\x20Request\r\nConnection:\x20close\r\nContent-Type:\x20text/plain  
SF:\r\nContent-Length:\x2012\r\n\r\nBad\x20Request\.")%r(FourOhFourRequest  
SF:,71,"HTTP/1\.1\x20404\x20Not\x20Found\r\nConnection:\x20close\r\nConten  
SF:t-Length:\x209\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\n\r\nN  
SF:ot\x20found")%r(LPDString,69,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCon  
SF:nection:\x20close\r\nContent-Type:\x20text/plain\r\nContent-Length:\x20  
SF:12\r\n\r\nBad\x20Request\.")%r(LDAPSearchReq,69,"HTTP/1\.0\x20400\x20Ba  
SF:d\x20Request\r\nConnection:\x20close\r\nContent-Type:\x20text/plain\r\n  
SF:Content-Length:\x2012\r\n\r\nBad\x20Request\.")%r(LDAPBindReq,69,"HTTP/  
SF:1\.0\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\nContent-Type:\  
SF:x20text/plain\r\nContent-Length:\x2012\r\n\r\nBad\x20Request\.");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port59879-TCP:V=7.25BETA2%I=7%D=2/5%Time=5897A33C%P=x86\_64-pc-linux-gnu  
SF:%r(GetRequest,4B,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Length:\x  
SF:203\r\nContent-Type:\x20text/html\r\n\r\n404\r\n")%r(FourOhFourRequest,  
SF:4B,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Length:\x203\r\nContent  
SF:-Type:\x20text/html\r\n\r\n404\r\n");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port64040-TCP:V=7.25BETA2%T=SSL%I=7%D=2/5%Time=5897A35E%P=x86\_64-pc-lin  
SF:ux-gnu%r(GetRequest,10A,"HTTP/1\.1\x20404\x20File\x20not\x20found\r\nCa  
SF:che-Control:\x20\r\nX-Frame-Options:\x20DENY\r\nContent-Type:\x20applic  
SF:ation/json\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2022:12:46\x20GM  
SF:T\r\nConnection:\x20close\r\nServer:\x20NessusWWW\r\nContent-Length:\x2  
SF:044\r\nExpires:\x200\r\nPragma:\x20\r\n\r\n{\"error\":\"The\x20requeste  
SF:d\x20file\x20was\x20not\x20found\"}")%r(HTTPOptions,83,"HTTP/1\.1\x2040  
SF:5\x20Method\x20not\x20Allowed\r\nConnection:\x20close\r\nContent-Length  
SF::\x200\r\nServer:\x20NessusWWW\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x2020  
SF:17\x2022:12:46\x20GMT\r\n\r\n")%r(RTSPRequest,7C,"HTTP/1\.1\x20400\x20B  
SF:ad\x20Request\r\nConnection:\x20close\r\nContent-Length:\x200\r\nServer  
SF::\x20NessusWWW\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2022:12:46\x  
SF:20GMT\r\n\r\n")%r(Help,7C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnec  
SF:tion:\x20close\r\nContent-Length:\x200\r\nServer:\x20NessusWWW\r\nDate:  
SF:\x20:\x20Sun,\x2005\x20Feb\x202017\x2022:13:01\x20GMT\r\n\r\n")%r(FourO  
SF:hFourRequest,10A,"HTTP/1\.1\x20404\x20File\x20not\x20found\r\nCache-Con  
SF:trol:\x20\r\nX-Frame-Options:\x20DENY\r\nContent-Type:\x20application/j  
SF:son\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2022:13:26\x20GMT\r\nCo  
SF:nnection:\x20close\r\nServer:\x20NessusWWW\r\nContent-Length:\x2044\r\n  
SF:Expires:\x200\r\nPragma:\x20\r\n\r\n{\"error\":\"The\x20requested\x20fi  
SF:le\x20was\x20not\x20found\"}")%r(SIPOptions,7C,"HTTP/1\.1\x20400\x20Bad  
SF:\x20Request\r\nConnection:\x20close\r\nContent-Length:\x200\r\nServer:\  
SF:x20NessusWWW\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2022:13:41\x20  
SF:GMT\r\n\r\n");  
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)  
Device type: general purpose  
Running: QEMU  
OS CPE: cpe:/a:qemu:qemu  
OS details: QEMU user mode network gateway  
Network Distance: 1 hop  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|\_clock-skew: mean: -0s, deviation: 0s, median: -0s  
| smb-security-mode:   
| account\_used: guest  
| authentication\_level: user  
| challenge\_response: supported  
|\_ message\_signing: disabled (dangerous, but default)  
|\_smbv2-enabled: Server supports SMBv2 protocol  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 260.86 ms 10.0.2.3  
  
Post-scan script results:  
| clock-skew:   
|\_ -0s: Majority of systems scanned  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 2 IP addresses (2 hosts up) scanned in 3427.74 seconds

﻿

**root@kali**:**~**# nmap -A -p 0-65535 -n -oA nmap metasploitable\_scan4 10.0.2.4  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-05 17:22 EST  
Nmap scan report for metasploitable (198.105.244.23)  
Host is up (0.010s latency).  
Other addresses for metasploitable (not scanned): 198.105.254.23  
Not shown: 65535 filtered ports  
PORT STATE SERVICE VERSION  
80/tcp open http nginx  
| http-robots.txt: 1 disallowed entry   
|\_/  
|\_http-server-header: nginx  
|\_http-title: Site doesn't have a title (text/html).  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: bridge  
Running: Oracle Virtualbox  
OS CPE: cpe:/o:oracle:virtualbox  
OS details: Oracle Virtualbox  
Network Distance: 2 hops  
  
