

# Wireless Attack Methodology

## Table of Contents

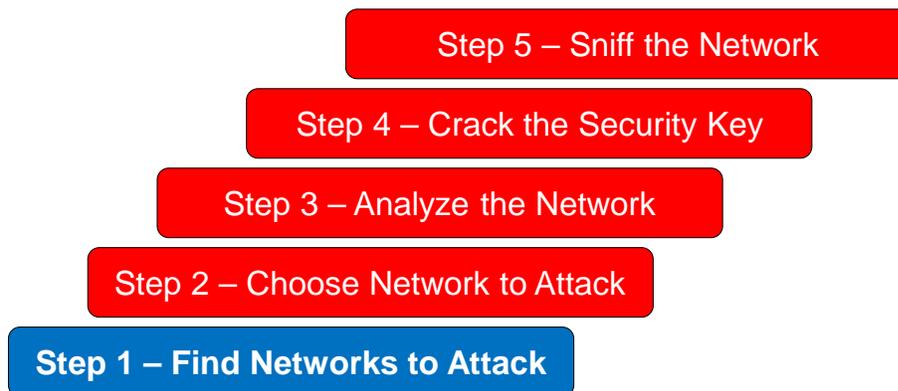
Wireless Attack Methodology – Step 1 .....	2
Wireless Attack Methodology – Step 2 .....	3
Wireless Attack Methodology – Step 3 .....	5
Wireless Attack Methodology – Step 4 .....	6
Wireless Attack Methodology – Step 5 .....	7
Detecting WLANs .....	8
Notices .....	10

# Wireless Attack Methodology – Step 1

---

## Find Networks

Using a scanning tool, such as NetStumbler, an attacker can map out potential wireless networks to target.



\*\*025 Wireless Attack Methodology.

Again, it wouldn't be ethical hacking without some type of well-defined process.

The first thing that you're going to want to do is find the various networks out there. How would you find a wireless network?

Student: Scan.

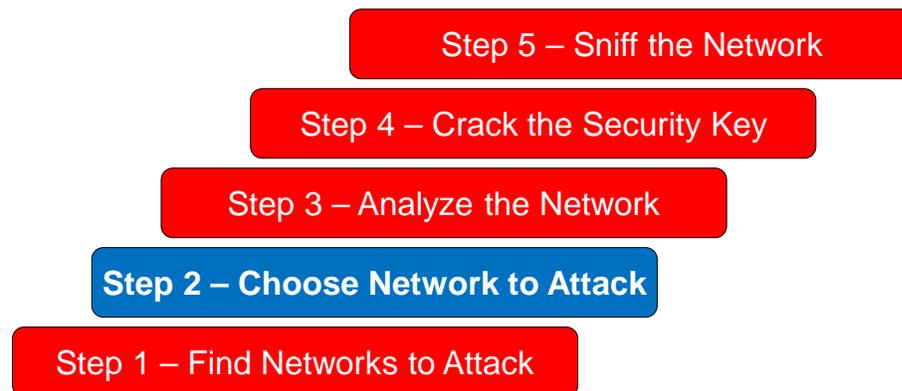
Chris Evans: Scan for it. Right? Run a tool that's picking up those beacon frames and consolidating it down. Yes. So you find networks that way. You can use tools like NetStumbler; and there's probably 20 or 30 different versions of tools out there that you can use for network discovery.

## Wireless Attack Methodology – Step 2

---

### Choose Network

Based on information gleaned from the scanning tool in Step 1, the attacker can select a network that meets the attacker's needs.



\*\*026 You pick a network to attack based on what you've picked up in your scanning. How do you determine which network you're going to attack? Let's say you've got a list of 20 networks, how do you pick one to focus on?

Student: The one without security.

Student: It's open.

Chris Evans: The one without security; maybe.

Student: Then by strength, I guess.

Chris Evans: By strength. So the one that's closest to you; maybe. What else? Which network actually connects to the network-- or which wireless device connects to the network that you're interested in?

Student: By name.

Chris Evans: By name; yes. So you pick the access point that's actually going to get you what you want.

Again, a list of 20 access points, not all of them may, you know, lead you to the network that you're doing an assessment on; or something like that. So you need to use whatever information you've got at your disposal to pick the right one.

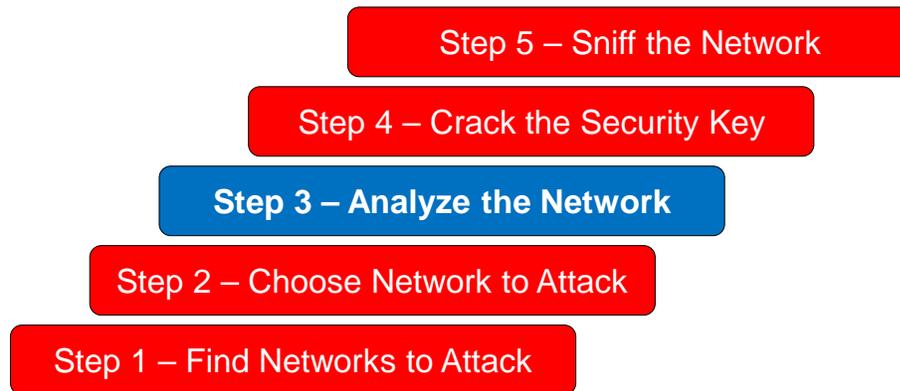
You don't want to spend time breaking into a network only to realize that oh, this is Billy-Bo-Bob's home wireless network, and not Company X that I was supposed to break into.

