Wireless Hacking

Getting onto a network, then what to do once you get there

What Makes Wireless Special?

- Clients on a wired network vs wireless
- Analogy: people with blindfolds
- Monitor mode vs Promiscuous
- How encryption factors in

WEP Cracking

- The different types of encryption
- WPS
- Why WEP is so vulnerable
- Aircrack

ARP spoofing

- You gained access, now what?
- Blindfolded people analogy
- MITM attack
- SSL strip
- note: no need for monitor mode

STOP

Demo time

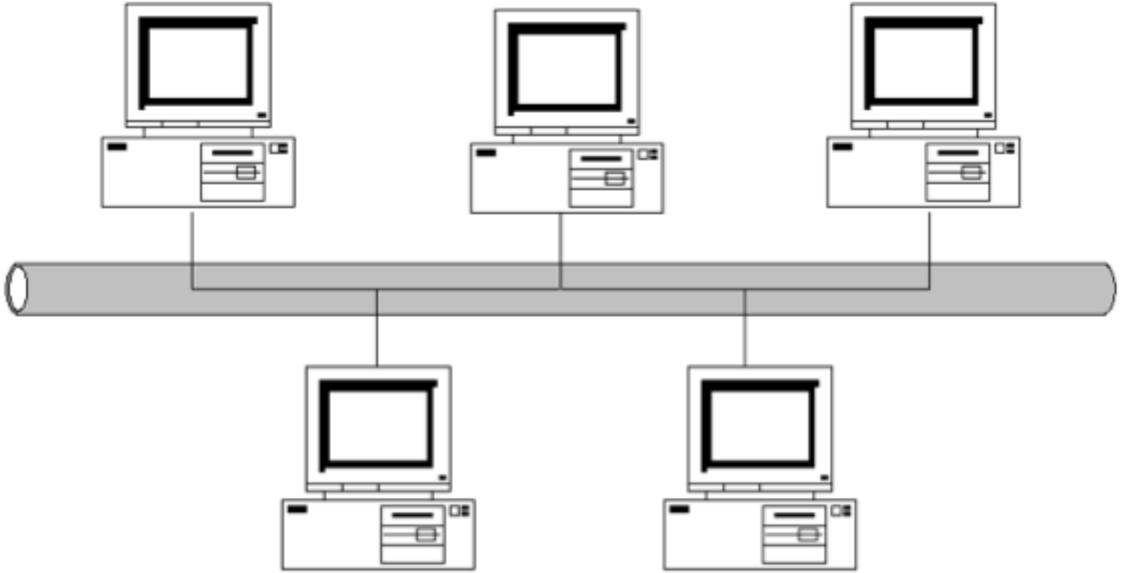
Networking

Hack Night 2015

Communicating

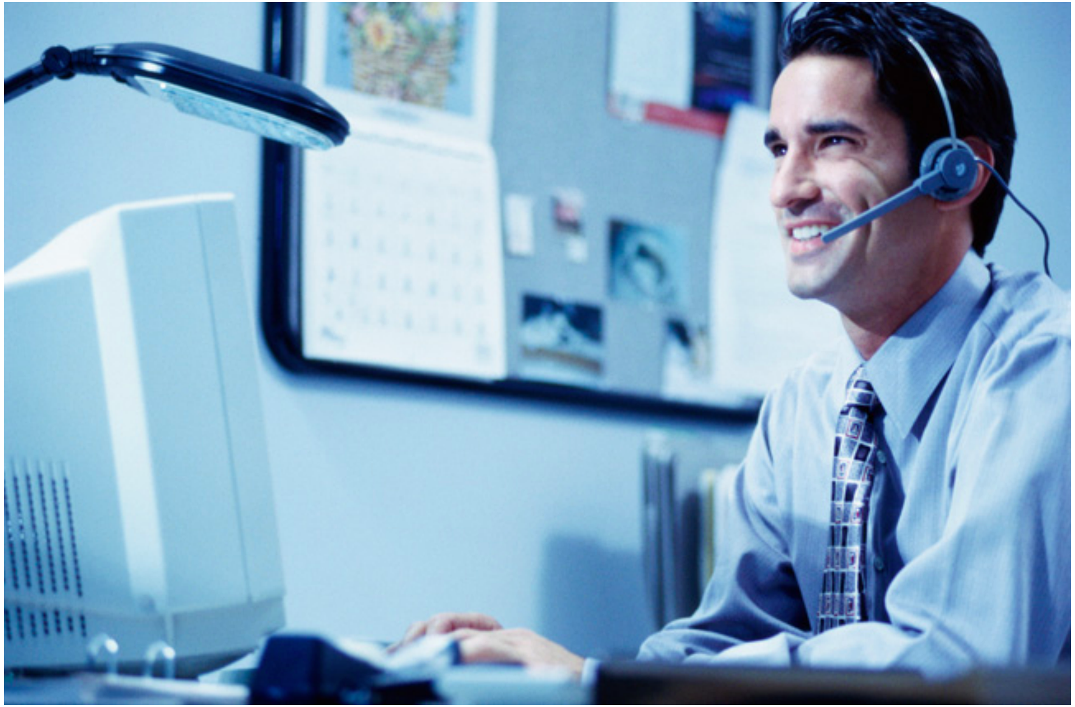
[4]