TRACEROUTE (using port 80/tcp)  
HOP RTT ADDRESS  
1 2.08 ms 10.0.2.2  
2 2.05 ms 198.105.244.23  
  
Nmap scan report for 10.0.2.4  
Host is up (0.26s latency).  
Not shown: 65508 closed ports  
PORT STATE SERVICE VERSION  
0/tcp filtered unknown  
135/tcp open msrpc Microsoft Windows RPC  
137/tcp filtered netbios-ns  
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds  
1120/tcp open unknown  
1241/tcp open ssl/nessus Nessus Daemon (NTP v1.2)  
| ssl-cert: Subject: commonName=DESKTOP-JKTTIDP/organizationName=Nessus Users United/stateOrProvinceName=NY/countryName=US  
| Not valid before: 2016-09-10T19:43:17  
|\_Not valid after: 2020-09-09T19:43:17  
|\_ssl-date: TLS randomness does not represent time  
3648/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|\_http-server-header: Microsoft-HTTPAPI/2.0  
|\_http-title: Not Found  
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|\_http-server-header: Microsoft-HTTPAPI/2.0  
|\_http-title: Service Unavailable  
7779/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|\_http-server-header: Microsoft-HTTPAPI/2.0  
|\_http-title: Not Found  
8834/tcp open ssl/unknown  
| ssl-cert: Subject: commonName=DESKTOP-JKTTIDP/organizationName=Nessus Users United/stateOrProvinceName=NY/countryName=US  
| Not valid before: 2016-09-10T19:43:17  
|\_Not valid after: 2020-09-09T19:43:17  
|\_ssl-date: TLS randomness does not represent time  
9990/tcp open osm-appsrvr?  
27036/tcp open ssl/steam Valve Steam In-Home Streaming service (TLSv1.2 PSK)  
47984/tcp open unknown  
47989/tcp open http Mongoose httpd  
|\_http-title: Site doesn't have a title.  
48010/tcp open rtsp?  
|\_rtsp-methods: ERROR: Script execution failed (use -d to debug)  
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  
49670/tcp open msrpc Microsoft Windows RPC  
49678/tcp open msrpc Microsoft Windows RPC  
49822/tcp open ssl/unknown  
| ssl-cert: Subject: commonName=localbattle.net  
| Not valid before: 2016-06-17T14:29:38  
|\_Not valid after: 2017-06-17T14:29:38  
|\_ssl-date: TLS randomness does not represent time  
52027/tcp open tcpwrapped  
59879/tcp open unknown  
62522/tcp open unknown  
64040/tcp open ssl/unknown  
| ssl-cert: Subject: commonName=DESKTOP-JKTTIDP/organizationName=Nessus Users United/stateOrProvinceName=NY/countryName=US  
| Not valid before: 2016-09-10T19:43:17  
|\_Not valid after: 2020-09-09T19:43:17  
|\_ssl-date: TLS randomness does not represent time  
65000/tcp filtered unknown  
65001/tcp open tcpwrapped  
7 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-Port1120-TCP:V=7.25BETA2%I=7%D=2/5%Time=5897B1FC%P=x86\_64-pc-linux-gnu%  
SF:r(GetRequest,32,"HTTP/1\.0\x20401\x20Unauthorized\r\nContent-Length:\x2  
SF:02\r\n\r\n{}")%r(FourOhFourRequest,32,"HTTP/1\.0\x20401\x20Unauthorized  
SF:\r\nContent-Length:\x202\r\n\r\n{}");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port8834-TCP:V=7.25BETA2%T=SSL%I=7%D=2/5%Time=5897B222%P=x86\_64-pc-linu  
SF:x-gnu%r(GetRequest,2F93,"HTTP/1\.1\x20200\x20OK\r\nCache-Control:\x20\r  
SF:\nX-Frame-Options:\x20DENY\r\nEtag:\x202e4d643a7bcd8715c25971121312c559  
SF:\r\nContent-Type:\x20text/html\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x2020  
SF:17\x2023:15:46\x20GMT\r\nConnection:\x20close\r\nServer:\x20NessusWWW\r  
SF:\nContent-Length:\x2011933\r\nExpires:\x200\r\nPragma:\x20\r\n\r\n<!doc  
SF:type\x20html>\n<html\x20lang=\"en\">\n\x20\x20\x20\x20<head>\n\x20\x20\  
SF:x20\x20\x20\x20\x20\x20<meta\x20http-equiv=\"X-UA-Compatible\"\x20conte  
SF:nt=\"IE=edge,chrome=1\"\x20/>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x2  
SF:0charset=\"utf-8\"\x20/>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20name  
SF:=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=1\.0,\x  
SF:20maximum-scale=1\.0,\x20user-scalable=0\"\x20/>\n\x20\x20\x20\x20\x20\  
SF:x20\x20\x20<meta\x20name=\"apple-mobile-web-app-capable\"\x20content=\"  
SF:yes\"\x20/>\n\x20\x20\x20\x20\x20\x20\x20\x20<link\x20rel=\"apple-touch  
SF:-icon\"\x20href=\"data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAJgAAAC  
SF:YCAIAAACXoLd2AAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAAAyNpVF  
SF:h0WE1MOmNvbS5hZG9iZS54bXAAAAAAADw/eHBhY2tldCBiZWdpbj0i77u/IiBpZD0iVzVNM  
SF:E1wQ2VoaUh6cmVTek5UY3prYzlkIj8\+IDx4OnhtcG1ldGEgeG1sbnM6eD0iYWRvYmU6bnM  
SF:6bWV0YS8iIHg")%r(HTTPOptions,83,"HTTP/1\.1\x20405\x20Method\x20not\x20A  
SF:llowed\r\nConnection:\x20close\r\nContent-Length:\x200\r\nServer:\x20Ne  
SF:ssusWWW\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2023:15:46\x20GMT\r  
