CLOSE ACCESS

Introduction to BADDECISION

December 15-16, 2010

CLOSE ACCESS

Classification

The overall classification of this presentation is

TOP SECRET//COMINT//NOFORN

All slides and materiels contained in this presentation should be considered classified TS//SI//NF

(unless otherwise noted)

CLOSE ACCESS

Section Overview

- BADDECISION Overview
- BADDECISION Components
- BADDECISION Prerequisites
- BADDECISION Operational Flow
- BADDECISION Step Through
- Instructor-led Demos and Labs
- BADDECISION Pros / Cons

At The End…

CLOSE ACCESS

You should be able to….

- Understand BADDECISION Components
- Understand the BADDECISION Prereqs.
- Conduct a BADDECISION Operation.
- List the Pros / Cons of NIGHTSTAND.

BADDECISION Overview

CLOSE ACCESS

- BADDECISION is an "802.11 CNE tool that uses a true man-in-the-middle attack and a frame injection technique to redirect a target client to a FOXACID server."
- Takes advantage of shared open medium and the HTTP protocol.
- Works for WPA / WPA2!

BADDECISION Prerequisites

CLOSE ACCESS

- **Working BLINDDATE Survey!**

- Client on the Target network
- Security Level: WPA / WPA2
- Ability to maintain a reliable connection to a target network.

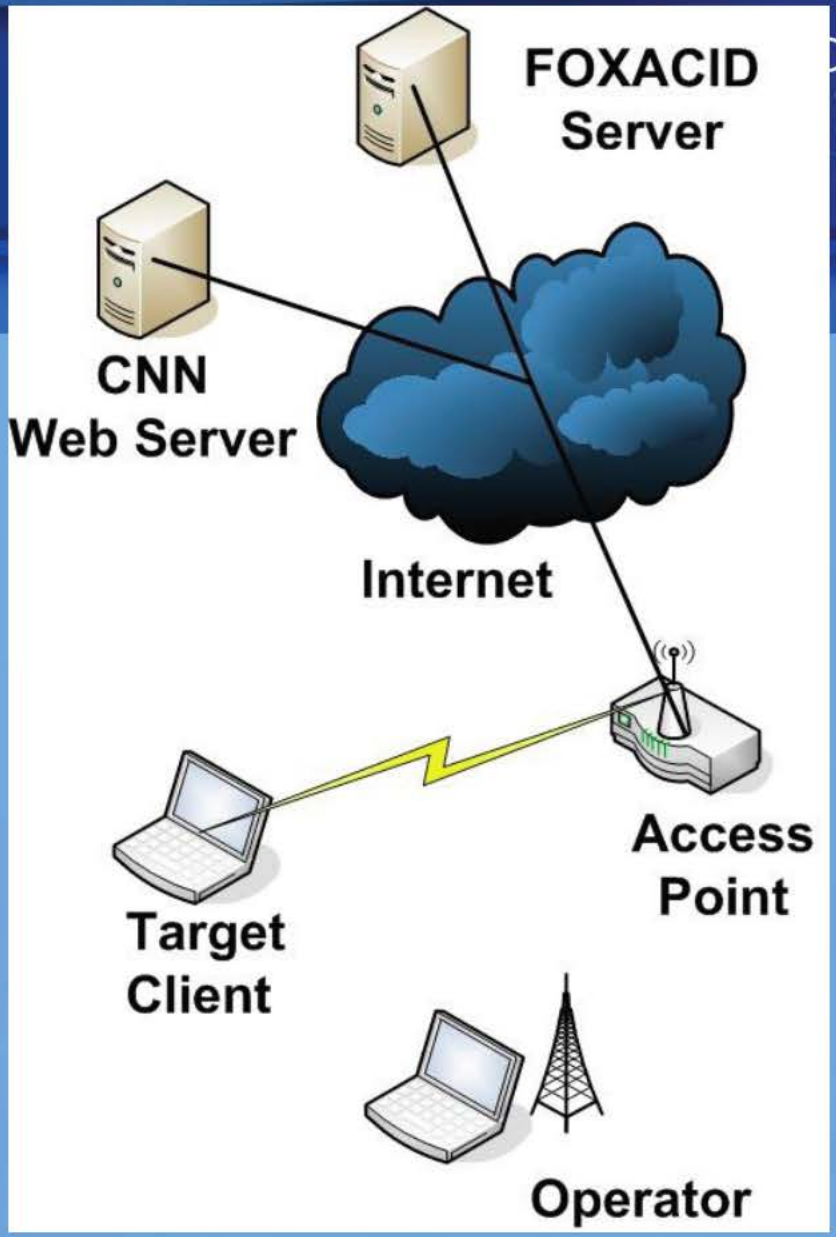
- Don't forget FOXACID Tag!

