



From theory to practice ...

bringing down the house
with extended DHCP exhausting attack

Gustavo Pimentel
[gusbit gmail dot com]

What the hell is DHCP ?

- Dynamic Host Configuration Protocol
 - Used to assign addresses directly to servers and desktop machines on a local link layer
- Defined as a successor for BOOTP
 - RFC 1531 - October 1993
- Current definition for IPV4 networks
 - RFC 2131 - March 1997

DHCP [security issues]

standardized before
network security became a
significant issue



- DHCP spoofing (rogue DHCP servers)
- DHCP pool exhaust attack (DHCP starvation)

Motivation

- AR Samhuri on Securebits Blog ...
 - “I am almost confident that a new extended version of the available exhausting attack is feasible.”
 - “I have not tested this practically; so, the following explanation is merely theoretical.”

Securebits Blog

[www.securebits.org/blog]

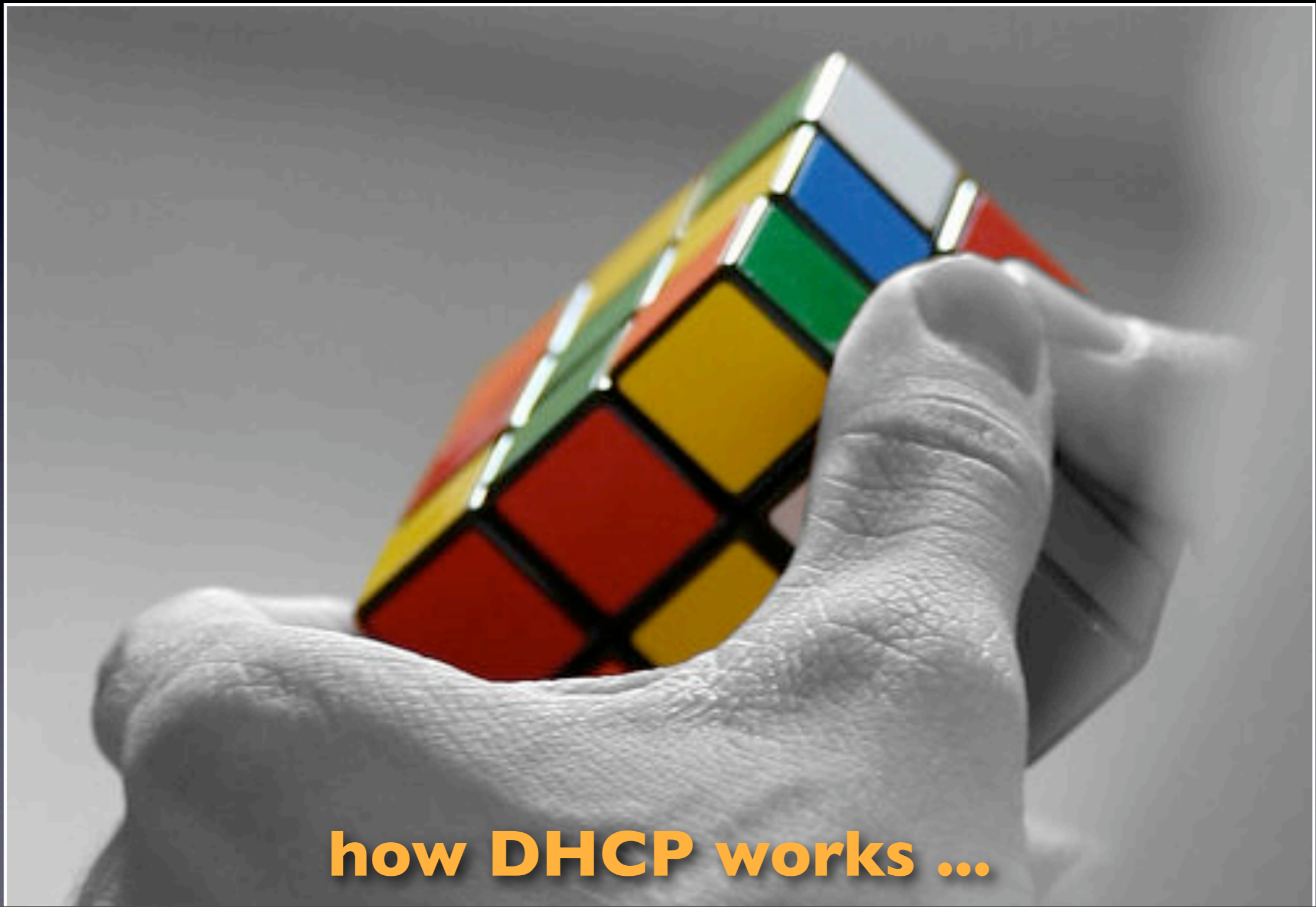


AR Samhuri (Hack In The Box)

... dezembro de 2008

EXTENDED DHCP Exhausting Attack

Before we begin



how DHCP works ...

DHCP [overview]

- IANA assigned ports
 - 67/udp for the server side
 - 68/udp for the client side
- All packets travel as UDP datagrams
 - client-sent packets: src port 68 and dst port 67
 - server-sent packets: src port 67 and dst port 68

DHCP [overview]