SF:\n\r\n")%r(RTSPRequest,7C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnec  
SF:tion:\x20close\r\nContent-Length:\x200\r\nServer:\x20NessusWWW\r\nDate:  
SF:\x20:\x20Sun,\x2005\x20Feb\x202017\x2023:15:46\x20GMT\r\n\r\n")%r(Help,  
SF:7C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\nConte  
SF:nt-Length:\x200\r\nServer:\x20NessusWWW\r\nDate:\x20:\x20Sun,\x2005\x20  
SF:Feb\x202017\x2023:16:01\x20GMT\r\n\r\n")%r(FourOhFourRequest,10A,"HTTP/  
SF:1\.1\x20404\x20File\x20not\x20found\r\nCache-Control:\x20\r\nX-Frame-Op  
SF:tions:\x20DENY\r\nContent-Type:\x20application/json\r\nDate:\x20:\x20Su  
SF:n,\x2005\x20Feb\x202017\x2023:16:26\x20GMT\r\nConnection:\x20close\r\nS  
SF:erver:\x20NessusWWW\r\nContent-Length:\x2044\r\nExpires:\x200\r\nPragma  
SF::\x20\r\n\r\n{\"error\":\"The\x20requested\x20file\x20was\x20not\x20fou  
SF:nd\"}");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port9990-TCP:V=7.25BETA2%I=7%D=2/5%Time=5897B201%P=x86\_64-pc-linux-gnu%  
SF:r(GenericLines,24,"\x20\0\0\0\xc2>\x1d\n\x1bReceived\x20an\x20unknown\x  
SF:20request")%r(GetRequest,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20pars  
SF:e\x20the\x20request\.")%r(HTTPOptions,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\  
SF:x20to\x20parse\x20the\x20request\.")%r(RTSPRequest,25,"!\0\0\0\xc2>\x1e  
SF:\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(RPCCheck,25,"!\0\0\  
SF:0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(DNSVersio  
SF:nBindReq,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20requ  
SF:est\.")%r(DNSStatusRequest,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20pa  
SF:rse\x20the\x20request\.")%r(Help,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to  
SF:\x20parse\x20the\x20request\.")%r(SSLSessionReq,25,"!\0\0\0\xc2>\x1e\n\  
SF:x1cFailed\x20to\x20parse\x20the\x20request\.")%r(TLSSessionReq,25,"!\0\  
SF:0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(Kerbero  
SF:s,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")  
SF:%r(SMBProgNeg,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x2  
SF:0request\.")%r(X11Probe,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse  
SF:\x20the\x20request\.")%r(FourOhFourRequest,25,"!\0\0\0\xc2>\x1e\n\x1cFa  
SF:iled\x20to\x20parse\x20the\x20request\.")%r(LPDString,25,"!\0\0\0\xc2>\  
SF:x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(LDAPSearchReq,25  
SF:,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(L  
SF:DAPBindReq,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20re  
SF:quest\.")%r(SIPOptions,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\  
SF:x20the\x20request\.")%r(LANDesk-RC,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20  
SF:to\x20parse\x20the\x20request\.")%r(TerminalServer,25,"!\0\0\0\xc2>\x1e  
SF:\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(NCP,25,"!\0\0\0\xc2  
SF:>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(NotesRPC,25,"!  
SF:\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20request\.")%r(WMSR  
SF:equest,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20the\x20reques  
SF:t\.")%r(oracle-tns,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse\x20t  
SF:he\x20request\.")%r(afp,25,"!\0\0\0\xc2>\x1e\n\x1cFailed\x20to\x20parse  
SF:\x20the\x20request\.");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port48010-TCP:V=7.25BETA2%I=7%D=2/5%Time=5897B1FC%P=x86\_64-pc-linux-gnu  
SF:%r(GenericLines,6E,"RTSP/1\.0\x20500\x20Server\x20Error\r\nContent-Leng  
SF:th:\x2042\r\nConnection:\x20close\r\n\r\nError\x20500:\x20Server\x20Err  
SF:or\nBad\x20request:\x20\[\r\n\r\]")%r(GetRequest,6E,"RTSP/1\.0\x20500\x  
SF:20Server\x20Error\r\nContent-Length:\x2042\r\nConnection:\x20close\r\n\  
SF:r\nError\x20500:\x20Server\x20Error\nBad\x20request:\x20\[GET\]")%r(HTT  
SF:POptions,72,"RTSP/1\.0\x20500\x20Server\x20Error\r\nContent-Length:\x20  
SF:46\r\nConnection:\x20close\r\n\r\nError\x20500:\x20Server\x20Error\nBad  
SF:\x20request:\x20\[OPTIONS\]");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port49822-TCP:V=7.25BETA2%T=SSL%I=7%D=2/5%Time=5897B20E%P=x86\_64-pc-lin  
SF:ux-gnu%r(GetRequest,71,"HTTP/1\.1\x20404\x20Not\x20Found\r\nConnection:  
SF:\x20close\r\nContent-Length:\x209\r\nContent-Type:\x20text/html;\x20cha  
SF:rset=UTF-8\r\n\r\nNot\x20found")%r(HTTPOptions,7E,"HTTP/1\.1\x20501\x20  
SF:Not\x20Implemented\r\nConnection:\x20close\r\nContent-Length:\x2015\r\n  
SF:Content-Type:\x20text/html;\x20charset=UTF-8\r\n\r\nNot\x20implemented"  
