How to confuse a port scanner

Vulnerabilities

UDP - Bypass Cryptographic Signature

```
if (!check_dst_port(sport, validation)) {
        return 0;
}
```

```
// Returns 0 if dst_port is outside the expected valid range, non-zero otherwise
static inline int check_dst_port(uint16_t port, uint32_t *validation) {
        if (port > zconf.source_port_last
                                        || port < zconf.source_port_first) {
                return EXIT_FAILURE;
        }
```

Constants:
stdlib.h:#define EXIT_FAILURE 1 /* Failing exit status. */

```
.source_port_first = 32768, // (these are the default
.source_port_last = 61000,  //   ephemeral range on Linux)
```

Vulnerabilities

ICMP - 16 bit signature brute forcible, but it’s even worse

```
mnewcomb@spolematt:~/cs838/proj/send_icmp$ sudo ./send_icmp -i wlan
0 -s 64.145.86.33 -d 192.168.1.4
my mac: 24:77:3:25:d8:1c
source ip: 21569140, dest_ip: 401a8c0
sizeof(struct ip)=20
sizeof(icmphdr)=8
data_len: 12
ether_header: 14
id: 065535
mnewcomb@spolematt:~/cs838/proj/send_icmp$
```

```
mnewcomb@spolematt:~/cs838/zmap-1.0.3/conf$ sudo zmap -i wlan0 -w ../s
rc/whitelist.conf -b ./blacklist.conf -N 500 -B 1M -q --probe-module=i
cmp_echoscan -o -
Dec 10 21:29:17.192 [INFO] zmap: started
64.145.86.33
```

Vulnerabilities

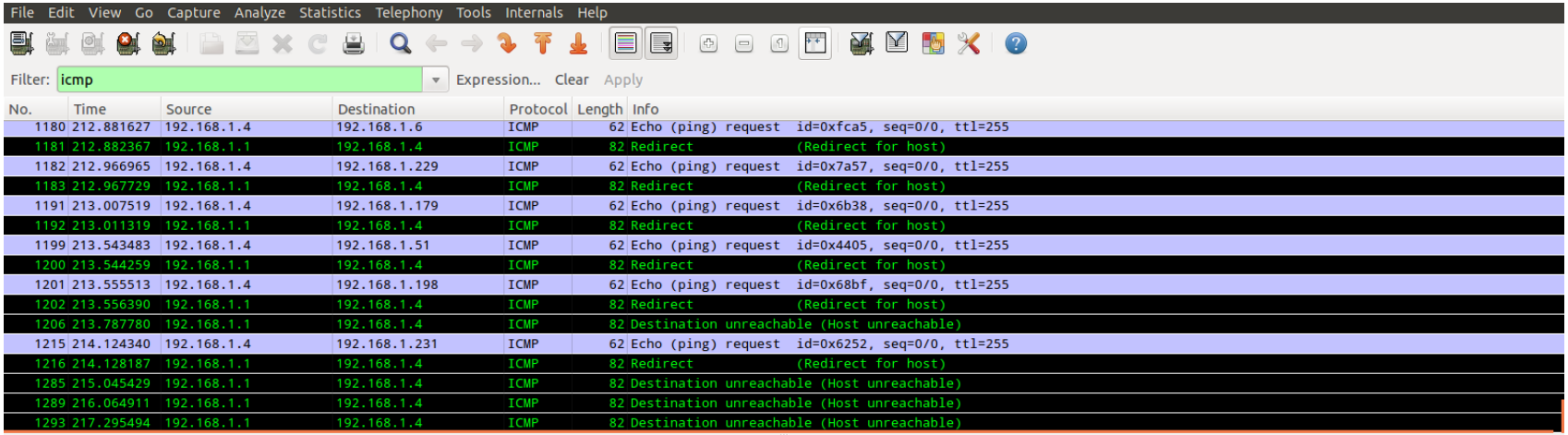
ZMAP does not check to see if a result is a packet comes from a blacklisted address (only 192.168.1.0/24 was whitelisted)

```
0.0.0.3
mnewcomb@spolematt:~/cs838/zmap-1.0.3/conf$ sudo zmap -i wlan0 -w ../src/white
list.conf -b ./blacklist.conf -N 500 -B 1M -q --probe-module=udp -p 1234 -o -
Dec 10 21:36:29.773 [INFO] zmap: started
0.0.0.3
0.0.0.1
1.2.3.4
128.2.1.2
```

```
mnewcomb@spolematt:~/cs838/proj/send_udp$ sudo ./su -i wlan0 -s 128
.2.1.2 -d 192.168.1.4 -p 1234 -q 1234
my mac: 24:77:3:25:d8:1c
source ip: 2010280, dest_ip: 401a8c0, source port: 1234, dest port:
 1234
length: 29
before sendpacket!
43 reply size
sendpacket succeeded 43!
mnewcomb@spolematt:~/cs838/proj/send_udp$
```

Local Subnet Requires Router Support

Zmap addresses packets to a single MAC address (default gateway).



