

Chrome | Downloads | Debian 10.x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)

Player | Downloads | Altoro Mutual - Mozilla Firefox | root@KaliLinux: /home/part

File Actions Edit View Help

Nmap done: 1 IP address (1 host up) scanned in 170.50 seconds
Raw packets sent: 3176 (144.802KB) | Rcvd: 2579 (103.618KB)

```
[root@KaliLinux-1:/home/part] # nmap -v -A kali.org
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-08 10:43 CDT
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:43
Completed NSE at 10:43, 0.00s elapsed
Initiating NSE at 10:43
Completed NSE at 10:43, 0.00s elapsed
Initiating NSE at 10:43
Completed NSE at 10:43, 0.00s elapsed
Initiating NSE at 10:43
Completed NSE at 10:43, 0.00s elapsed
Initiating Ping Scan at 10:43
Scanning kali.org (50.116.58.136) [4 ports]
Completed Ping Scan at 10:43, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:43
Completed Parallel DNS resolution of 1 host. at 10:43, 0.21s elapsed
Initiating SYN Stealth Scan at 10:43
Scanning kali.org (50.116.58.136) [1000 ports]
Discovered open port 80/tcp on 50.116.58.136
Discovered open port 22/tcp on 50.116.58.136
Discovered open port 443/tcp on 50.116.58.136
Increasing send delay for 50.116.58.136 from 0 to 5 due to 12 out of 39 dropped probes since last increase.
SYN Stealth Scan Timing: About 36.63% done; ETC: 10:44 (0:00:54 remaining)
SYN Stealth Scan Timing: About 38.70% done; ETC: 10:45 (0:01:37 remaining)
Completed SYN Stealth Scan at 10:44, 94.84s elapsed (1000 total ports)
Initiating Service scan at 10:44
Scanning 3 services on kali.org (50.116.58.136)
Completed Service scan at 10:44, 5.01s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against kali.org (50.116.58.136)
Retrying OS detection (try #2) against kali.org (50.116.58.136)
Initiating Traceroute at 10:44
Completed Traceroute at 10:44, 0.03s elapsed
Initiating Parallel DNS resolution of 1 host. at 10:44
Completed Parallel DNS resolution of 1 host. at 10:44, 0.02s elapsed
NSE: Script scanning 50.116.58.136.
Initiating NSE at 10:44
Completed NSE at 10:45, 22.13s elapsed
Initiating NSE at 10:45
Completed NSE at 10:45, 7.90s elapsed
Initiating NSE at 10:45
Completed NSE at 10:45, 0.00s elapsed
Nmap scan report for kali.org (50.116.58.136)
Host is up (0.001s latency).
```

Privacy and Security
The 2022 experts of Altoro Mutual are dedicated to protecting your assets and **you**. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win a Samsung Galaxy S20 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S20 smartphones! We look forward to hearing your important feedback.

Show in folder

Downloads | Debian 10.x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)

Player | Downloads | +

Altoro Mutual - Mozilla ... root@KaliLinux: /home/part

root@KaliLinux: /home/part

File Actions Edit View Help

Initiating NSE at 10:45
Completed NSE at 10:45, 0.00s elapsed
Nmap scan report for kali.org (50.116.58.136)
Host is up (0.0014s latency).
rDNS record for 50.116.58.136: li458-136.members.linode.com
Not shown: 880 filtered ports, 117 closed ports
PORT STATE SERVICE VERSION
22/tcp open tcwwrapped
_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp open tcwwrapped
443/tcp open tcwwrapped
ssl-cert: Subject: CommonName=kali.org
Subject Alternative Name: DNS:kali.org
Issuer: commonName=R3/organizationName=Let's Encrypt/countryName=US
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2022-02-14T16:31:48
Not valid after: 2022-05-15T16:31:47
MD5: 1e52 c9f9 d353 6c9d 1e52 5777 2bbd 75ae
SHA-1: 00c6 66e3 11e1 4956 0374 4408 1712 3471 79fd 2ccc
tls-alpn:
_ http/1.1
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -ssU
No OS matches for host
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.17 ms 192.168.35.2
2 0.06 ms li458-136.members.linode.com (50.116.58.136)