BADDECISION Components

CLOSE ACCESS

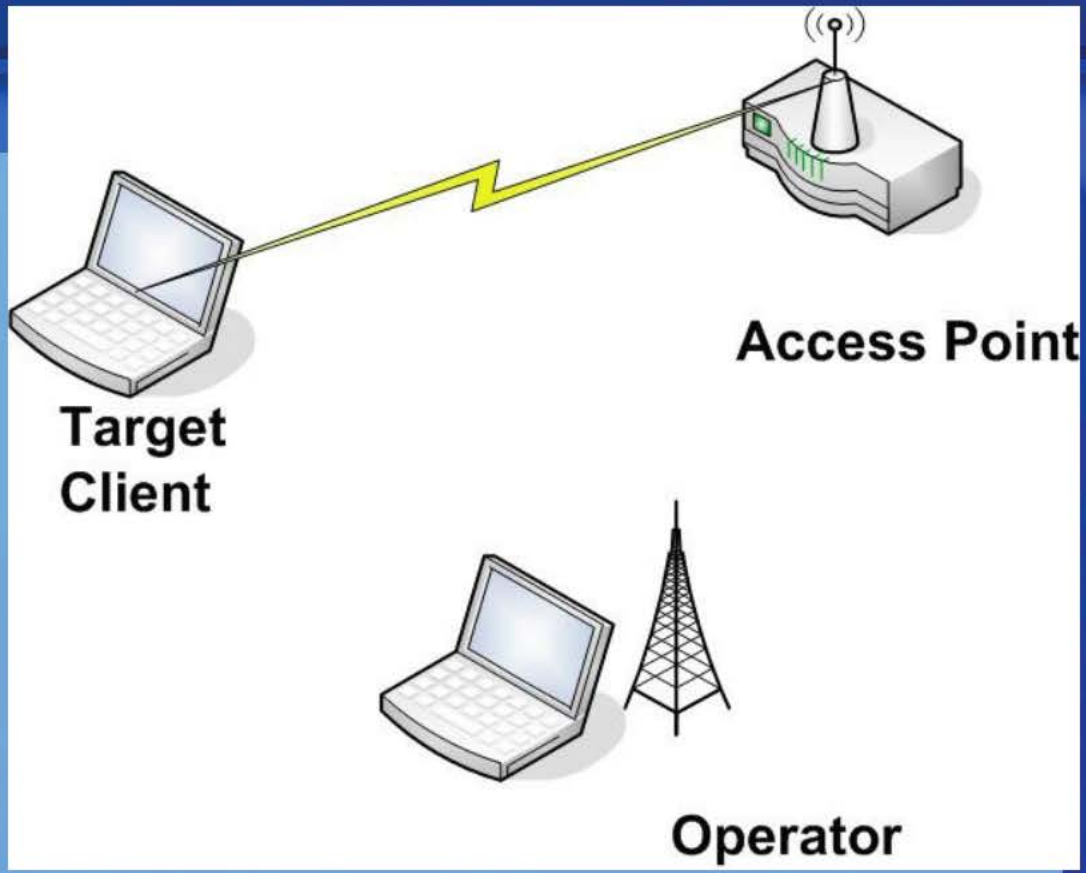
- HAPPYHOUR
- SECONDDATE
- Open Sources Tools
  - macchanger
  - wireshark
  - nmap
  - ettercap