- Operations fall into four basic phases [D.O.R.A.]
 - **DISCOVER**
 - **OFFER**
 - **REQUEST**
 - **ACKNOWLEDGEMENT**

D.O.R.A.

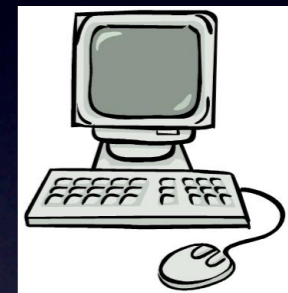
client



00:0c:29:87:74:2d

0.0.0.0

dhcprsv



dhcprd 67/udp

10.1.0.74

10.1.0.0/24

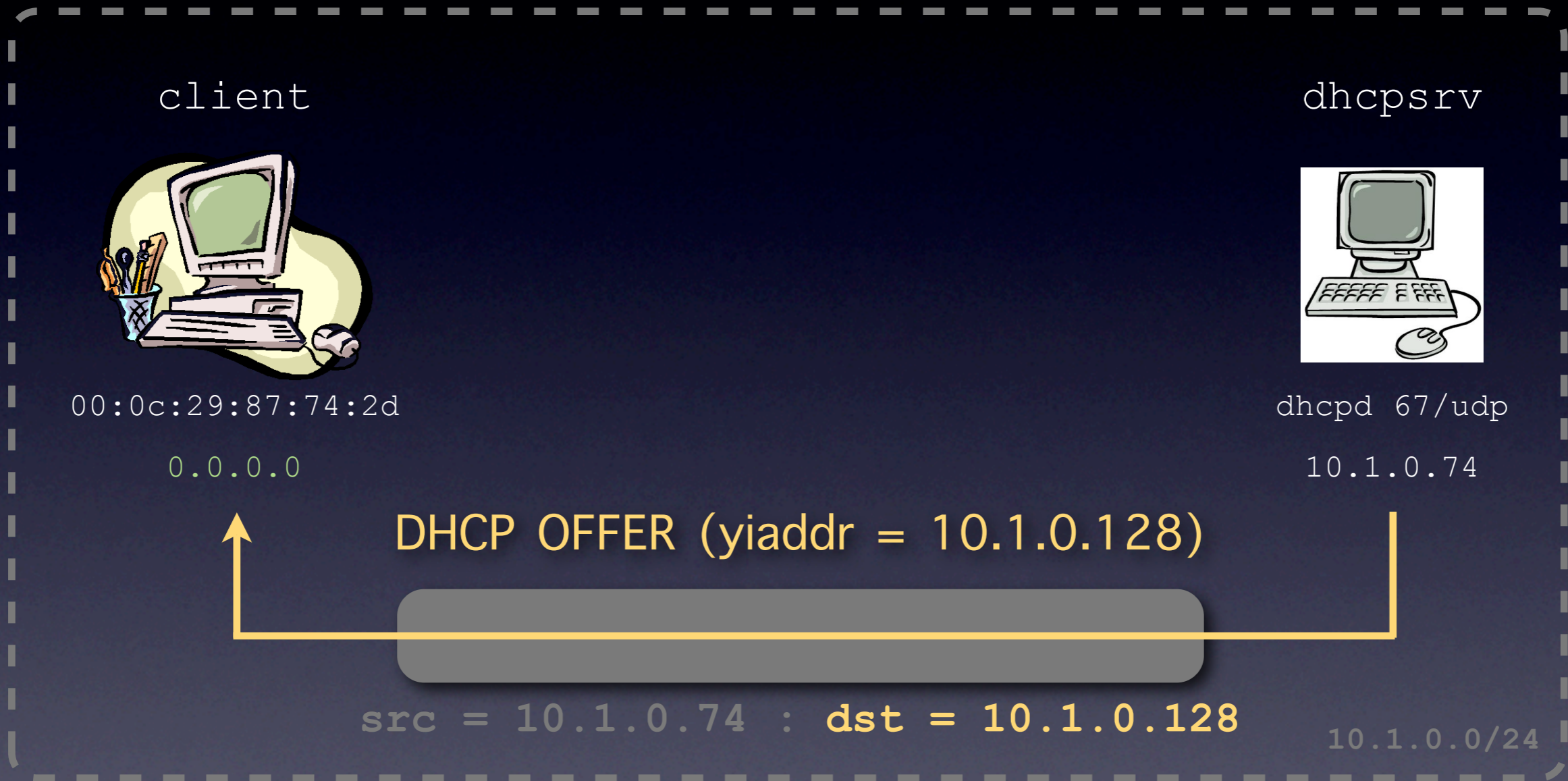
```
Feb 17 03:41:39 dhcprsv dhcprd: DHCPDISCOVER from 00:0c:29:87:74:2d via eth0
Feb 20 02:36:51 dhcprsv dhcprd: DHCPOFFER on 10.1.0.128 to b7:df:19:8f:00:fc via eth0
Feb 20 02:36:56 dhcprsv dhcprd: DHCPREQUEST for 10.1.0.128 from b7:df:19:8f:00:fc via eth0
Feb 20 02:36:56 dhcprsv dhcprd: DHCPACK on 10.1.0.128 to b7:df:19:8f:00:fc via eth0
```