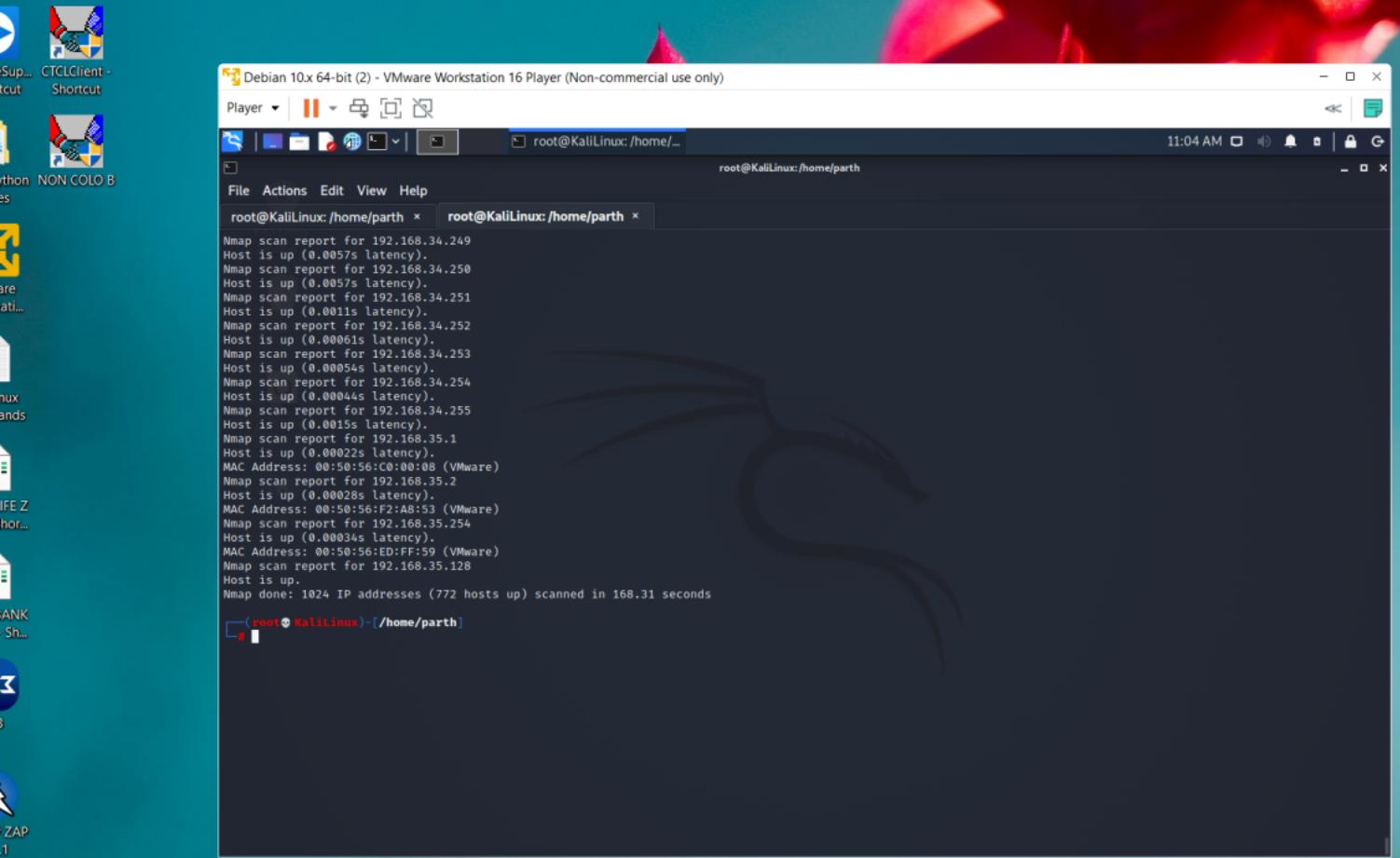
NSE: Script Post-scanning.
Initiating NSE at 10:45
Completed NSE at 10:45, 0.00s elapsed
Initiating NSE at 10:45
Completed NSE at 10:45, 0.00s elapsed
Initiating NSE at 10:45
Completed NSE at 10:45, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
Nmap done: 1 IP address (1 host up) scanned in 136.62 seconds
Raw packets sent: 3099 (142.080KB) | Rcvd: 1468 (60.728KB)

Privacy and Security
The 2020 response of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Business Credit Cards
You're always looking for ways to impress your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