SF:)%r(RPCCheck,69,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nConnection:\x20c  
SF:lose\r\nContent-Type:\x20text/plain\r\nContent-Length:\x2012\r\n\r\nBad  
SF:\x20Request\.")%r(DNSStatusRequest,69,"HTTP/1\.0\x20400\x20Bad\x20Reque  
SF:st\r\nConnection:\x20close\r\nContent-Type:\x20text/plain\r\nContent-Le  
SF:ngth:\x2012\r\n\r\nBad\x20Request\.")%r(FourOhFourRequest,71,"HTTP/1\.1  
SF:\x20404\x20Not\x20Found\r\nConnection:\x20close\r\nContent-Length:\x209  
SF:\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\n\r\nNot\x20found")%  
SF:r(LPDString,69,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nConnection:\x20cl  
SF:ose\r\nContent-Type:\x20text/plain\r\nContent-Length:\x2012\r\n\r\nBad\  
SF:x20Request\.")%r(LDAPBindReq,69,"HTTP/1\.0\x20400\x20Bad\x20Request\r\n  
SF:Connection:\x20close\r\nContent-Type:\x20text/plain\r\nContent-Length:\  
SF:x2012\r\n\r\nBad\x20Request\.")%r(SIPOptions,69,"HTTP/1\.0\x20400\x20Ba  
SF:d\x20Request\r\nConnection:\x20close\r\nContent-Type:\x20text/plain\r\n  
SF:Content-Length:\x2012\r\n\r\nBad\x20Request\.")%r(LANDesk-RC,69,"HTTP/1  
SF:\.0\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\nContent-Type:\x  
SF:20text/plain\r\nContent-Length:\x2012\r\n\r\nBad\x20Request\.")%r(Termi  
SF:nalServer,69,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nConnection:\x20clos  
SF:e\r\nContent-Type:\x20text/plain\r\nContent-Length:\x2012\r\n\r\nBad\x2  
SF:0Request\.")%r(oracle-tns,69,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCon  
SF:nection:\x20close\r\nContent-Type:\x20text/plain\r\nContent-Length:\x20  
SF:12\r\n\r\nBad\x20Request\.");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port59879-TCP:V=7.25BETA2%I=7%D=2/5%Time=5897B207%P=x86\_64-pc-linux-gnu  
SF:%r(GetRequest,4B,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Length:\x  
SF:203\r\nContent-Type:\x20text/html\r\n\r\n404\r\n")%r(FourOhFourRequest,  
SF:4B,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Length:\x203\r\nContent  
SF:-Type:\x20text/html\r\n\r\n404\r\n");  
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============  
SF-Port64040-TCP:V=7.25BETA2%T=SSL%I=7%D=2/5%Time=5897B228%P=x86\_64-pc-lin  
SF:ux-gnu%r(GetRequest,10A,"HTTP/1\.1\x20404\x20File\x20not\x20found\r\nCa  
SF:che-Control:\x20\r\nX-Frame-Options:\x20DENY\r\nContent-Type:\x20applic  
SF:ation/json\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2023:15:52\x20GM  
SF:T\r\nConnection:\x20close\r\nServer:\x20NessusWWW\r\nContent-Length:\x2  
SF:044\r\nExpires:\x200\r\nPragma:\x20\r\n\r\n{\"error\":\"The\x20requeste  
SF:d\x20file\x20was\x20not\x20found\"}")%r(HTTPOptions,83,"HTTP/1\.1\x2040  
SF:5\x20Method\x20not\x20Allowed\r\nConnection:\x20close\r\nContent-Length  
SF::\x200\r\nServer:\x20NessusWWW\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x2020  
SF:17\x2023:15:52\x20GMT\r\n\r\n")%r(RTSPRequest,7C,"HTTP/1\.1\x20400\x20B  
SF:ad\x20Request\r\nConnection:\x20close\r\nContent-Length:\x200\r\nServer  
SF::\x20NessusWWW\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2023:15:52\x  
SF:20GMT\r\n\r\n")%r(Help,7C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnec  
SF:tion:\x20close\r\nContent-Length:\x200\r\nServer:\x20NessusWWW\r\nDate:  
SF:\x20:\x20Sun,\x2005\x20Feb\x202017\x2023:16:07\x20GMT\r\n\r\n")%r(FourO  
SF:hFourRequest,10A,"HTTP/1\.1\x20404\x20File\x20not\x20found\r\nCache-Con  
SF:trol:\x20\r\nX-Frame-Options:\x20DENY\r\nContent-Type:\x20application/j  
SF:son\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2023:16:32\x20GMT\r\nCo  
SF:nnection:\x20close\r\nServer:\x20NessusWWW\r\nContent-Length:\x2044\r\n  
SF:Expires:\x200\r\nPragma:\x20\r\n\r\n{\"error\":\"The\x20requested\x20fi  
SF:le\x20was\x20not\x20found\"}")%r(SIPOptions,7C,"HTTP/1\.1\x20400\x20Bad  
SF:\x20Request\r\nConnection:\x20close\r\nContent-Length:\x200\r\nServer:\  
SF:x20NessusWWW\r\nDate:\x20:\x20Sun,\x2005\x20Feb\x202017\x2023:16:47\x20  
SF:GMT\r\n\r\n");  
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)  
Device type: general purpose  
Running: QEMU  
OS CPE: cpe:/a:qemu:qemu  
OS details: QEMU user mode network gateway  
Network Distance: 1 hop  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|\_clock-skew: mean: -0s, deviation: 0s, median: -0s  
| smb-security-mode:   
| account\_used: guest  
| authentication\_level: user  
| challenge\_response: supported  
|\_ message\_signing: disabled (dangerous, but default)  
|\_smbv2-enabled: Server supports SMBv2 protocol  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 260.96 ms 10.0.2.4  
  