[DHCP DISCOVER]



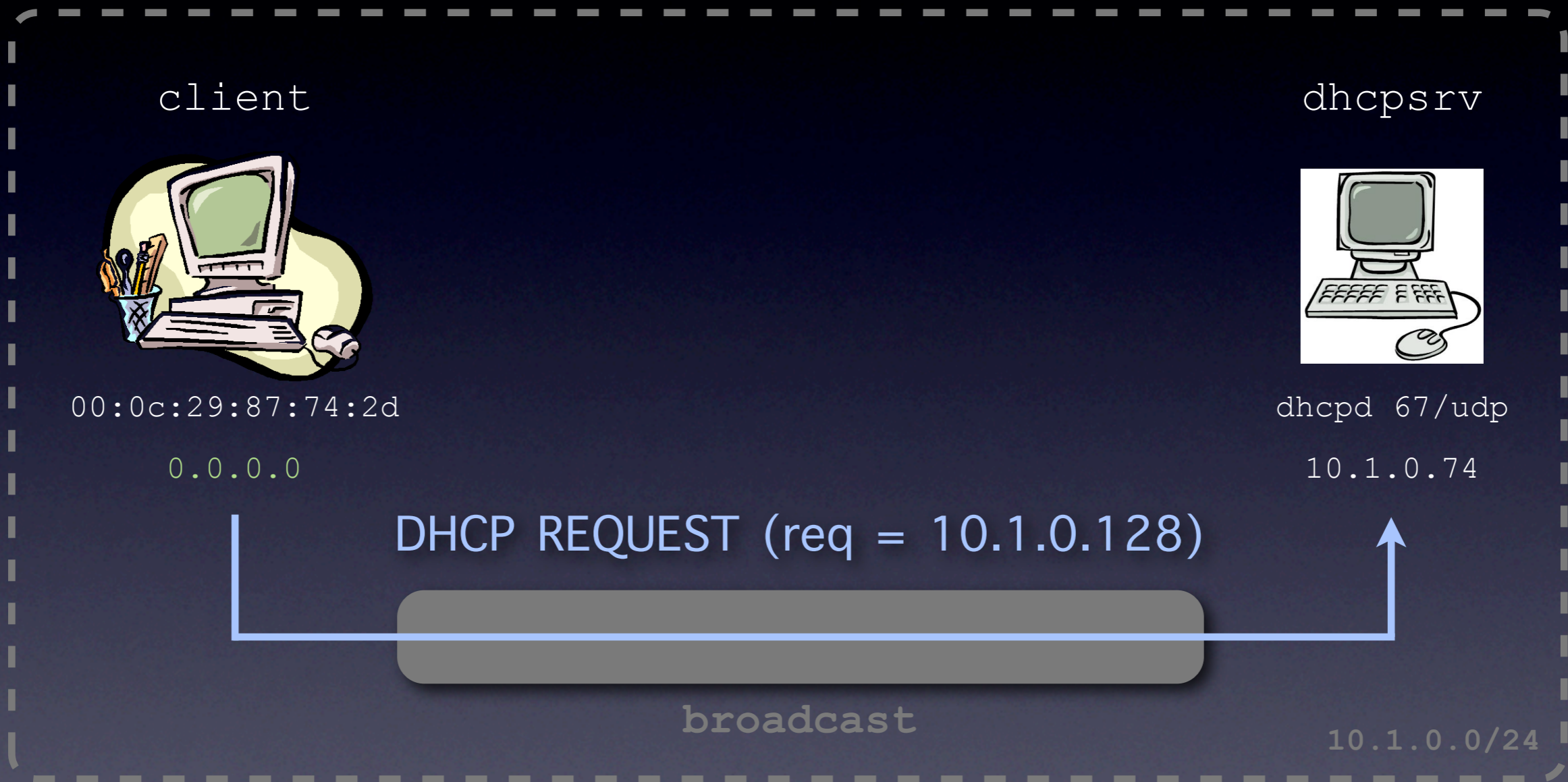
```
Feb 17 03:41:39 dhcpsrv dhcpcd: DHCPDISCOVER from 00:0c:29:87:74:2d via eth0
Feb 20 02:36:51 dhcpsrv dhcpcd: DHCPOFFER on 10.1.0.128 to b7:df:19:8f:00:fc via eth0
Feb 20 02:36:56 dhcpsrv dhcpcd: DHCPREQUEST for 10.1.0.128 from b7:df:19:8f:00:fc via eth0
Feb 20 02:36:56 dhcpsrv dhcpcd: DHCPACK on 10.1.0.128 to b7:df:19:8f:00:fc via eth0
```

[DHCP OFFER]



```
Feb 17 03:41:39 dhcprsv dhcprd: DHCPDISCOVER from 00:0c:29:87:74:2d via eth0
Feb 20 02:36:51 dhcprsv dhcprd: DHCPOFFER on 10.1.0.128 to b7:df:19:8f:00:fc via eth0
Feb 20 02:36:56 dhcprsv dhcprd: DHCPREQUEST for 10.1.0.128 from b7:df:19:8f:00:fc via eth0
Feb 20 02:36:56 dhcprsv dhcprd: DHCPACK on 10.1.0.128 to b7:df:19:8f:00:fc via eth0
```

[DHCP REQUEST]



```
Feb 17 03:41:39 dhcprsv dhcprd: DHCPDISCOVER from 00:0c:29:87:74:2d via eth0
Feb 20 02:36:51 dhcprsv dhcprd: DHCPOFFER on 10.1.0.128 to b7:df:19:8f:00:fc via eth0
Feb 20 02:36:56 dhcprsv dhcprd: DHCPREQUEST for 10.1.0.128 from b7:df:19:8f:00:fc via eth0
Feb 20 02:36:56 dhcprsv dhcprd: DHCPACK on 10.1.0.128 to b7:df:19:8f:00:fc via eth0
```