BADDECISION
Preparation



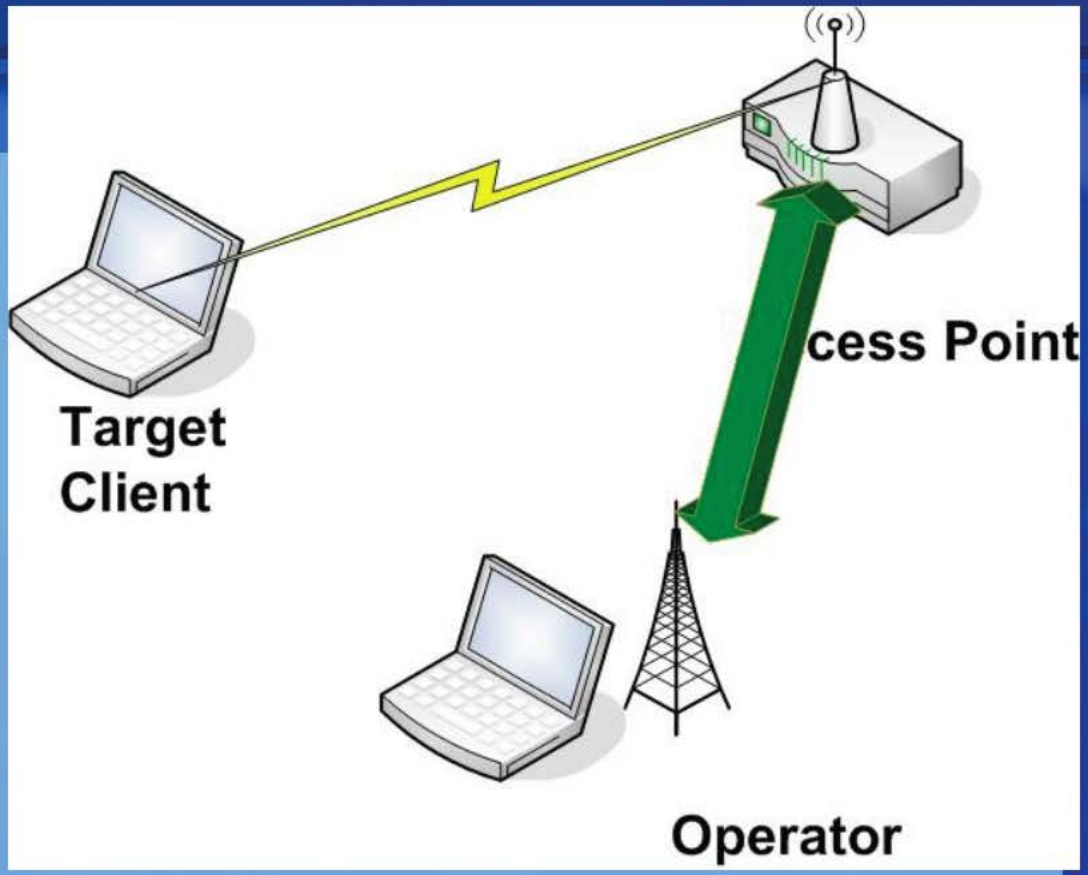
CLOSE ACCESS

BADDECISION
Preparation



