

GEEK@SOMEHOST ~ \$ SUDO NMAP -VV -PN -A -O -SV RUCTF.ORG

```
STARTING NMAP 6.25 ( HTTP://NMAP.ORG ) AT 2013-02-23 13:19 YEKT
NSE: LOADED 106 SCRIPTS FOR SCANNING.
NSE: SCRIPT PRE-SCANNING.
NSE: STARTING RUNLEVEL 1 (OF 2) SCAN.
NSE: STARTING RUNLEVEL 2 (OF 2) SCAN.
INITIATING PARALLEL DNS RESOLUTION OF 1 HOST. AT 13:19
COMPLETED PARALLEL DNS RESOLUTION OF 1 HOST. AT 13:19, 0.06S ELAPSED
INITIATING SYN STEALTH SCAN AT 13:19
SCANNING RUCTF.ORG (194.226.235.189) [1000 PORTS]
DISCOVERED OPEN PORT 80/TCP ON 194.226.235.189
DISCOVERED OPEN PORT 8080/TCP ON 194.226.235.189
DISCOVERED OPEN PORT 22/TCP ON 194.226.235.189
COMPLETED SYN STEALTH SCAN AT 13:20, 4.88S ELAPSED (1000 TOTAL PORTS)
INITIATING SERVICE SCAN AT 13:20
SCANNING 3 SERVICES ON RUCTF.ORG (194.226.235.189)
COMPLETED SERVICE SCAN AT 13:20, 6.01S ELAPSED (3 SERVICES ON 1 HOST)
INITIATING OS DETECTION (TRY #1) AGAINST RUCTF.ORG (194.226.235.189)
RETRYING OS DETECTION (TRY #2) AGAINST RUCTF.ORG (194.226.235.189)
INITIATING TRACEROUTE AT 13:20
COMPLETED TRACEROUTE AT 13:20, 0.88S ELAPSED
INITIATING PARALLEL DNS RESOLUTION OF 5 HOSTS. AT 13:20
COMPLETED PARALLEL DNS RESOLUTION OF 5 HOSTS. AT 13:20, 0.13S ELAPSED
NSE: SCRIPT SCANNING 194.226.235.189.
NSE: STARTING RUNLEVEL 1 (OF 2) SCAN.
INITIATING NSE AT 13:20
COMPLETED NSE AT 13:20, 0.56S ELAPSED
NSE: STARTING RUNLEVEL 2 (OF 2) SCAN.
NMAP SCAN REPORT RUCTF.ORG (194.226.235.189)
HOST IS UP (0.0056S LATENCY).
RDNS RECORD FOR 194.226.235.189: 235.189.DHCP.MATH.USU.RU
SCANNED AT 2013-02-23 13:19:58 YEKT FOR 18S
NOT SHOWN: 997 FILTERED PORTS
PORT STATE SERVICE VERSION
22/TCP OPEN SSH OPENSSSH 5.5P1 DEBIAN 6+SQUEEZE2 (PROTOCOL 2.0)
| SSH-HOSTKEY: 1024 E1:3E:8F:F9:4C:6F:E2:7D:2F:9D:19:B2:5B:2B:E2:1A (DSA)
| SSH-DSS AAAAB3NZA1KC3MAAACBP+SSDAKXYWPZZABVJE31WL+JWILS00LSICFJABXGHUZCOY6K00I4+WHS+ZT4X8GUGMMHC/VMFDRPFBU+JYUKCBRDCLQZ
ACOLDPBBUONXNM+N2DYMJ7AHS+HBZCKBH2QDR0CU87JFBDDLA0XKHJYFTFS4ENNDPN3XAJSGHORPAAAAFQCSR7Z0BCRZIJISIS5FUU7IMAVZ1WAAAIEATSLNH0VF
56RU6FKX45BRI+PR5XYRYS13DFGMF6K5XE21/HXTXSBGTUFXLW1+DRZMJDKNIHSDTGLHTVLVBEG2RBMBY9CPJRYUWQ5SRLFAR35JUMMESTZA30W50MTHTS8FOBR
ONRD/XSVD4W6GKAJZWXOBNTPOFIGWRF/C/59GMAAACBAMBIB8YAVVJXWMM7RILHE6LXMYDH9J8BHUVFIIQT0FBP+UJRX4AFEWXBGKKA0YALJP6DGDWLFEBIXI4RDG
4BA0BIFMC/LEWC9XZPVH4282BZ4Z2MWMQZCRWBGM+BLJPAWVHZKIUBNOZJK04F1ZUI5DSSYEGRISMCPM3W/7FLWB
| 2048 BD:7F:47:45:B2:71:FF:DD:CA:C2:53:69:CC:9B:9B:E1 (RSA)
| SSH-RSA AAAAB3NZA1YC2EAAAAB1WAAAQEA10HXQZDIWITCVIPBHMDECY0TU/1YVATOFST82FCLHOXAMUGMRP7JLFLCHDEPXS6QM0FDNXTDEEPM85HMH8GN
9JZVKUHANHAZZLPCUPPI6OESN9EEPHUVFGY0/4NNW8+KF60QH9KTW5JC79VKLLDNHJPHXNXQ2JQ/MNXUKJS6F7EYXTGNQYPTUUVLUF8YGEWZF3HLK6TDTXVGK