[DHCP ACK]

client

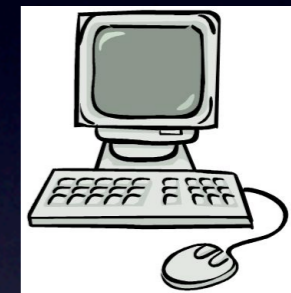


00:0c:29:87:74:2d

10.1.0.128

```
lease 10.1.0.128 {  
  starts 5 2009/02/17 02:36:56;  
  ends 5 2009/02/17 02:46:56;  
  binding state active;  
  next binding state free;  
  hardware ethernet 00:0c:29:87:74:2d;  
}
```

dhcprsv



dhcprd 67/udp

10.1.0.74

DHCP ACK

src = 10.1.0.74 : dst = 10.1.0.128

10.1.0.0/24

```
Feb 17 03:41:39 dhcprsv dhcprd: DHCPDISCOVER from 00:0c:29:87:74:2d via eth0  
Feb 20 02:36:51 dhcprsv dhcprd: DHCPOFFER on 10.1.0.128 to b7:df:19:8f:00:fc via eth0  
Feb 20 02:36:56 dhcprsv dhcprd: DHCPREQUEST for 10.1.0.128 from b7:df:19:8f:00:fc via eth0  
Feb 20 02:36:56 dhcprsv dhcprd: DHCPACK on 10.1.0.128 to b7:df:19:8f:00:fc via eth0
```

DHCP got owned !

RFC 2131 / Section 7



DHCP pool exhaust attack



00:0c:29:87:74:2d
0.0.0.0

DHCP DISCOVER

broadcast



00:0c:29:87:74:2e
0.0.0.0

DHCP DISCOVER

broadcast

[...]



00:0c:29:87:74:ab
0.0.0.0

DHCP DISCOVER

broadcast

```
subnet 10.1.0.0 netmask 255.255.255.0 {  
    range 10.1.0.128 10.1.0.254;  
}
```

dhcpsrv



dhcpcd 67/udp

10.1.0.74

DHCP pool exhaust attack



00:0c:29:87:74:2d
0.0.0.0

DHCP DISCOVER
(yiaddr = 10.1.0.128)

broadcast



00:0c:29:87:74:2e
0.0.0.0

DHCP DISCOVER
(yiaddr = 10.1.0.129)

broadcast

[...]



00:0c:29:87:74:ab
0.0.0.0

DHCP DISCOVER
(yiaddr = 10.1.0.254)

broadcast

```
subnet 10.1.0.0 netmask 255.255.255.0 {  
    range 10.1.0.128 10.1.0.254;  
}
```

dhcpsrv



dhcpcd 67/udp

10.1.0.74

DHCP pool exhaust attack



00:0c:29:87:74:2d
0.0.0.0

DHCP DISCOVER
(req = 10.1.0.128)

broadcast



00:0c:29:87:74:2e
0.0.0.0

DHCP DISCOVER
(req = 10.1.0.129)

broadcast

[...]



00:0c:29:87:74:ab
0.0.0.0

DHCP DISCOVER
(req = 10.1.0.254)

broadcast

```
subnet 10.1.0.0 netmask 255.255.255.0 {  
    range 10.1.0.128 10.1.0.254;  
}
```

dhcpsrv



dhcpcd 67/udp

10.1.0.74

DHCP pool exhaust attack



00:0c:29:87:74:2d
10.1.0.128

DHCP DISCOVER

broadcast



00:0c:29:87:74:2e
10.1.0.129

DHCP DISCOVER

broadcast

[...]



00:0c:29:87:74:ab
10.1.0.254

DHCP DISCOVER

broadcast

```
subnet 10.1.0.0 netmask 255.255.255.0 {  
  range 10.1.0.128 10.1.0.254;  
}
```



dhcpsrv

dhcpd 67/udp

10.1.0.74

```
lease 10.1.0.128 {  
  hardware ethernet 00:0c:29:87:74:2d;  
}  
lease 10.1.0.129 {  
  hardware ethernet 00:0c:29:87:74:2e;  
}  
[ ... ]  
lease 10.1.0.254 {  
  hardware ethernet 00:0c:29:87:74:ab;  
}
```



Exploiting DORA: attacks on the DHCP protocol

Phenoelit IRPAS



Felix “FX” Lindner (Hack In The Box)

FX is currently the Head of Research of Recurity Labs

What happens when DHCP server is located outside client's subnet ?