Sending and Receiving



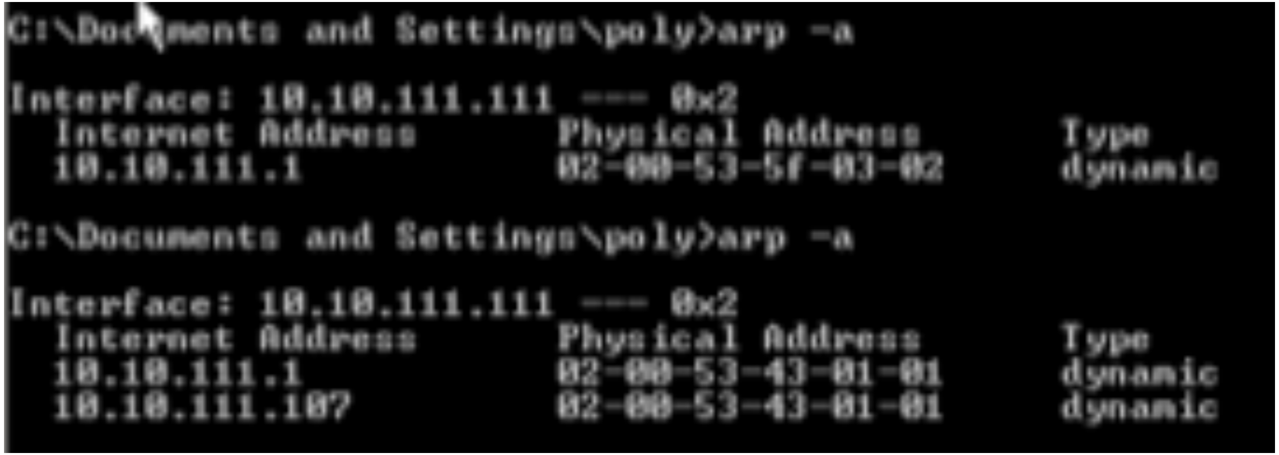
[1]

Help Desk



[5]

ARP Tables, MAC address, IP Address



```
C:\Documents and Settings\poly>arp -a

Interface: 10.10.111.111 --- 0x2
  Internet Address      Physical Address      Type
  10.10.111.1           02-00-53-5f-03-02     dynamic

C:\Documents and Settings\poly>arp -a

Interface: 10.10.111.111 --- 0x2
  Internet Address      Physical Address      Type
  10.10.111.1           02-00-53-43-01-01     dynamic
  10.10.111.107         02-00-53-43-01-01     dynamic
```

Packets

[2]

TCP vs UDP

Position
Flavor -TCP
Position
Flavor -UDP

“Woops I’ve Dropped It!”

[3]

DNS

https://howdns.works/

Domain to IP address: `nslookup ebay.com`

Ping/Pong: `ping google.com`

Following: `tracert google.com`

Tools

- Google Chrome Developer
  - Network
- Wireshark
  - Right click > Follow TCP Stream
  - File > Export Objects > HTTP
  - Using the filter

Exercise: picoCTF 2013

https://www.cloudshark.org/captures/f0741cdfee53

What is the author of the thing that this person is searching for?

Exercise: CSAW 2012

http://shell-storm.org/repo/CTF/CSAW-2012/Networking/100/

Hints:

What is the pcap file called?

What protocols are there within the pcap file?

Homework

The rest of the Networking challenges of CSAW 2012

http://shell-storm.org/repo/CTF/CSAW-2012/Networking/

Sauces

[1]: http://csawgirls.isis.poly.edu/2015ppts/1_Networks_Pt1_Naming.pptx

[2] & [3]: http://www.chriswrites.com/thetheory-behind-building-multiplayer-ios-apps/

[4]: http://busyevent.com/wp-content/uploads/2013/03/talking.jpg