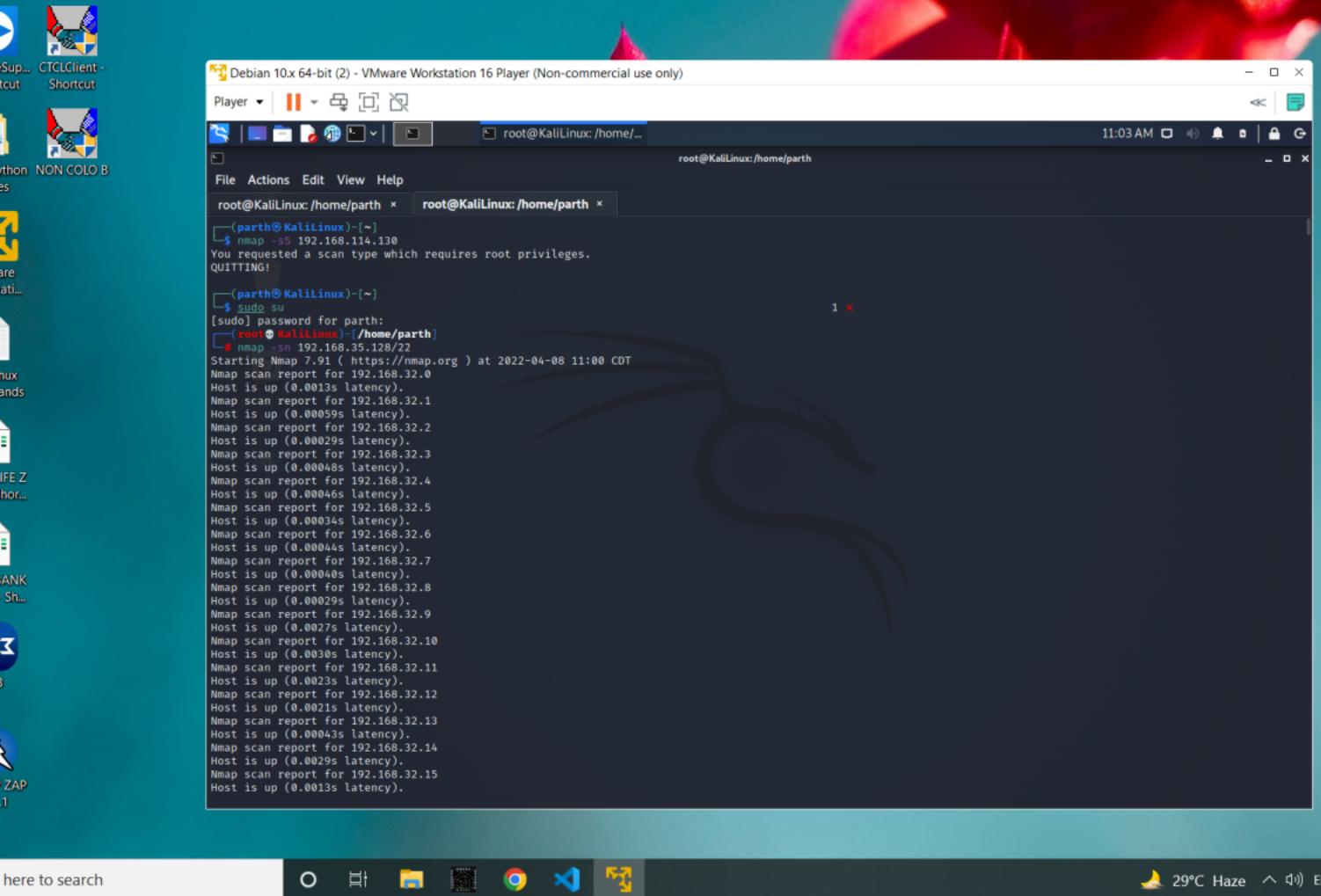
Show in folder

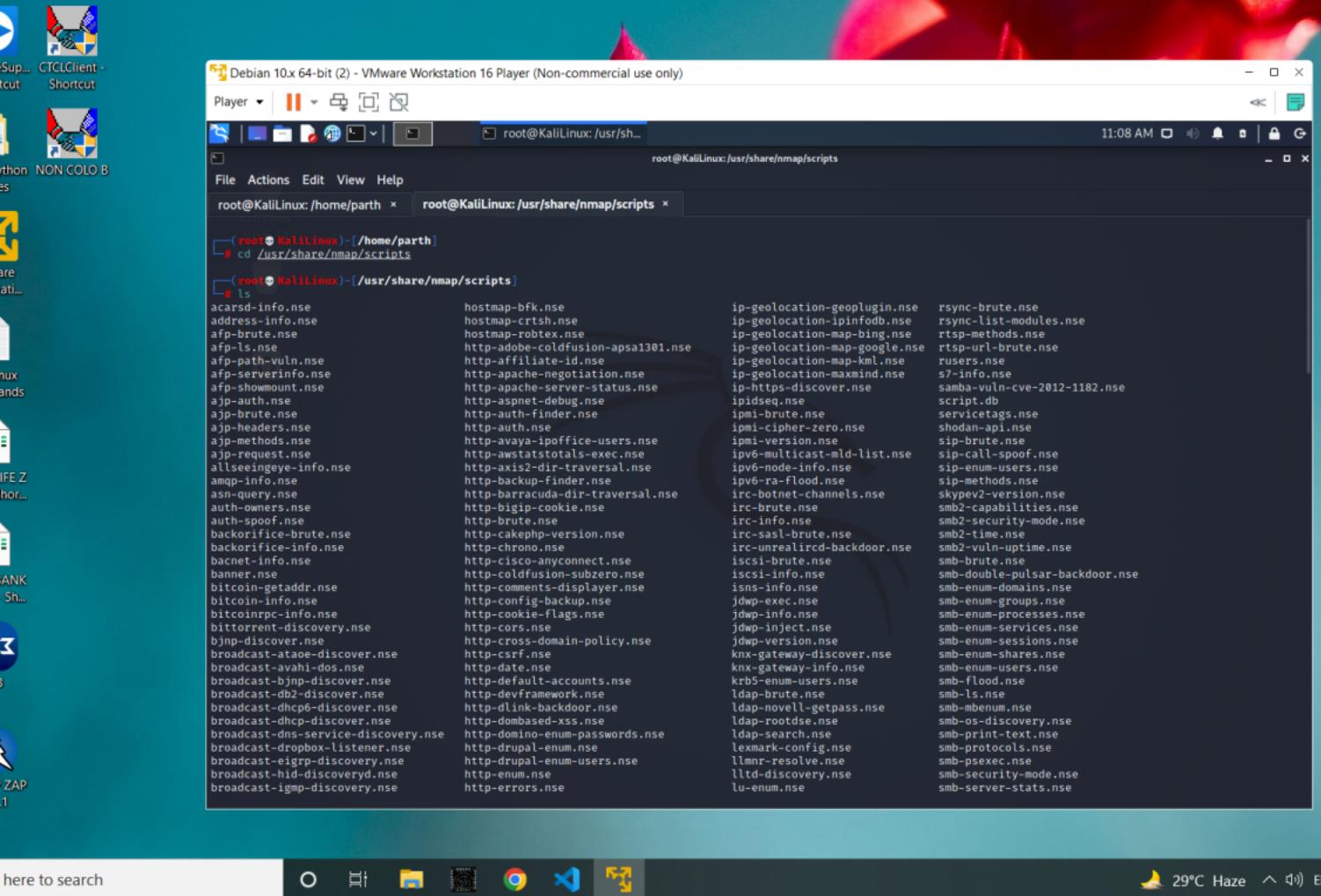


here to search



29°C Haze ENG



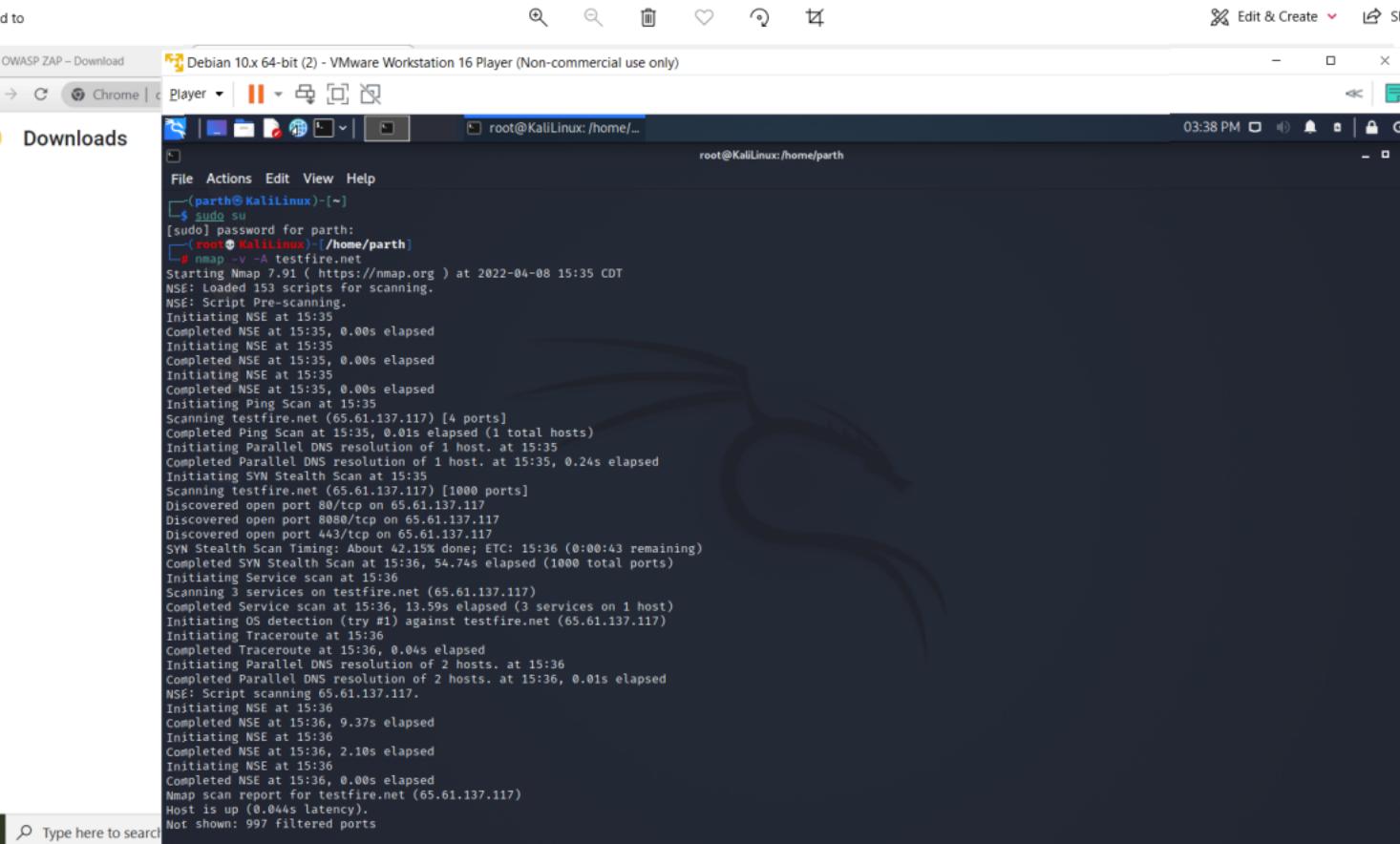


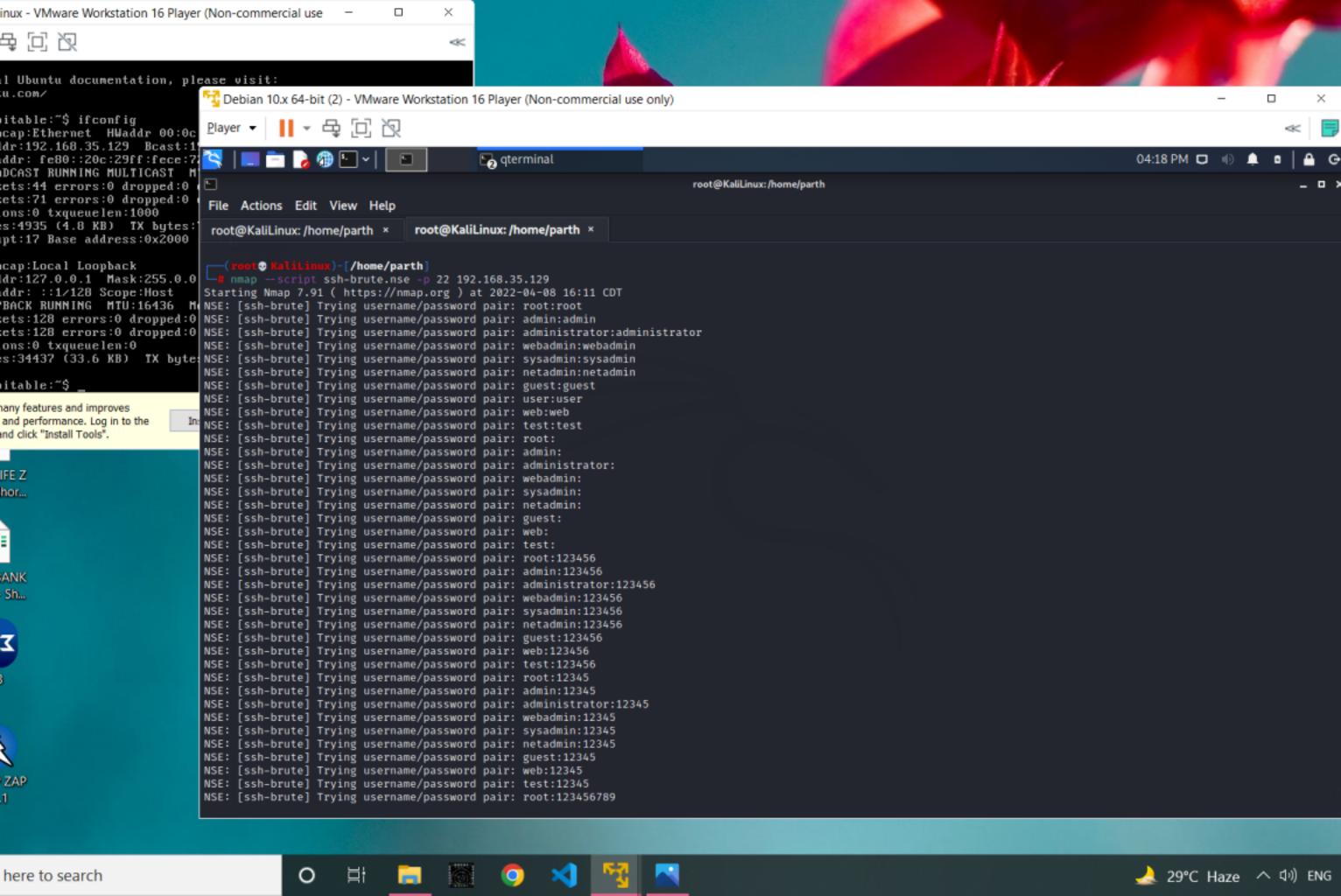
here to search



29°C Haze ENG

+ Add to

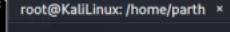
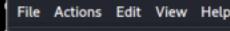
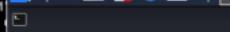




Ubuntu documentation, please visit:
u.com

```
itable:~$ ifconfig  
cap:Ethernet HWaddr 00:0c:  
addr: 192.168.35.129 Bcast:192.168.35.255 Mask:  
inet brd: fe80::20c:2ff:fece:7  
MCast RUNNING MULTICAST M  
ackets:44 errors:0 dropped:0  
txqueuelen:1000  
bytes:4935 (4.8 KB) TX bytes:  
txqueuelen:17 Base address:0x2000
```