DHCP Relay Agent

DHCP RELAY [architecture]

client

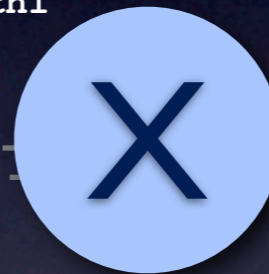
10.1.13.0/24



00:0c:29:87:74:2d

0.0.0.0

10.1.13.1 :eth1



dhcrelay 67/udp

10.1.0.0/24

eth0: 10.1.0.13

dhcpsrv



10.1.0.74

dhcpcd 67/udp

[DHCP DISCOVER]

client

10.1.13.0/24



00:0c:29:87:74:2d

0.0.0.0

DHCP DISCOVER

10.1.13.1 :eth1

broadcast

```
xid 0x2d38095d {  
  msg_type = DHCP DISCOVER;  
  chaddr = 00:0c:29:87:74:2d;  
}
```



dhcprelay 67/udp

10.1.0.0/24

eth0: 10.1.0.13

dhcpsrv



10.1.0.74

dhcpd 67/udp

```
Feb 17 03:41:39 dhcpsrv dhcpd: DHCPDISCOVER from 00:0c:29:87:74:2d via 10.1.13.1  
Feb 20 02:36:51 dhcpsrv dhcpd: DHCPOFFER on 10.1.0.128 to b7:df:19:8f:00:fc via 10.1.13.1  
Feb 20 02:36:56 dhcpsrv dhcpd: DHCPREQUEST for 10.1.0.128 from b7:df:19:8f:00:fc via 10.1.13.1  
Feb 20 02:36:56 dhcpsrv dhcpd: DHCPACK on 10.1.0.128 to b7:df:19:8f:00:fc via 10.1.13.1
```

DHCP DISCOVER (giaddr = 10.1.13.1)

src = 10.1.0.74 : dst = 10.1.13.1

[DHCP OFFER]

client

10.1.13.0/24



00:0c:29:87:74:2d

0.0.0.0

DHCP OFFER (yiaddr = 10.1.13.128)

10.1.13.1 :eth1

src = 10.1.13.1 : dst = 10.1.13.128

```
xid 0x2d38095d {  
  msg_type = DHCP DISCOVER;  
  chaddr = 00:0c:29:87:74:2d;  
}
```



dhcrelay 67/udp

10.1.0.0/24

eth0: 10.1.0.13

dhcpsrv



10.1.0.74

dhcpd 67/udp

```
Feb 17 03:41:39 dhcpsrv dhcpd: DHCPDISCOVER from 00:0c:29:87:74:2d via 10.1.13.1  
Feb 20 02:36:51 dhcpsrv dhcpd: DHCPOFFER on 10.1.0.128 to b7:df:19:8f:00:fc via 10.1.13.1  
Feb 20 02:36:56 dhcpsrv dhcpd: DHCPREQUEST for 10.1.0.128 from b7:df:19:8f:00:fc via 10.1.13.1  
Feb 20 02:36:56 dhcpsrv dhcpd: DHCPACK on 10.1.0.128 to b7:df:19:8f:00:fc via 10.1.13.1
```

DHCP OFFER (giaddr = 10.1.13.1, yiaddr = 10.1.13.128)

src = 10.1.0.74 : dst = 10.1.13.1

[DHCP REQUEST]

client

10.1.13.0/24



00:0c:29:87:74:2d

0.0.0.0

DHCP REQUEST (req = 10.1.13.128)