FKWHCEEMF9RLDA4Q3+KDVNTUKQR374DHI4QL32UNZG/KNPGVJX/5OMB5WFJEWB3QM7FYV53KVS6FA2TDL0BLCNHHUCT7S4RCB9P39CIOALQGVL0M8SLBIJYNPL3BU
TOFIQ==
80/TCP OPEN HTTP NGINX 0.7.67
|_HTTP-METHODS: NO ALLOW OR PUBLIC HEADER IN OPTIONS RESPONSE (STATUS CODE 200)
| HTTP-ROBOTS.TXT: 4 DISALLOWED ENTRIES
| /2010/USER/FRASK /2011/USER/FRASK /2012/USER/FRASK
|_/USER/FRASK
|_HTTP-TITLE: RUCTF
8080/TCP OPEN HTTP BITTORRENT P2P TRACKER 3.4.2 (BTTRACK.PY)
|_HTTP-TITLE: BITTORRENT DOWNLOAD INFO
WARNING: OSSCAN RESULTS MAY BE UNRELIABLE BECAUSE WE COULD NOT FIND AT LEAST 1 OPEN AND 1 CLOSED PORT
DEVICE TYPE: GENERAL PURPOSE|FIREWALL|WAP|TERMINAL
RUNNING (JUST GUESSING): LINUX 2.6.X|2.4.X|3.X (92%), IPFIRE LINUX 2.6.X (89%), IGEL LINUX 2.6.X (86%)
OS CPE: CPE:/O:LINUX:LINUX_KERNEL:2.6.35 CPE:/O:IPFIRE:LINUX:2.6.32 CPE:/O:LINUX:LINUX_KERNEL:2.4 CPE:/O:LINUX:LINUX_KERNEL:3
CPE:/O:IGEL:LINUX:2.6
OS FINGERPRINT NOT IDEAL BECAUSE: MISSING A CLOSED TCP PORT SO RESULTS INCOMPLETE
AGGRESSIVE OS GUESSES: LINUX 2.6.35 (92%), LINUX 2.6.32 (91%), IPFIRE FIREWALL 2.11 (LINUX 2.6.32) (89%), DD-WRT V24-SPI (LIN
UX 2.4) (89%), LINUX 3.2.0 (87%), IGEL UD3 THIN CLIENT (LINUX 2.6) (86%), LINUX 2.6.35 (UBUNTU) (86%)
NO EXACT OS MATCHES FOR HOST (TEST CONDITIONS NON-IDEAL).
TCP/IP FINGERPRINT:
SCAN(V=6,25E=4%D=2/23%O=22%CT=2%CU=%PV=N%DS=9%DC=T%G=N%TM=51286DB0P=X86_64-APPLE-DARWIN10.8.0)
SEQ(SP=104%GCD=1%ISR=107%TI=Z%TS=8)
OPS(O1=M564ST11NW5%O2=M564ST11NW5%O3=M564NNT11NW5%O4=M564ST11NW5%O5=M564ST11NW5%O6=M564ST11)
WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)
ECN(R=Y%DF=Y%TG=40%W=16D0%O=M564NNSNW5%CC=Y%Q=)
T1(R=Y%DF=Y%TG=40%S=0%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
U1(R=N)
IE(R=N)
UPTIME GUESS: 125.892 DAYS (SINCE SAT OCT 20 15:55:36 2012)
NETWORK DISTANCE: 5 HOPS
TCP SEQUENCE PREDICTION: DIFFICULTY=262 (GOOD LUCK!)
IP ID SEQUENCE GENERATION: ALL ZEROS
SERVICE INFO: OS: LINUX; CPE: CPE:/O:LINUX:LINUX_KERNEL
TRACEROUTE (USING PORT 80/TCP)
HOP RTT ADDRESS
1 4.07 MS URFU-EIX.EUNNET.NET (194.85.107.48)
2 4.04 MS 10.255.99.2
3 10.46 MS 10.255.11.1
4 6.22 MS 10.96.254.73
5 9.81 MS 235.189.DHCP.MATH.USU.RU (194.226.235.189)
NSE: SCRIPT POST-SCANNING.
NSE: STARTING RUNLEVEL 1 (OF 2) SCAN.
INITIATING NSE AT 13:20
COMPLETED NSE AT 13:20, 0.00S ELAPSED
NSE: STARTING RUNLEVEL 2 (OF 2) SCAN.
READ DATA FILES FROM: /USR/LOCAL/BIN/./SHARE/NMAP
OS AND SERVICE DETECTION PERFORMED. PLEASE REPORT ANY INCORRECT RESULTS AT HTTP://NMAP.ORG/SUBMIT/ .
NMAP DONE: 1 IP ADDRESS (1 HOST UP) SCANNED IN 19.58 SECONDS
RAW PACKETS SENT: 2096 (97.360KB) | RCVD: 56 (3.500KB)
```