Debian 10.x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)



qterminal

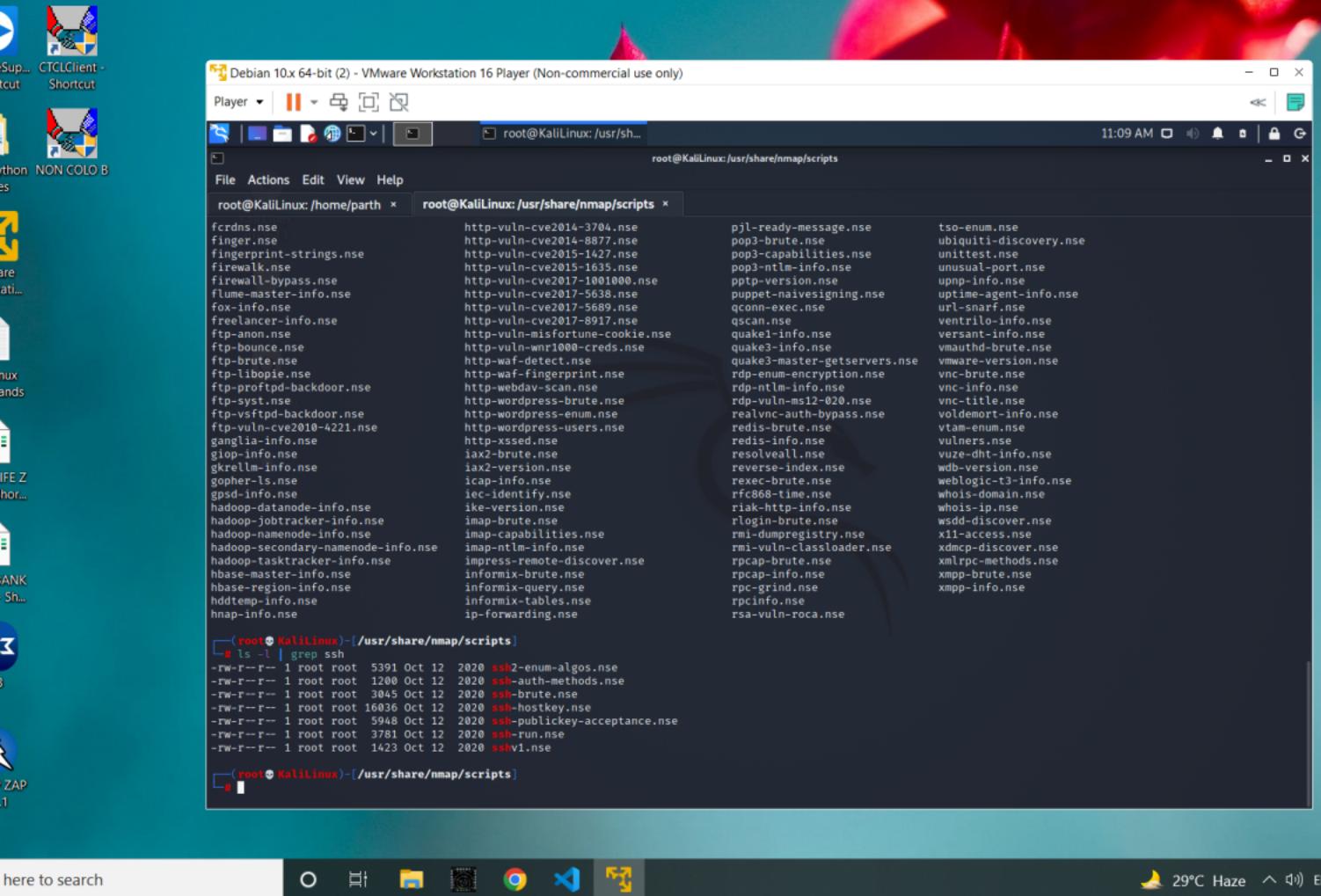
04:18 PM



File Actions Edit View Help

root@KaliLinux:/home/partx x root@KaliLinux:/home/partx x

```
[root@KaliLinux ~]# /home/partx  
# nmap -script ssh-brute.nse -p 22 192.168.35.129  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-08 16:11 CDT  
NSE: [ssh-brute] Trying username/password pair: root:root  
NSE: [ssh-brute] Trying username/password pair: admin:admin  
NSE: [ssh-brute] Trying username/password pair: administrator:administrator  
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin  
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin  
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin  
NSE: [ssh-brute] Trying username/password pair: guest:guest  
NSE: [ssh-brute] Trying username/password pair: user:user  
NSE: [ssh-brute] Trying username/password pair: web:web  
NSE: [ssh-brute] Trying username/password pair: test:test  
NSE: [ssh-brute] Trying username/password pair: root:  
NSE: [ssh-brute] Trying username/password pair: admin:  
NSE: [ssh-brute] Trying username/password pair: administrator:  
NSE: [ssh-brute] Trying username/password pair: webadmin:  
NSE: [ssh-brute] Trying username/password pair: sysadmin:  
NSE: [ssh-brute] Trying username/password pair: netadmin:  
NSE: [ssh-brute] Trying username/password pair: guest:  
NSE: [ssh-brute] Trying username/password pair: web:  
NSE: [ssh-brute] Trying username/password pair: test:  
NSE: [ssh-brute] Trying username/password pair: root:123456  
NSE: [ssh-brute] Trying username/password pair: admin:123456  
NSE: [ssh-brute] Trying username/password pair: administrator:123456  
NSE: [ssh-brute] Trying username/password pair: webadmin:123456  
NSE: [ssh-brute] Trying username/password pair: sysadmin:123456  
NSE: [ssh-brute] Trying username/password pair: netadmin:123456  
NSE: [ssh-brute] Trying username/password pair: guest:123456  
NSE: [ssh-brute] Trying username/password pair: web:123456  
NSE: [ssh-brute] Trying username/password pair: test:123456  
NSE: [ssh-brute] Trying username/password pair: root:12345  
NSE: [ssh-brute] Trying username/password pair: admin:12345  
NSE: [ssh-brute] Trying username/password pair: administrator:12345  
NSE: [ssh-brute] Trying username/password pair: webadmin:12345  
NSE: [ssh-brute] Trying username/password pair: sysadmin:12345  
NSE: [ssh-brute] Trying username/password pair: netadmin:12345  
NSE: [ssh-brute] Trying username/password pair: guest:12345  
NSE: [ssh-brute] Trying username/password pair: web:12345  
NSE: [ssh-brute] Trying username/password pair: test:12345  
NSE: [ssh-brute] Trying username/password pair: root:123456789
```