10.1.13.1 :eth1

broadcast

```
xid 0x2d38095d {  
  msg_type = DHCP REQUEST;  
  chaddr = 00:0c:29:87:74:2d;  
}
```



dhcrelay 67/udp

10.1.0.0/24

eth0: 10.1.0.13

dhcpsrv



10.1.0.74

dhcpcd 67/udp

```
Feb 17 03:41:39 dhcpsrv dhcpcd: DHCPDISCOVER from 00:0c:29:87:74:2d via 10.1.13.1  
Feb 20 02:36:51 dhcpsrv dhcpcd: DHCPOFFER on 10.1.0.128 to b7:df:19:8f:00:fc via 10.1.13.1  
Feb 20 02:36:56 dhcpsrv dhcpcd: DHCPREQUEST for 10.1.0.128 from b7:df:19:8f:00:fc via 10.1.13.1  
Feb 20 02:36:56 dhcpsrv dhcpcd: DHCPACK on 10.1.0.128 to b7:df:19:8f:00:fc via 10.1.13.1
```

DHCP REQUEST (giaddr = 10.1.13.1, req = 10.1.13.128)

src = 10.1.0.74 : dst = 10.1.13.1

[DHCP ACK]

client

10.1.13.0/24



00:0c:29:87:74:2d

10.1.13.128

DHCP ACK

10.1.13.1 :eth1

src = 10.1.13.1 : dst = 10.1.13.128

```
xid 0x2d38095d {  
  msg_type = DHCP REQUEST;  
  chaddr = 00:0c:29:87:74:2d;  
}
```



dhcprelay 67/udp

10.1.0.0/24

eth0: 10.1.0.13

```
lease 10.1.13.128 {  
  [ ... ]  
  hardware ethernet 00:0c:29:87:74:2d;  
}
```

dhcpsrv



10.1.0.74

dhcpd 67/udp

```
Feb 17 03:41:39 dhcpsrv dhcpd: DHCPDISCOVER from 00:0c:29:87:74:2d via 10.1.13.1  
Feb 20 02:36:51 dhcpsrv dhcpd: DHCPOFFER on 10.1.0.128 to b7:df:19:8f:00:fc via 10.1.13.1  
Feb 20 02:36:56 dhcpsrv dhcpd: DHCPREQUEST for 10.1.0.128 from b7:df:19:8f:00:fc via 10.1.13.1  
Feb 20 02:36:56 dhcpsrv dhcpd: DHCPACK on 10.1.0.128 to b7:df:19:8f:00:fc via 10.1.13.1
```

DHCP ACK (giaddr = 10.1.13.1)

src = 10.1.0.74 : dst = 10.1.13.1

What about the ...

EXTENDED DHCP exhausting attack ?

Proposed Architecture

10.1.0.0/24

```
subnet 10.1.15.0 netmask 255.255.255.0 {  
  range 10.1.15.2 10.1.13.254  
}
```



dhcpsrv (dhcpd 67/udp)

10.1.0.74

eth0: 10.1.0.15



10.1.0.13 :eth0



eth1: 10.1.13.1

10.1.15.1 :eth1
dhcrelay 67/udp



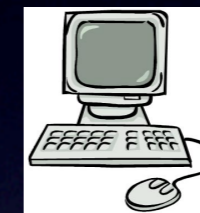
10.1.15.0/24

10.1.13.0/24

EXTENDED exhausting attack

10.1.0.0/24

```
subnet 10.1.15.0 netmask 255.255.255.0 {  
  range 10.1.15.2 10.1.13.254  
}
```



dhcpsrv (dhcpd 67/udp)

10.1.0.74

10.1.0.15 :eth0



eth0: 10.1.0.13



10.1.15.1 :eth1
dhcprelay 67/udp

eth1: 10.1.13.1



DHCP DISCOVER (giaddr = 10.1.15.1, charrd = 00:0c:29:87:74:2d)

src = 10.1.0.15 : dst = 10.1.0.74

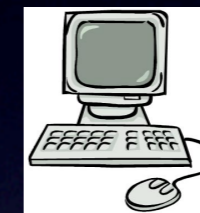
10.1.15.0/24

10.1.13.0/24

EXTENDED exhausting attack

10.1.0.0/24

```
subnet 10.1.15.0 netmask 255.255.255.0 {  
  range 10.1.15.2 10.1.13.254  
}
```



dhcpsrv (dhcpd 67/udp)