## Wireless Attack Methodology – Step 3

---

### Analyze Network

The scanning tools give the attacker all the information needed to determine the network's specific configuration (channel, encryption, etc.).



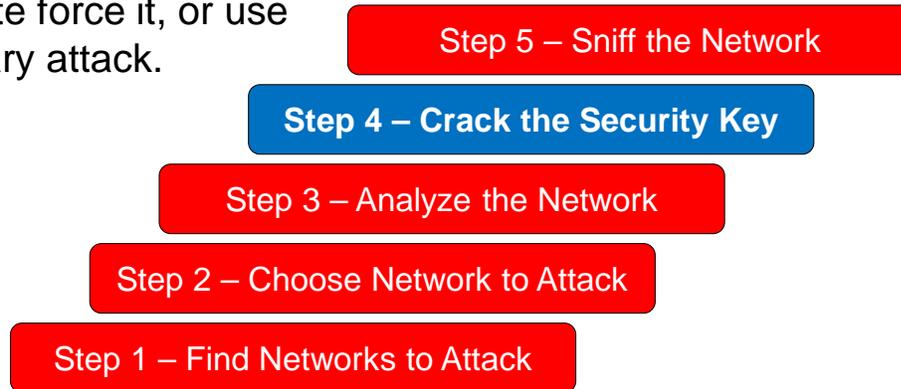
\*\*027 You can analyze the network; determine the channel, any type of encryption properties on it. You may actually get underlying network details, because you're able to sniff that. So you might know what the IP address is or the gateway IP address on the inside is. You might be able to figure out if there's internet access behind it, or what network it connects to.

## Wireless Attack Methodology – Step 4

---

### Crack Security

The attacker can monitor and capture wireless network traffic; once a large enough dataset is obtained, the attacker can then run it through WEPCrack or aircrack-ng to break the security keys, brute force it, or use a dictionary attack.



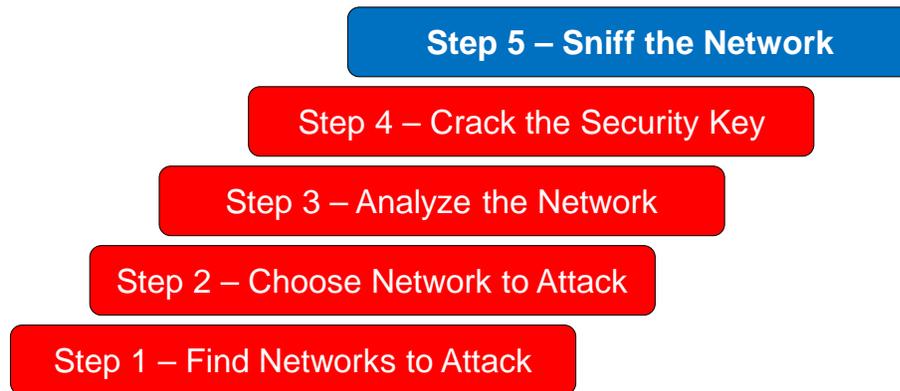
\*\*028 The next step is to crack the security key, or the encryption key on it. So you can capture wireless traffic, run it through crackers. You can do brute forcing or Rainbow table lookups. Generally any type of attack with passwords applies to cracking the security key on encryption- on encrypted networks.

## Wireless Attack Methodology – Step 5

---

### Sniff Network

Once the encryption is broken, the attacker can use the network as a “legitimate” client, sniff for usernames and passwords, or attempt further attacks on the underlying network.



\*\*029 And the last thing you're going to do is you're actually going to join the network and start looking at the traffic on it and maybe running attacks at underlying systems or servers that connect to that access point.

So you've gone from I found the network, I know which one I'm going to go against; I know what kind of encryption it's got, break out the encryption and then connect to it.

## Detecting WLANs

---

Use Operating System tools such as wireless network discovery built-in to Windows or Airport for MAC.

Use handheld devices specifically designed to detect wireless networks, or small hand-held PCs, or a smart phone!

Use passive scanners such as Kismet or KisMAC when you may be concerned with someone discovering your actions.

Use active scanners such as NetStumber, when you're not concerned with being detected.



\*\*030 So a little bit more on detecting wireless LANs. How do you actually go about doing this?

There are operating system based tools certainly built into Windows, and some built into Linux, that you can use to detect access points that are beaconing out. There are handheld, little handheld devices that will do WiFi detection for you and show you what networks are around.

You can use your phone. There are programs available to do that on your phone.

There are various passive scanners out there, like Kismet or KisMAC, that all they do is sit there and accept beacon frames from everybody else.

What type of attack is this? Is this active or passive? Where you're just sitting there listening for--

Student: Passive.

Student: Passive.

Chris Evans: It's a passive attack. Again, you're not sending anything, you're just listening for the broadcast from the access points.

Or you can use a more active scanner like NetStumbler, which is going to broadcast out packets and see who responds to it.

## Notices

# Notices

---

Copyright 2013 Carnegie Mellon University

This material has been approved for public release and unlimited distribution except as restricted below.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

NO WARRANTY. THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark of Carnegie Mellon University.