+ Add to



X Edit & Create ▾ ↗ Sh

OWASP ZAP – Download

Debian 10x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)

- □ X

Downloads



root@KaliLinux:/home/parth

03:38 PM ↗ ENG



File Actions Edit View Help

```
Mmap scan report for testfire.net (65.61.137.117)
Host is up (0.044s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache Tomcat/Coyote JSP engine 1.1
  http-methods:
    _ Supported Methods: GET HEAD POST OPTIONS
    _http-server-header: Apache-Coyote/1.1
    _http-title: Altoro Mutual
443/tcp   open  ssl/http Apache Tomcat/Coyote JSP engine 1.1
  http-methods:
    _ Supported Methods: GET HEAD POST OPTIONS
    _http-server-header: Apache-Coyote/1.1
    _http-title: Altoro Mutual
  ssl-cert: Subject: commonName=demo.testfire.net
  Subject Alternative Name: DNS:demo.testfire.net, DNS:altoromutual.com
  Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB
  Public Key type: rsa
  Public Key bits: 2048
  Signature Algorithm: sha256WithRSAEncryption
  Not valid before: 2020-05-22T00:00:00
  Not valid after:  2022-05-22T23:59:59
  MD5:  c5a6 d3d2 92a1 6089 26a0 4d42 1f57 cd1d
  SHA-1: b300 b380 6bb4 ac20 3236 5cc0 8051 fa5f a97e 1342
  _ssl-date: 2022-04-08T20:36:28+00:00; -5s from scanner time.
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
  http-methods:
    _ Supported Methods: GET HEAD POST OPTIONS
    _http-open-proxy: Proxy might be redirecting requests
    _http-server-header: Apache-Coyote/1.1
    _http-title: Altoro Mutual
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running: Microsoft Windows XP[7]2012, VMware Player
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, VMware Player virtual NAT device
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=248 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class

Host script results:
  _clock-skew: -5s

TRACEROUTE (using port 80/tcp)
```



Type here to search

here to search



29°C Haze ⚡ ENG

+ Add to



Edit & Create ▾



OWASP ZAP – Download

Debian 10x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)



Downloads

Player



root@KaliLinux:/home/parth

03:38 PM

```

File Actions Edit View Help
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2020-05-22T00:00:00
Not valid after: 2022-05-22T23:59:59
MD5: c5a6 d33d 92a1 6089 26a0 4d42 f157 cd1d
SHA-1: b300 b380 6bb4 ac20 3236 5cc0 8051 fa5f a97e 1342
_ssl-date: 2022-04-08T20:36:28+00:00; -5s from scanner time.
8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
http-methods:
  Supported Methods: GET HEAD POST OPTIONS
  _http-open-proxy: Proxy might be redirecting requests
  _http-server-header: Apache-Coyote/1.1
  _http-title: Altoro Mutual
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running: Microsoft Windows XP|7/2012, VMware Player
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, VMware Player virtual NAT device
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=248 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class

Host script results:
|_clock-skew: -5s

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  0.15 ms 192.168.35.2
2  0.17 ms 65.61.137.117

NSE: Script Post-scanning.
Initiating NSE at 15:36
Completed NSE at 15:36, 0.00s elapsed
Initiating NSE at 15:36
Completed NSE at 15:36, 0.00s elapsed
Initiating NSE at 15:36
Completed NSE at 15:36, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.76 seconds
  Raw packets sent: 2058 (92.446KB) | Rcvd: 1336 (53.650KB)