10.1.0.74

DHCP OFFER (giaddr = 10.1.15.1, yiaddr = 10.1.15.128)

src = 10.1.0.74 : dst = 10.1.15.128

10.1.0.15 :eth0



eth0: 10.1.0.13



10.1.15.1 :eth1
dhcprelay 67/udp

eth1: 10.1.13.1



10.1.15.0/24

10.1.13.0/24

EXTENDED exhausting attack

10.1.0.0/24

```
subnet 10.1.15.0 netmask 255.255.255.0 {  
  range 10.1.15.2 10.1.13.254  
}
```



dhcpsrv (dhcpd 67/udp)

10.1.0.74

10.1.0.15 :eth0



eth0: 10.1.0.13



10.1.15.1 :eth1
dhcprelay 67/udp

eth1: 10.1.13.1



DHCP REQUEST (giaddr = 10.1.15.1, req = 10.1.13.[2..254])

src = 10.1.0.15 : dst = 10.1.0.74

10.1.15.0/24

10.1.13.0/24

EXTENDED exhausting attack

10.1.0.0/24

```
lease 10.1.15.128 {  
  hardware ethernet 00:0c:29:87:74:2d;  
}
```

```
subnet 10.1.15.0 netmask 255.255.255.0 {  
  range 10.1.15.2 10.1.13.254  
}
```



dhcpsrv (dhcpd 67/udp)

10.1.0.74

DHCP ACK (giaddr = 10.1.15.1)

src = 10.1.0.74 : dst = 10.1.15.128

10.1.0.15 :eth0



eth0: 10.1.0.13



eth1: 10.1.13.1

10.1.15.1 :eth1

dhcrelay 67/udp



10.1.15.0/24

10.1.13.0/24

**repeat the process for 254 times, at maximum,
to exhaust the pool for 10.1.15.0/24**

EXTENDED exhausting attack

10.1.0.0/24

```
subnet 10.1.15.0 netmask 255.255.255.0 {  
  range 10.1.15.2 10.1.13.254  
}
```



dhcpsrv (dhcpd 67/udp)

10.1.0.74

DHCP OFFER (giaddr = 10.1.15.1, yiaddr = 10.1.15.[2..254])

src = 10.1.0.74 : dst = 10.1.15.[2..254]

10.1.0.15 :eth0



10.1.15.1 :eth1
dhcprelay 67/udp



254 x

DHCP DISCOVER (giaddr = 10.1.15.1, charrd = 00:0c:29:87:74:2d)

src = 10.1.0.15 : dst = 10.1.0.74

eth0: 10.1.0.13



eth1: 10.1.13.1

10.1.15.0/24

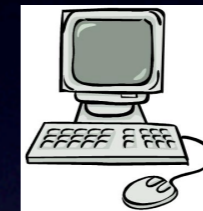
10.1.13.0/24

EXTENDED exhausting attack

10.1.0.0/24

```
lease 10.1.15.2 {  
  hardware ethernet 00:0c:29:87:74:2d;  
}  
  
[ ... ]  
  
lease 10.1.15.254 {  
  hardware ethernet 00:0c:29:87:74:ab;  
}
```

```
subnet 10.1.15.0 netmask 255.255.255.0 {  
  range 10.1.15.2 10.1.13.254  
}
```



dhcpsrv (dhcpd 67/udp)

10.1.0.74

DHCP ACK (giaddr = 10.1.15.1)

src = 10.1.0.74 : dst = 10.1.15.[2..254]

10.1.0.15 :eth0



10.1.15.1 :eth1
dhcprelay 67/udp



DHCP REQUEST (giaddr = 10.1.15.1, req = 10.1.13.[2..254])

src = 10.1.0.15 : dst = 10.1.0.74

eth0: 10.1.0.13



eth1: 10.1.13.1

10.1.15.0/24

10.1.13.0/24

**stop blabbering and
show me the code !**

Q & A



greet

- **Julio Cesar Fort**
 - for discussing attack details and giving support during first stages of the research
- **Bing Bong**
 - for providing good quality coffee that helps me to keep awake during night research sessions