Post-scan script results:  
| clock-skew:   
|\_ -0s: Majority of systems scanned  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 2 IP addresses (2 hosts up) scanned in 3355.89 seconds

**I figured I would run nmap on myself to see what would happen. :)**

﻿

**root@kali**:**~**# nmap -A -p 0-65535 -n -oA nmap metasploitable\_scan\_me 10.0.2.15  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-05 19:10 EST  
Nmap scan report for metasploitable (198.105.244.23)  
Host is up (0.013s latency).  
Other addresses for metasploitable (not scanned): 198.105.254.23  
Not shown: 65535 filtered ports  
PORT STATE SERVICE VERSION  
80/tcp open http nginx  
| http-robots.txt: 1 disallowed entry   
|\_/  
|\_http-server-header: nginx  
|\_http-title: Site doesn't have a title (text/html).  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: bridge  
Running: Oracle Virtualbox  
OS CPE: cpe:/o:oracle:virtualbox  
OS details: Oracle Virtualbox  
Network Distance: 2 hops  
  
TRACEROUTE (using port 80/tcp)  
HOP RTT ADDRESS  
1 1.92 ms 10.0.2.2  
2 2.06 ms 198.105.244.23  
  
Nmap scan report for 10.0.2.15  
Host is up (0.000044s latency).  
All 65536 scanned ports on 10.0.2.15 are closed  
Too many fingerprints match this host to give specific OS details  
Network Distance: 0 hops  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 2 IP addresses (2 hosts up) scanned in 1022.48 seconds

Nmap script scan:

**NMAP Service and Application Version Detection; which tells us what ports are open and what is running on those ports. I know the meta nmap scan you showed us does a more thorough job of this but this scan is alot faster.**

﻿

**root@kali**:**~**# nmap -sV -T4 -F 10.0.2.2  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-05 23:35 EST  
Nmap scan report for 10.0.2.2  
Host is up (1.0s latency).  
Not shown: 97 closed ports  
PORT STATE SERVICE VERSION  
135/tcp open msrpc Microsoft Windows RPC  
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds  
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 13.63 seconds  
**root@kali**:**~**# nmap -sV -T4 -F 10.0.2.3  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-05 23:38 EST  
Nmap scan report for 10.0.2.3  
Host is up (1.0s latency).  
Not shown: 97 closed ports  
PORT STATE SERVICE VERSION  
135/tcp open msrpc Microsoft Windows RPC  
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds  
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 13.64 seconds  
**root@kali**:**~**# nmap -sV -T4 -F 10.0.2.4  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-05 23:38 EST  
Nmap scan report for 10.0.2.4  
Host is up (1.0s latency).  
Not shown: 97 closed ports  
PORT STATE SERVICE VERSION  
135/tcp open msrpc Microsoft Windows RPC  
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds  
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds

**Scanning a range of IP addresses:**

﻿

root@kali:~# nmap 10.0.2.2-4  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-06 14:11 EST  
Nmap scan report for 10.0.2.2  
Host is up (1.0s latency).  
Not shown: 996 closed ports  
PORT STATE SERVICE  
135/tcp open msrpc  
445/tcp open microsoft-ds  
5357/tcp open wsdapi  
65000/tcp filtered unknown  
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)  
  
Nmap scan report for 10.0.2.3  
Host is up (1.0s latency).  
Not shown: 996 closed ports  
PORT STATE SERVICE  
135/tcp open msrpc  
445/tcp open microsoft-ds  
5357/tcp open wsdapi  
65000/tcp filtered unknown  
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)  
  
Nmap scan report for 10.0.2.4  
Host is up (1.0s latency).  
Not shown: 996 closed ports  
PORT STATE SERVICE  
135/tcp open msrpc  
445/tcp open microsoft-ds  
5357/tcp open wsdapi  
65000/tcp filtered unknown  
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)  
  
Nmap done: 3 IP addresses (3 hosts up) scanned in 49.59 seconds

**Ranged Stealth Scanning with a UDP port scan and ignoring the directory:**

**﻿**

root@kali:~# nmap -sS -sU -PN 10.0.2.2-4  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-06 14:33 EST  
Nmap scan report for 10.0.2.2  
Host is up (0.00043s latency).  
Not shown: 1989 closed ports  
PORT STATE SERVICE  
135/tcp open msrpc  
445/tcp open microsoft-ds  
5357/tcp open wsdapi  
65000/tcp filtered unknown  
67/udp open|filtered dhcps  
137/udp open|filtered netbios-ns  
1900/udp open|filtered upnp  
4500/udp open|filtered nat-t-ike  
5050/udp open|filtered mmcc  
5353/udp open|filtered zeroconf  
5355/udp open|filtered llmnr  
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)  
  