No.	Time	Source	Destination	Protocol	Length	Info
1180	212.881627	192.168.1.4	192.168.1.6	ICMP	62	Echo (ping) request id=0xfca5, seq=0/0, ttl=255
1181	212.882367	192.168.1.1	192.168.1.4	ICMP	82	Redirect (Redirect for host)
1182	212.966965	192.168.1.4	192.168.1.229	ICMP	62	Echo (ping) request id=0x7a57, seq=0/0, ttl=255
1183	212.967729	192.168.1.1	192.168.1.4	ICMP	82	Redirect (Redirect for host)
1191	213.007519	192.168.1.4	192.168.1.179	ICMP	62	Echo (ping) request id=0x6b38, seq=0/0, ttl=255
1192	213.011319	192.168.1.1	192.168.1.4	ICMP	82	Redirect (Redirect for host)
1199	213.543483	192.168.1.4	192.168.1.51	ICMP	62	Echo (ping) request id=0x4405, seq=0/0, ttl=255
1200	213.544259	192.168.1.1	192.168.1.4	ICMP	82	Redirect (Redirect for host)
1201	213.555513	192.168.1.4	192.168.1.198	ICMP	62	Echo (ping) request id=0x68bf, seq=0/0, ttl=255
1202	213.556390	192.168.1.1	192.168.1.4	ICMP	82	Redirect (Redirect for host)
1206	213.787780	192.168.1.1	192.168.1.4	ICMP	82	Destination unreachable (Host unreachable)
1215	214.124340	192.168.1.4	192.168.1.231	ICMP	62	Echo (ping) request id=0x6252, seq=0/0, ttl=255
1216	214.128187	192.168.1.1	192.168.1.4	ICMP	82	Redirect (Redirect for host)
1285	215.045429	192.168.1.1	192.168.1.4	ICMP	82	Destination unreachable (Host unreachable)
1289	216.064911	192.168.1.1	192.168.1.4	ICMP	82	Destination unreachable (Host unreachable)
1293	217.295494	192.168.1.1	192.168.1.4	ICMP	82	Destination unreachable (Host unreachable)

Result: using zmap on your local subnet will be hard

A ZMAP Honeypot

dark_responder

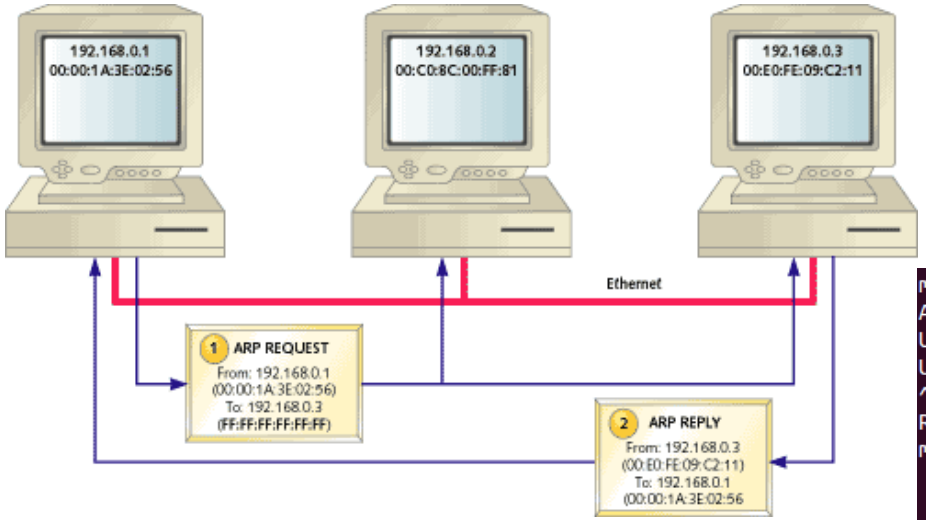
Given a list of dark IP addresses, TCP ports, and UDP ports reply to any traffic with just enough information to fool a portmapper

All examples are configured for 192.168.1.224/27

Receiving Dark IP Traffic

Dark_responder listens for ARP_REQUEST and sends ARP_REPLY

NO SECURITY AT THIS LEVEL!!!