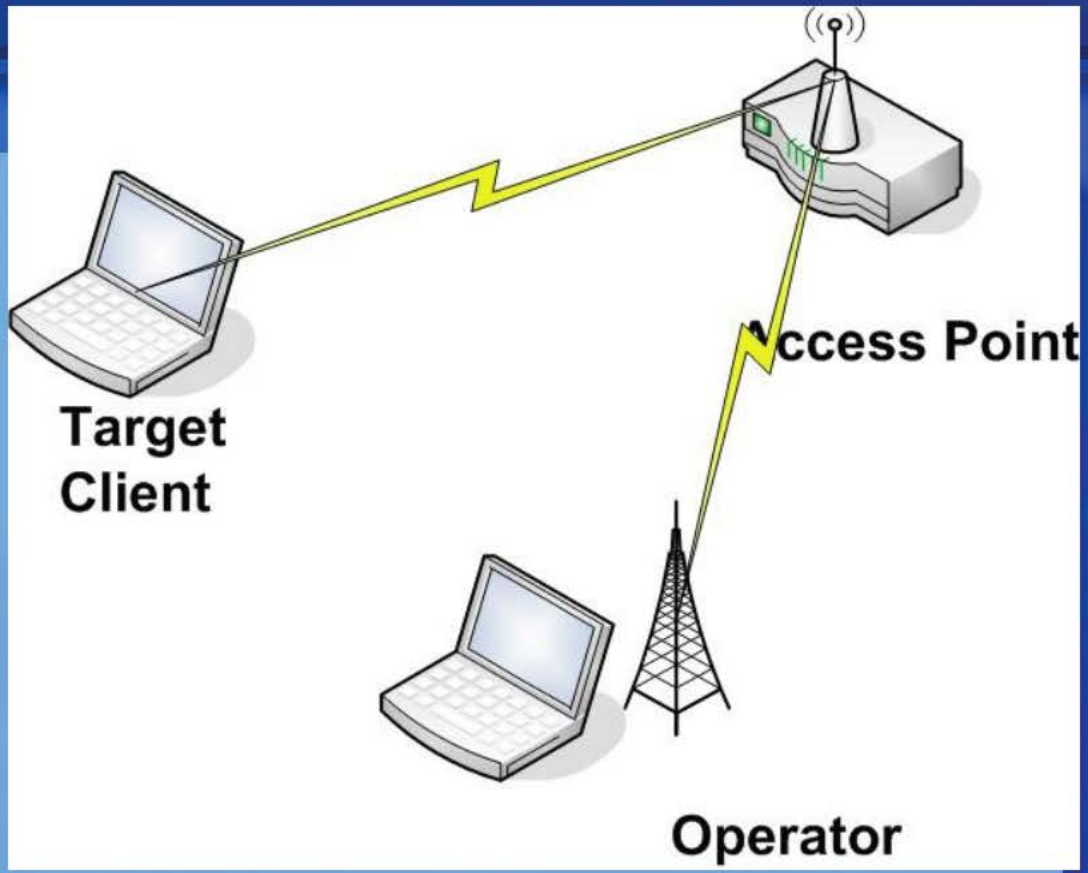
CLOSE ACCESS

BADDECISION
Preparation



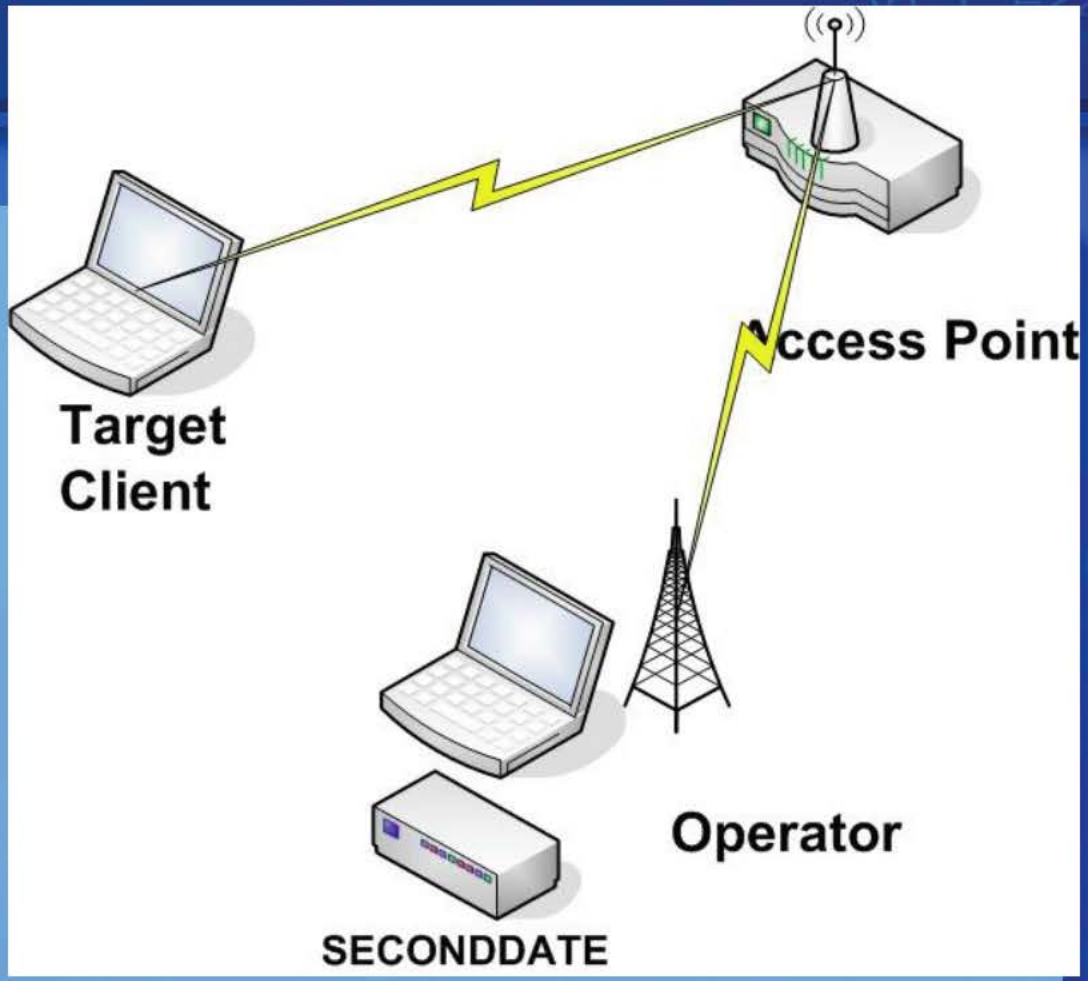
CLOSE ACCESS

BADDECISION