Nmap scan report for 10.0.2.3  
Host is up (0.00054s latency).  
Not shown: 996 closed ports, 994 filtered ports  
PORT STATE SERVICE  
135/tcp open msrpc  
445/tcp open microsoft-ds  
5357/tcp open wsdapi  
67/udp open|filtered dhcps  
137/udp open|filtered netbios-ns  
1900/udp open|filtered upnp  
3702/udp open|filtered ws-discovery  
4500/udp open|filtered nat-t-ike  
5050/udp open|filtered mmcc  
5355/udp open|filtered llmnr  
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)  
  
Nmap scan report for 10.0.2.4  
Host is up (0.00046s latency).  
Not shown: 996 closed ports, 994 filtered ports  
PORT STATE SERVICE  
135/tcp open msrpc  
445/tcp open microsoft-ds  
5357/tcp open wsdapi  
67/udp open|filtered dhcps  
69/udp open|filtered tftp  
137/udp open|filtered netbios-ns  
1900/udp open|filtered upnp  
3702/udp open|filtered ws-discovery  
4500/udp open|filtered nat-t-ike  
5355/udp open|filtered llmnr  
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)  
  
Nmap done: 3 IP addresses (3 hosts up) scanned in 180.45 seconds

**An aggressive service and OS Detection scan on the Domain:**

**root@kali**:**~**# nmap -A -sV --version-intensity 5 10.0.2.0/24  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-06 18:47 EST  
Nmap scan report for 10.0.2.2  
Host is up (0.00053s latency).  
Not shown: 997 closed ports  
PORT STATE SERVICE VERSION  
135/tcp open msrpc Microsoft Windows RPC  
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds  
65000/tcp filtered unknown  
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)  
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=7.25BETA2%E=4%D=2/6%OT=135%CT=1%CU=37362%PV=Y%DS=1%DC=D%G=Y%M=525  
OS:400%TM=58990B86%P=x86\_64-pc-linux-gnu)SEQ(SP=11%GCD=FA00%ISR=A8%TI=I%CI=  
OS:RD%II=I%SS=S%TS=U)SEQ(SP=11%GCD=FA00%ISR=9C%TI=I%II=I%SS=S%TS=U)OPS(O1=M  
OS:5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=FFFF%W2=FFFF%W3=FFFF%  
OS:W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=N%T=40%W=FFFF%O=M5B4%CC=N%Q=)T1(R=Y%D  
OS:F=N%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=N%T=FF%W=0%S=Z%A=S%F=AR%O=%RD=0  
OS:%Q=)T3(R=Y%DF=N%T=FF%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T4(R=Y%DF=N%T=FF%W=0%S  
OS:=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=FF%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T5(R  
OS:=N)T6(R=Y%DF=N%T=FF%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=FF%W=0%S=Z%  
OS:A=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=FF%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RU  
OS:CK=G%RUD=G)IE(R=Y%DFI=S%T=26%CD=S)  
  
Network Distance: 1 hop  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|\_clock-skew: mean: -0s, deviation: 0s, median: -0s  
| smb-security-mode:   
| account\_used: guest  
| authentication\_level: user  
| challenge\_response: supported  
|\_ message\_signing: disabled (dangerous, but default)  
|\_smbv2-enabled: Server supports SMBv2 protocol  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 0.54 ms 10.0.2.2  
  
Nmap scan report for 10.0.2.3  
Host is up (0.072s latency).  
Not shown: 997 closed ports  
PORT STATE SERVICE VERSION  
135/tcp open msrpc Microsoft Windows RPC  
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds  
65000/tcp filtered unknown  
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)  
Device type: general purpose|bridge  
Running (JUST GUESSING): QEMU (99%), Oracle Virtualbox (95%)  
OS CPE: cpe:/a:qemu:qemu cpe:/o:oracle:virtualbox  
Aggressive OS guesses: QEMU user mode network gateway (99%), Oracle Virtualbox (95%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 1 hop  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|\_clock-skew: mean: -0s, deviation: 0s, median: -0s  
| smb-security-mode:   
| authentication\_level: user  
| challenge\_response: supported  
|\_ message\_signing: disabled (dangerous, but default)  
|\_smbv2-enabled: Server supports SMBv2 protocol  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 71.62 ms 10.0.2.3  
  
Nmap scan report for 10.0.2.4  
Host is up (0.072s latency).  
Not shown: 997 closed ports  
PORT STATE SERVICE VERSION  
135/tcp open msrpc Microsoft Windows RPC  
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds  
65000/tcp filtered unknown  
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)  
Device type: general purpose|bridge  
Running (JUST GUESSING): QEMU (99%), Oracle Virtualbox (95%)  
OS CPE: cpe:/a:qemu:qemu cpe:/o:oracle:virtualbox  
Aggressive OS guesses: QEMU user mode network gateway (99%), Oracle Virtualbox (95%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 1 hop  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|\_clock-skew: mean: -0s, deviation: 0s, median: -0s  
| smb-security-mode:   
| authentication\_level: user  
| challenge\_response: supported  
|\_ message\_signing: disabled (dangerous, but default)  
|\_smbv2-enabled: Server supports SMBv2 protocol  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 71.57 ms 10.0.2.4  
  