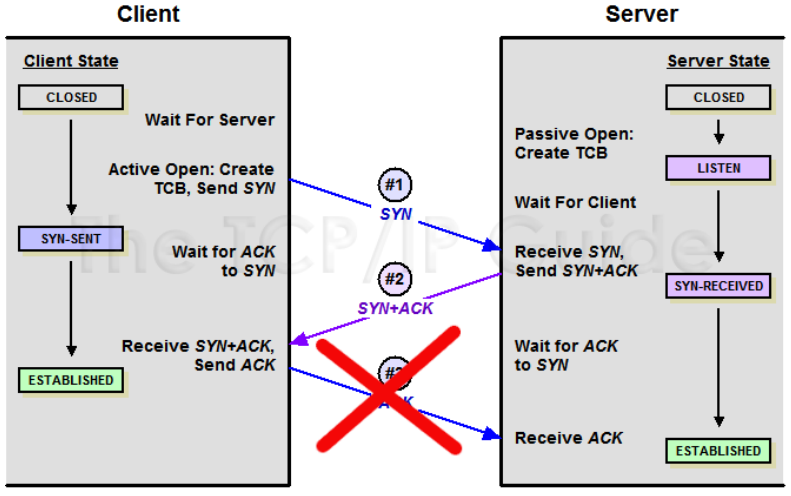



```
mnewcomb@spolematt:~$ sudo arping -I wlan0 192.168.1.224
ARPING 192.168.1.224 from 192.168.1.4 wlan0
Unicast reply from 192.168.1.224 [02:02:02:02:02:02]  24.179ms
Unicast reply from 192.168.1.224 [02:02:02:02:02:02]  4.148ms
^CSent 2 probes (1 broadcast(s))
Received 2 response(s)
mnewcomb@spolematt:~$
```

TCP SYN Scan

Respond to SYN with SYN ack and never issue an ACK. Causes zmapper using forge-socket to consume resources.

```
mnewcomb@spolematt:~/cs838/zmap-1.0.3/conf$ sudo zmap -i
 wlan0 -w ../src/whitelist.conf -b ./blacklist.conf -N 5
00 -B 1M -q --probe-module=tcp_synscan -p 443 -o -
Dec 10 21:53:18.037 [INFO] zmap: started
192.168.1.247
192.168.1.236
192.168.1.235
192.168.1.231
192.168.1.229
192.168.1.232
192.168.1.240
192.168.1.226
192.168.1.230
192.168.1.245
192.168.1.228
192.168.1.249
192.168.1.251
192.168.1.225
192.168.1.252
192.168.1.234
192.168.1.233
192.168.1.250
192.168.1.224
192.168.1.242
192.168.1.248
192.168.1.243
192.168.1.253
192.168.1.241
192.168.1.254
192.168.1.238
192.168.1.255
192.168.1.246
192.168.1.237
192.168.1.244
192.168.1.239
192.168.1.227
Dec 10 21:55:01.666 [INFO] zmap: completed
```



UDP Scan

Respond to a UDP packet With A UDP packet.

```
mnewcomb@spolematt:~/cs838/zmap-1.0.3/conf$ sudo zmap -i
 wlan0 -w ../src/whitelist.conf -b ./blacklist.conf -N 5
00 -B 1M -q --probe-module=udp -p 1900 -o -
Dec 10 22:12:54.803 [INFO] zmap: started
192.168.1.229
192.168.1.247
192.168.1.249
192.168.1.251
192.168.1.226
192.168.1.244
192.168.1.233
192.168.1.240
192.168.1.253
192.168.1.236
192.168.1.252
192.168.1.238
192.168.1.228
192.168.1.246
192.168.1.255
192.168.1.232
192.168.1.254
192.168.1.231
192.168.1.224
192.168.1.250
192.168.1.235
192.168.1.241
192.168.1.227
192.168.1.237
```

```
Host: 192.168.1.243 ()  Ports: 1900/open/udp//upnp///
Host: 192.168.1.244 ()  Status: Up
Host: 192.168.1.244 ()  Ports: 1900/open/udp//upnp///
Host: 192.168.1.245 ()  Status: Up
Host: 192.168.1.245 ()  Ports: 1900/open/udp//upnp///
Host: 192.168.1.246 ()  Status: Up
Host: 192.168.1.246 ()  Ports: 1900/open/udp//upnp///
Host: 192.168.1.247 ()  Status: Up
Host: 192.168.1.247 ()  Ports: 1900/open/udp//upnp///
Host: 192.168.1.248 ()  Status: Up
Host: 192.168.1.248 ()  Ports: 1900/open/udp//upnp///
Host: 192.168.1.249 ()  Status: Up
Host: 192.168.1.249 ()  Ports: 1900/open/udp//upnp///
Host: 192.168.1.250 ()  Status: Up
Host: 192.168.1.250 ()  Ports: 1900/open/udp//upnp///
Host: 192.168.1.251 ()  Status: Up
Host: 192.168.1.251 ()  Ports: 1900/open/udp//upnp///
Host: 192.168.1.252 ()  Status: Up
Host: 192.168.1.252 ()  Ports: 1900/open/udp//upnp///
Host: 192.168.1.253 ()  Status: Up
Host: 192.168.1.253 ()  Ports: 1900/open/udp//upnp///
Host: 192.168.1.254 ()  Status: Up
Host: 192.168.1.254 ()  Ports: 1900/open/udp//upnp///
Host: 192.168.1.255 ()  Status: Up
Host: 192.168.1.255 ()  Ports: 1900/open/udp//upnp///
# Nmap done at Tue Dec 10 23:02:31 2013 -- 32 IP addresses (32 host
s up) scanned in 0.46 seconds
mnewcomb@spolematt:~/Downloads$
```