Preparation



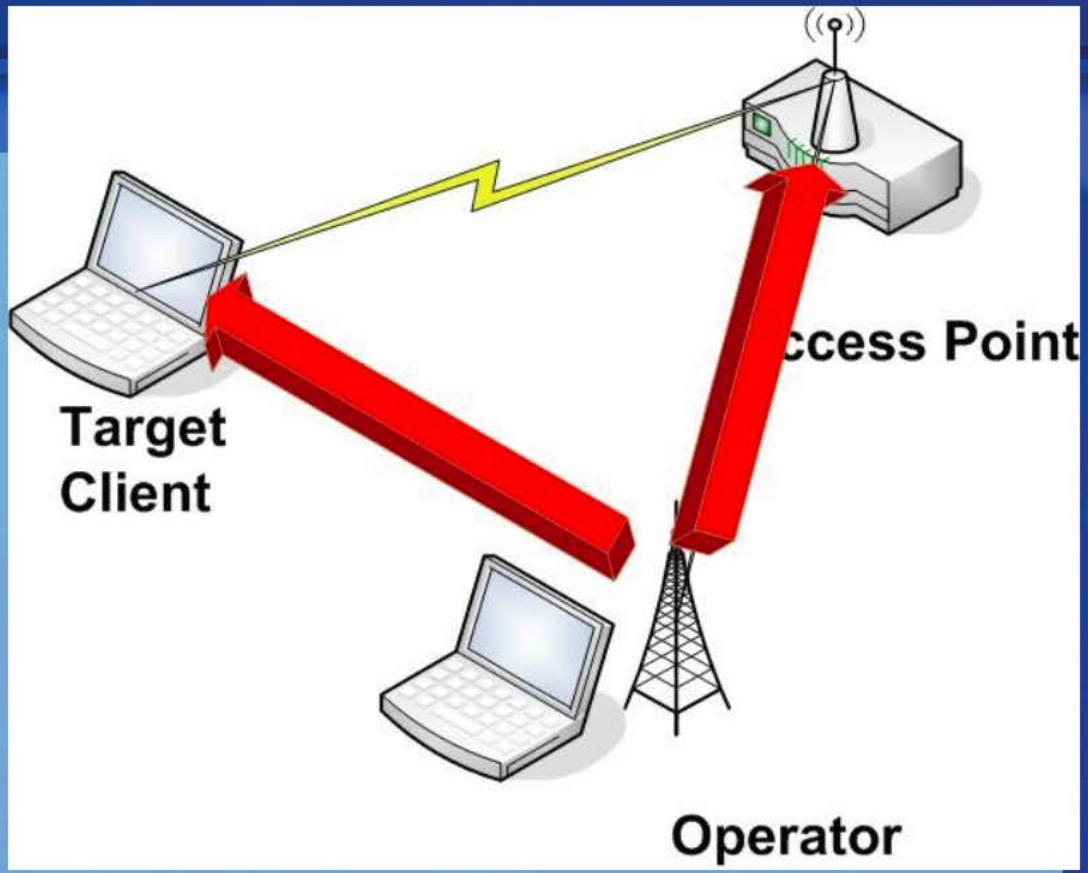
CLOSE ACCESS

BADDECISION
Preparation



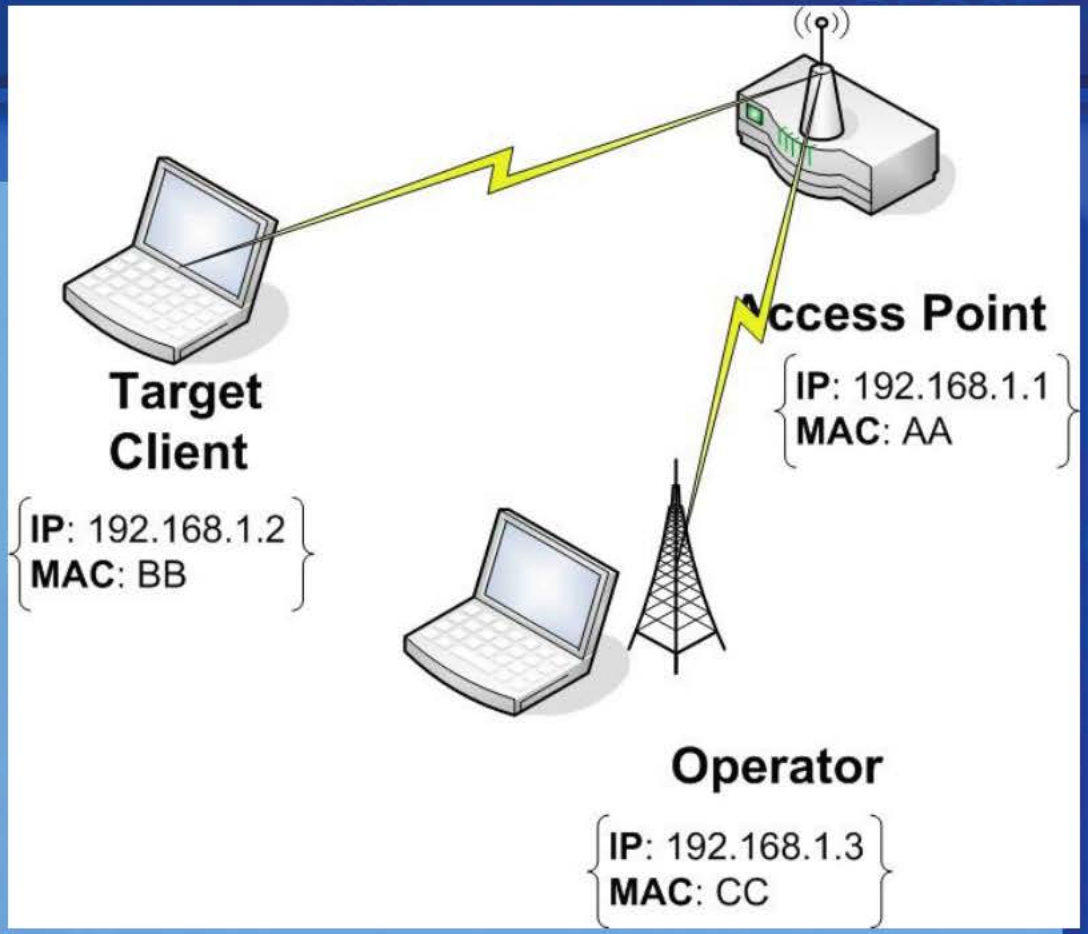