Nmap scan report for 10.0.2.15  
Host is up (0.000059s latency).  
All 1000 scanned ports on 10.0.2.15 are closed  
Too many fingerprints match this host to give specific OS details  
Network Distance: 0 hops  
  
Post-scan script results:  
| clock-skew:   
|\_ -0s: Majority of systems scanned  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 256 IP addresses (4 hosts up) scanned in 109.46 seconds

**DNS Brute Scripted on happypacket.net from last week:**

﻿

**root@kali**:**~**# nmap -p 80 --script dns-brute.nse happypacket.net  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-06 19:23 EST  
Nmap scan report for happypacket.net (104.28.2.51)  
Host is up (0.0099s latency).  
Other addresses for happypacket.net (not scanned): 104.28.3.51 2400:cb00:2048:1::681c:333 2400:cb00:2048:1::681c:233  
PORT STATE SERVICE  
80/tcp open http  
  
Host script results:  
| dns-brute:   
| DNS Brute-force hostnames:   
| svn.happypacket.net - 199.195.254.73  
| direct.happypacket.net - 104.28.2.51  
| direct.happypacket.net - 104.28.3.51  
| direct.happypacket.net - 2400:cb00:2048:1:0:0:681c:233  
| direct.happypacket.net - 2400:cb00:2048:1:0:0:681c:333  
| mail.happypacket.net - 216.58.217.51  
| blog.happypacket.net - 104.28.3.51  
| blog.happypacket.net - 104.28.2.51  
| mail.happypacket.net - 2607:f8b0:400f:803:0:0:0:2013  
| blog.happypacket.net - 2400:cb00:2048:1:0:0:681c:233  
| blog.happypacket.net - 2400:cb00:2048:1:0:0:681c:333  
| www.happypacket.net - 104.28.2.51  
| www.happypacket.net - 104.28.3.51  
| www.happypacket.net - 2400:cb00:2048:1:0:0:681c:233  
| www.happypacket.net - 2400:cb00:2048:1:0:0:681c:333  
|\_ ftp.happypacket.net - 199.195.254.73  
  
Nmap done: 1 IP address (1 host up) scanned in 5.40 seconds

**Traceroute script nmap scan which finds geo locations for target IP addresses. I tried it on the happypacket.net from last week:**

﻿

**root@kali**:**~**# sudo nmap --traceroute --script traceroute-geolocation.nse -p 80 happypacket.net  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-06 19:43 EST  
Nmap scan report for happypacket.net (104.28.2.51)  
Host is up (0.0028s latency).  
Other addresses for happypacket.net (not scanned): 104.28.3.51 2400:cb00:2048:1::681c:333 2400:cb00:2048:1::681c:233  
PORT STATE SERVICE  
80/tcp open http  
  
Host script results:  
| traceroute-geolocation:   
| HOP RTT ADDRESS GEOLOCATION  
| 1 0.18 10.0.2.2 - ,-   
|\_ 2 0.20 104.28.2.51 37.770,-122.393 United States (California)  
  
TRACEROUTE (using port 80/tcp)  
HOP RTT ADDRESS  
1 0.18 ms 10.0.2.2  
2 0.20 ms 104.28.2.51  
  
Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds

**Scanning the smb for OS, computer names, netbios name and domain information nmap script:**

﻿

**root@kali**:**~**# nmap -p 445 --script smb-os-discovery.nse 10.0.2.2  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-06 19:48 EST  
Nmap scan report for 10.0.2.2  
Host is up (0.00041s latency).  
PORT STATE SERVICE  
445/tcp open microsoft-ds  
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds

**Attempting to brute force local account with SMB service:**

﻿

**root@kali**:**~**# nmap -p 445 --script smb-brute.nse 10.0.2.2  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-06 19:52 EST  
Nmap scan report for 10.0.2.2  
Host is up (0.00031s latency).  
PORT STATE SERVICE  
445/tcp open microsoft-ds  
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)  
  
Host script results:  
| smb-brute:   
| administrator:<blank> => Valid credentials, account disabled  
|\_ guest:<blank> => Valid credentials, account disabled  
  
Nmap done: 1 IP address (1 host up) scanned in 55.20 seconds

**I have never used hping before. Hping3 is a network tool with the ability to craft packets. This is good for testing firewall rules, port scanning, testing network performance using different protocols, Remote OS fingerprinting, network troubleshooting, avoiding detection from IDS’s/firewalls, and also DDoS attack:**

﻿

**root@kali**:**~**# hping3 -S -p 445 10.0.2.2 -c 10  
HPING 10.0.2.2 (eth0 10.0.2.2): S set, 40 headers + 0 data bytes  
len=46 ip=10.0.2.2 ttl=64 id=32902 sport=445 flags=SA seq=0 win=65535 rtt=0.6 ms  
len=46 ip=10.0.2.2 ttl=64 id=32903 sport=445 flags=SA seq=1 win=65535 rtt=0.7 ms  
len=46 ip=10.0.2.2 ttl=64 id=32904 sport=445 flags=SA seq=2 win=65535 rtt=0.7 ms  
len=46 ip=10.0.2.2 ttl=64 id=32905 sport=445 flags=SA seq=3 win=65535 rtt=0.8 ms  
len=46 ip=10.0.2.2 ttl=64 id=32906 sport=445 flags=SA seq=4 win=65535 rtt=0.8 ms  
len=46 ip=10.0.2.2 ttl=64 id=32907 sport=445 flags=SA seq=5 win=65535 rtt=0.6 ms  
len=46 ip=10.0.2.2 ttl=64 id=32908 sport=445 flags=SA seq=6 win=65535 rtt=0.8 ms  
len=46 ip=10.0.2.2 ttl=64 id=32909 sport=445 flags=SA seq=7 win=65535 rtt=0.7 ms  
len=46 ip=10.0.2.2 ttl=64 id=32910 sport=445 flags=SA seq=8 win=65535 rtt=0.7 ms  
len=46 ip=10.0.2.2 ttl=64 id=32911 sport=445 flags=SA seq=9 win=65535 rtt=0.5 ms  
  