```

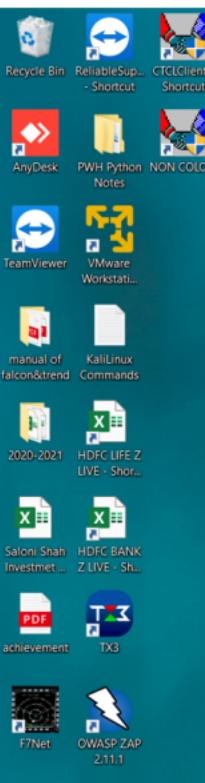
(root@KaliLinux)-[/home/parth]



+ Add to



Edit & Create Share



Debian 10x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)

Player

qterminal Wireshark

Wireshark - Packet 9 - eth0

Frame 9: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
 Ethernet II, Src: VMware_cd:cb:b1 (00:0c:29:cd:cb:b1), Dst: VMware_f2:a8:53 (00:50:56:f2:a8:53)
 Internet Protocol Version 4, Src: 192.168.35.128, Dst: 50.116.58.136
 Transmission Control Protocol, Src Port: 58891, Dst Port: 5963, Seq: 0, Len: 0

No.	Time
1	0.00
2	0.00
3	1.00
4	1.00
5	2.00
6	2.00
7	2.00
8	3.00
9	3.00
10	4.00
11	4.00

Frame 9: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
 Ethernet II, Src: VMware_cd:cb:b1 (00:0c:29:cd:cb:b1), Dst: VMware_f2:a8:53 (00:50:56:f2:a8:53)
 Internet Protocol Version 4, Src: 192.168.35.128, Dst: 50.116.58.136
 Transmission Control Protocol, Src Port: 58891, Dst Port: 5963, Seq: 0, Len: 0

```

0000  00 50 56 f2 a8 53 00 0c 29 cd cb b1 08 00 45 00  PV - S )....E.
0010  00 2c 0b ca 00 00 25 06 38 de c0 a8 23 80 32 74  , , % 8 #.2t
0020  3a 88 e6 0b 17 4b 7d b9 9b e6 00 00 00 00 60 02 : , K . .
0030  04 00 2c 0b 00 00 02 04 05 b4 , , , .

```

No.: 9 - Time: 3.041219139 - Source: 192.168.35.128 - Destination: 50.116.58.136 - Protocol: TCP - Length: 58 - Info: 58891 → 5963 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Close **Help**

wireshark_ether0ARUPK1.pcapng

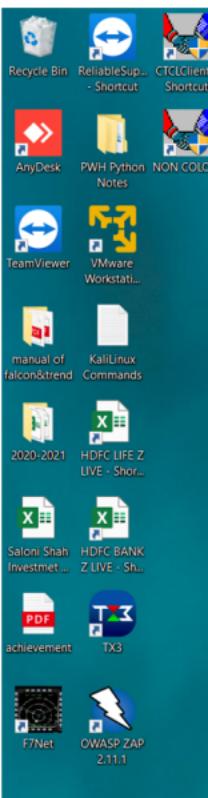
Packets: 360 - Displayed: 360 (100.0%)

Profile: Default

+ Add to



X Edit & Create ▾ L Sh



Debian 10x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)

Player

qterminal Wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

*eth0

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
469	229.379931133	50.116.58.136	192.168.35.128	TCP	60	1154 → 58894 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
470	229.382987624	192.168.35.128	50.116.58.136	TCP	58	58886 → 1033 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
471	230.384593702	192.168.35.128	50.116.58.136	TCP	58	58887 → 1033 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
472	230.409491979	50.116.58.136	192.168.35.128	TCP	60	1154 → 58895 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
473	231.392359356	192.168.35.128	50.116.58.136	TCP	58	58888 → 1033 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
474	231.404951165	50.116.58.136	192.168.35.128	TCP	60	1154 → 58896 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
475	232.365429554	50.116.58.136	192.168.35.128	TCP	60	1033 → 58860 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
476	232.392786604	192.168.35.128	50.116.58.136	TCP	58	58889 → 1033 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
477	233.395078873	192.168.35.128	50.116.58.136	TCP	58	58890 → 1033 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
478	233.503510230	50.116.58.136	192.168.35.128	TCP	60	1033 → 58887 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0

> Frame 9: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
 Ethernet II, Src: VMware_cd:cb:b1 (00:0c:29:cd:cb:b1), Dst: VMware_f2:a8:53 (00:56:56:f2:a8:53)
 > Internet Protocol Version 4, Src: 192.168.35.128, Dst: 50.116.58.136
 > Transmission Control Protocol, Src Port: 58891, Dst Port: 5963, Seq: 0, Len: 0

```

0000  00 50 56 f2 a8 53 00 0c  29 cd cb b1 08 00 45 00  PV - S - ) . . . E
0010  00 2c 0b ca 00 00 25 06  38 de c0 a8 23 80 32 74 , , % 8 . . # 2t
0020  3a 88 e6 0b 17 4b 7d b9  9b e6 00 00 00 00 60 02 : . K . . . .
0030  04 00 2c 0b 00 00 02 04  05 b4 , , . . . .

```

wireshark_ether0ARUPK1.pcapng

Packets: 478 · Displayed: 478 (100.0%)

Profile: Default