CLOSE ACCESS

BADDECISION
Preparation



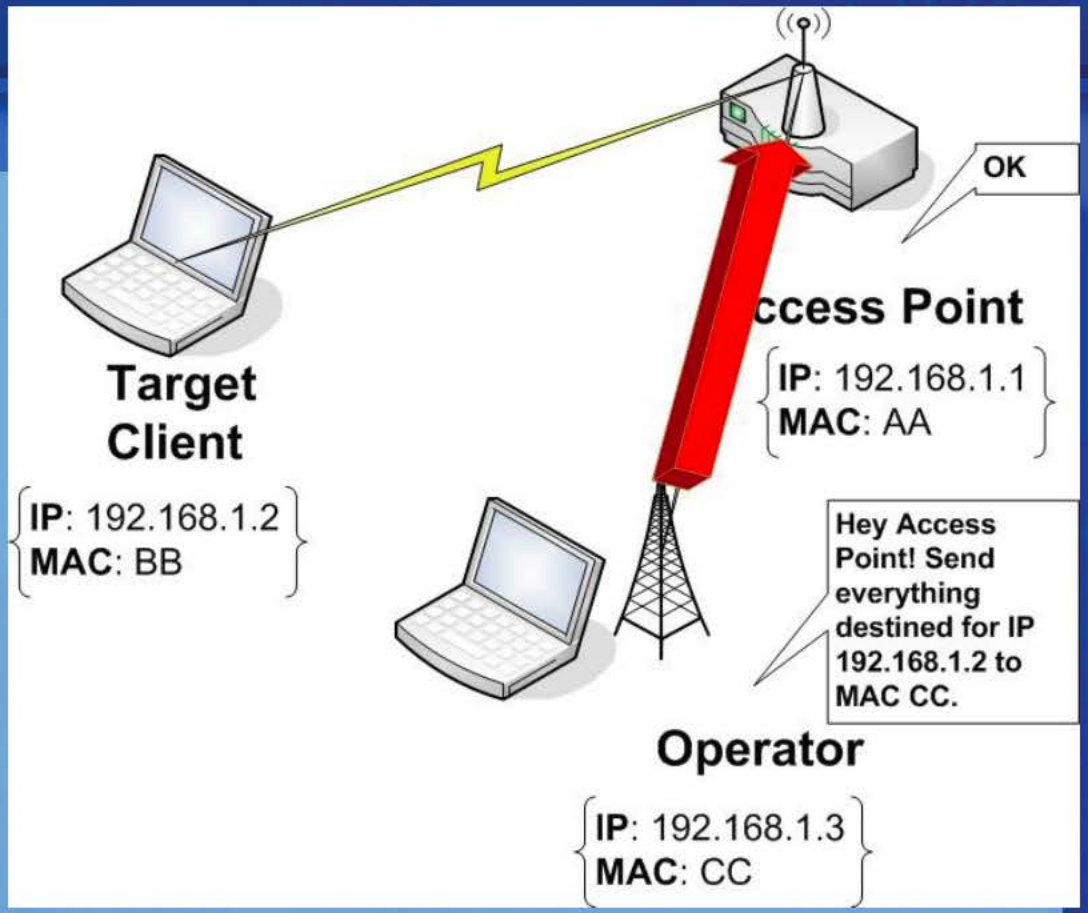
CLOSE ACCESS

BADDECISION