ICMP Response

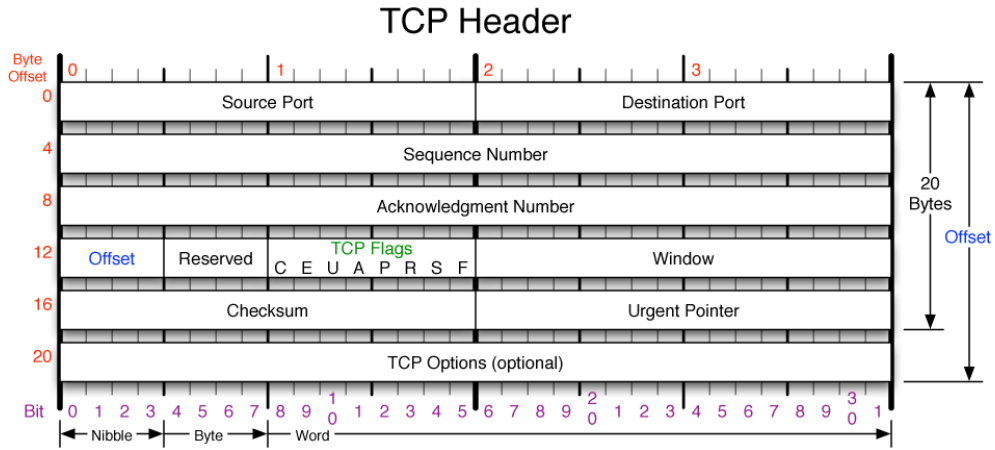
Respond to ICMP Echo Request With Echo Reply (ping works!)

```
mnewcomb@spolematt:~$ ping -c 10 192.168.1.224
PING 192.168.1.224 (192.168.1.224) 56(84) bytes of data.
64 bytes from 192.168.1.224: icmp_req=1 ttl=255 time=0.892 ms
64 bytes from 192.168.1.224: icmp_req=2 ttl=255 time=0.884 ms
64 bytes from 192.168.1.224: icmp_req=3 ttl=255 time=0.843 ms
64 bytes from 192.168.1.224: icmp_req=4 ttl=255 time=1.01 ms
64 bytes from 192.168.1.224: icmp_req=5 ttl=255 time=0.893 ms
64 bytes from 192.168.1.224: icmp_req=6 ttl=255 time=0.881 ms
64 bytes from 192.168.1.224: icmp_req=7 ttl=255 time=0.878 ms
64 bytes from 192.168.1.224: icmp_req=8 ttl=255 time=0.892 ms
64 bytes from 192.168.1.224: icmp_req=9 ttl=255 time=0.926 ms
64 bytes from 192.168.1.224: icmp_req=10 ttl=255 time=0.897 ms

--- 192.168.1.224 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9008r
s
rtt min/avg/max/mdev = 0.843/0.900/1.018/0.051 ms
mnewcomb@spolematt:~$
```

Different Scanning Techniques

XMAS, FIN, NULL, Maimon TCP Scans



Dark Responder / NMAP works, zmap does not

When scanning RFC 793 compliant systems, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open. As long as none of those three bits are included, any combination of the other three (FIN, PSH, and URG) are OK. ZMAP model not suitable for these modes!

Future Work

Integrate *dark_responder* into a dhcp server

Monitoring Unused IP Addresses on Segments Managed by DHCP -

Networked Computing and Advanced Information Management, 2008. NCM '08. Fourth International Conference on (Volume:1)

DHCP churn averages 6.83, magnify the effects of dark_responder

Your botnet is my botnet: analysis of a botnet takeover

CCS '09 Proceedings of the 16th ACM conference on Computer and communications security Pages 635-647