--- 10.0.2.2 hping statistic ---  
10 packets transmitted, 10 packets received, 0% packet loss  
round-trip min/avg/max = 0.5/0.7/0.8 ms

﻿

**root@kali**:**~**# hping3 -S -p 135 10.0.2.2 -c 10  
HPING 10.0.2.2 (eth0 10.0.2.2): S set, 40 headers + 0 data bytes  
len=46 ip=10.0.2.2 ttl=64 id=32912 sport=135 flags=SA seq=0 win=65535 rtt=0.7 ms  
len=46 ip=10.0.2.2 ttl=64 id=32913 sport=135 flags=SA seq=1 win=65535 rtt=0.7 ms  
len=46 ip=10.0.2.2 ttl=64 id=32914 sport=135 flags=SA seq=2 win=65535 rtt=3.2 ms  
len=46 ip=10.0.2.2 ttl=64 id=32915 sport=135 flags=SA seq=3 win=65535 rtt=0.9 ms  
len=46 ip=10.0.2.2 ttl=64 id=32916 sport=135 flags=SA seq=4 win=65535 rtt=0.8 ms  
len=46 ip=10.0.2.2 ttl=64 id=32917 sport=135 flags=SA seq=5 win=65535 rtt=0.7 ms  
len=46 ip=10.0.2.2 ttl=64 id=32918 sport=135 flags=SA seq=6 win=65535 rtt=0.7 ms  
len=46 ip=10.0.2.2 ttl=64 id=32919 sport=135 flags=SA seq=7 win=65535 rtt=0.8 ms  
len=46 ip=10.0.2.2 ttl=64 id=32920 sport=135 flags=SA seq=8 win=65535 rtt=1.0 ms  
len=46 ip=10.0.2.2 ttl=64 id=32921 sport=135 flags=SA seq=9 win=65535 rtt=0.6 ms  
  
--- 10.0.2.2 hping statistic ---  
10 packets transmitted, 10 packets received, 0% packet loss  
round-trip min/avg/max = 0.6/1.0/3.2 ms

**You will notice that TCP port 65000 gives us a Damage or duplicate packet:**

**root@kali**:**~**# hping3 -S -p 65000 10.0.2.2 -c 10  
HPING 10.0.2.2 (eth0 10.0.2.2): S set, 40 headers + 0 data bytes  
len=46 ip=10.0.2.2 ttl=64 id=32922 sport=65000 flags=SA seq=0 win=65535 rtt=0.6 ms  
len=46 ip=10.0.2.2 ttl=64 id=32923 sport=65000 flags=SA seq=1 win=65535 rtt=0.7 ms  
DUP! len=46 ip=10.0.2.2 ttl=64 id=32924 sport=65000 flags=AF seq=1 win=65535 rtt=0.9 ms  
DUP! len=46 ip=10.0.2.2 ttl=255 id=32925 sport=65000 flags=RA seq=1 win=0 rtt=0.9 ms  
len=46 ip=10.0.2.2 ttl=64 id=32926 sport=65000 flags=SA seq=2 win=65535 rtt=0.9 ms  
len=46 ip=10.0.2.2 ttl=64 id=32927 sport=65000 flags=SA seq=3 win=65535 rtt=1.0 ms  
DUP! len=46 ip=10.0.2.2 ttl=64 id=32928 sport=65000 flags=AF seq=3 win=65535 rtt=1.2 ms  
DUP! len=46 ip=10.0.2.2 ttl=255 id=32929 sport=65000 flags=RA seq=3 win=0 rtt=1.4 ms  
len=46 ip=10.0.2.2 ttl=64 id=32930 sport=65000 flags=SA seq=4 win=65535 rtt=0.8 ms  
DUP! len=46 ip=10.0.2.2 ttl=64 id=32931 sport=65000 flags=AF seq=4 win=65535 rtt=1.4 ms  
  
--- 10.0.2.2 hping statistic ---  
5 packets transmitted, 10 packets received, -100% packet loss  
round-trip min/avg/max = 0.6/1.0/1.4 ms  
﻿

**root@kali**:**~**# hping3 -8 1-1000,8888,known -S 10.0.2.2  
Scanning 10.0.2.2 (10.0.2.2), port 1-1000,8888,known  
1193 ports to scan, use -V to see all the replies  
+----+-----------+---------+---+-----+-----+-----+  
|port| serv name | flags |ttl| id | win | len |  
+----+-----------+---------+---+-----+-----+-----+  
 1241 nessus : .S..A... 64 42368 65535 46  
 445 microsoft-d: .S..A... 64 42624 65535 46  
 135 loc-srv : .S..A... 64 42880 65535 46  
All replies received. Done.  
Not responding ports: (137 netbios-ns)