Preparation



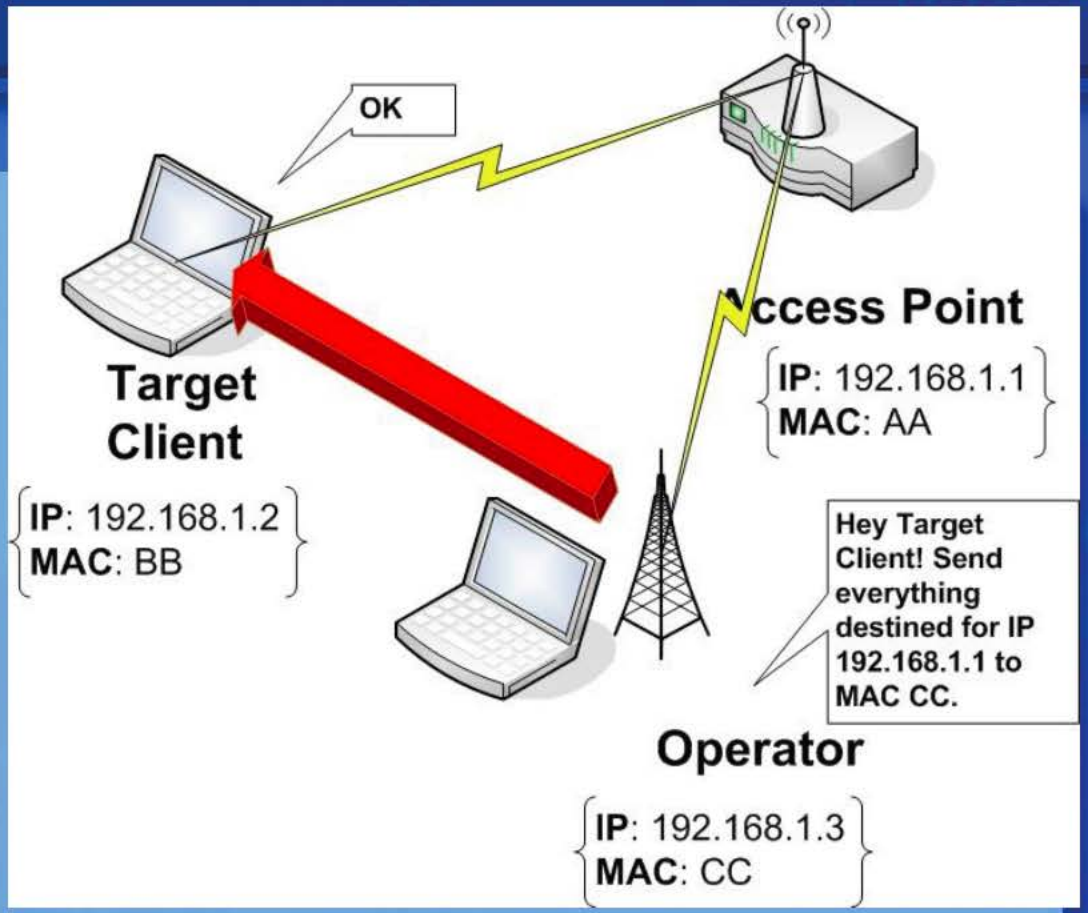
CLOSE ACCESS

BADDECISION
Preparation



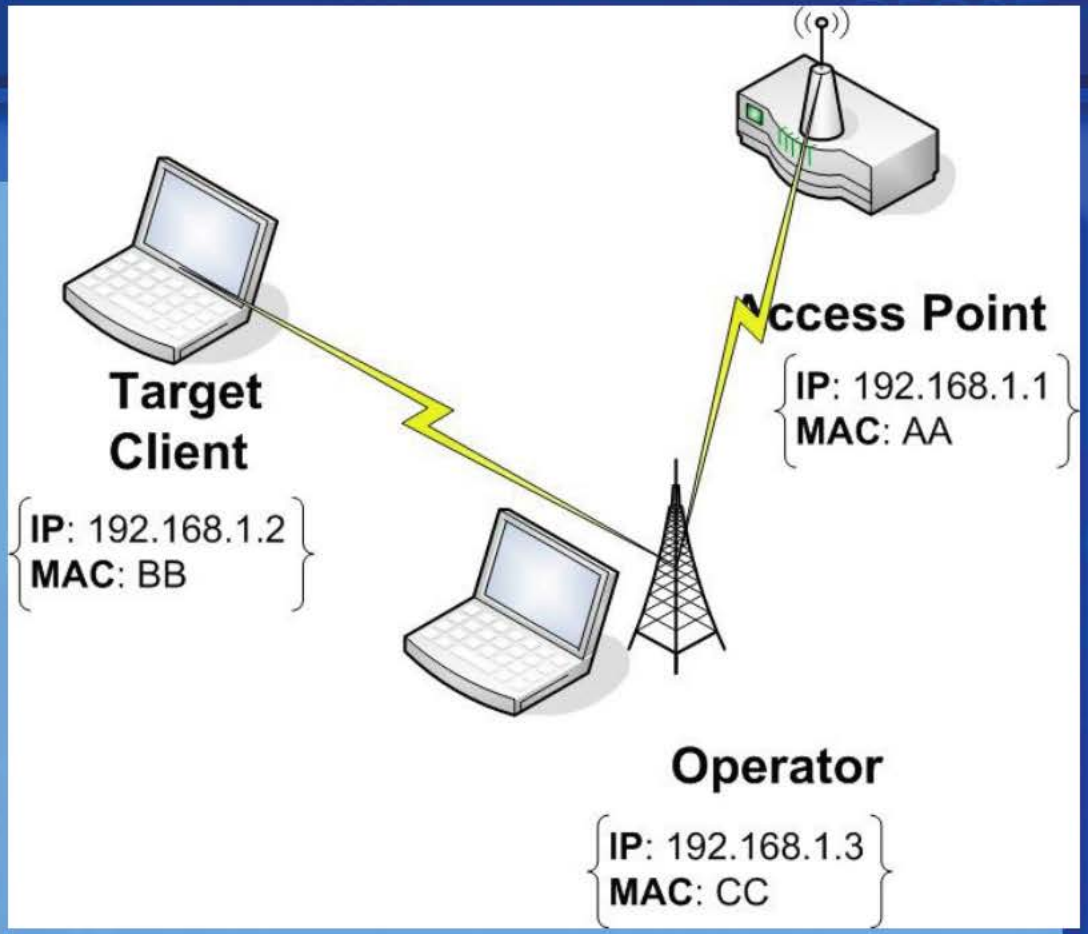
CLOSE ACCESS

BADDECISION
Preparation



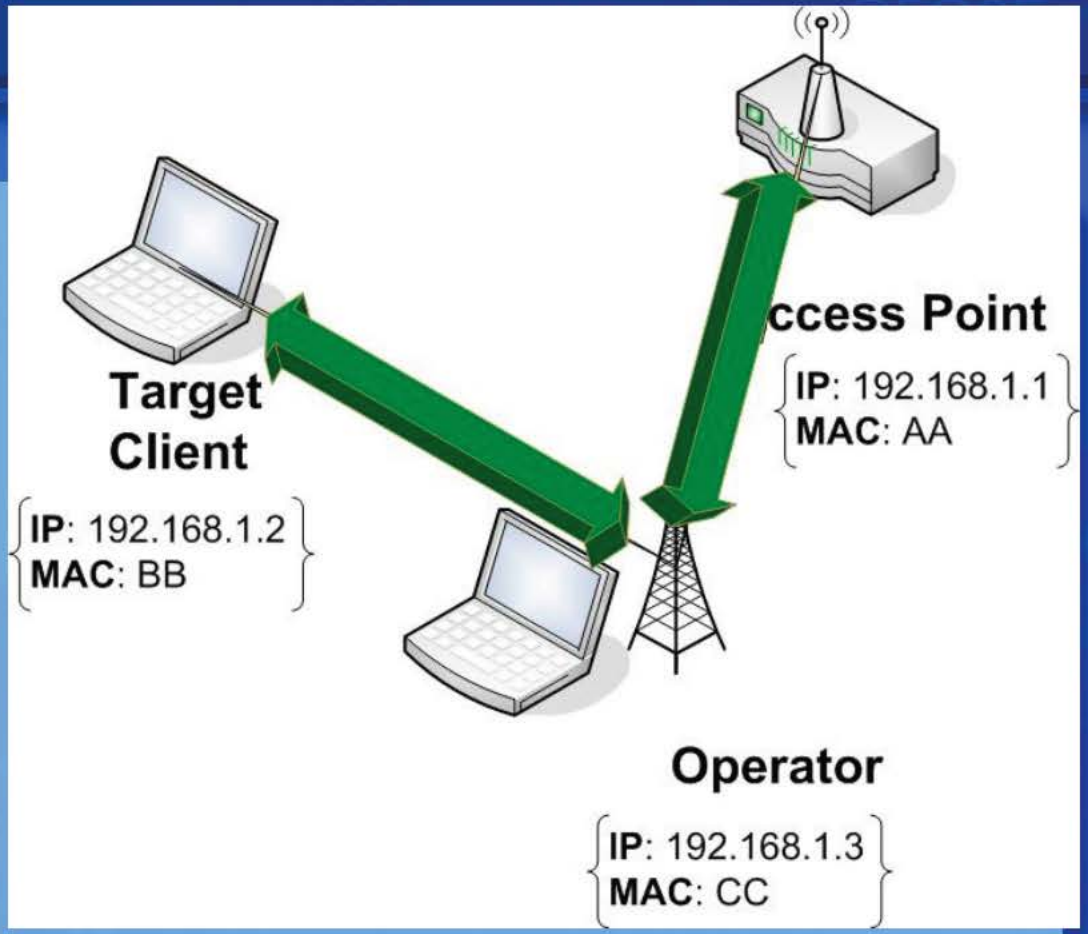
CLOSE ACCESS

BADDECISION
Preparation



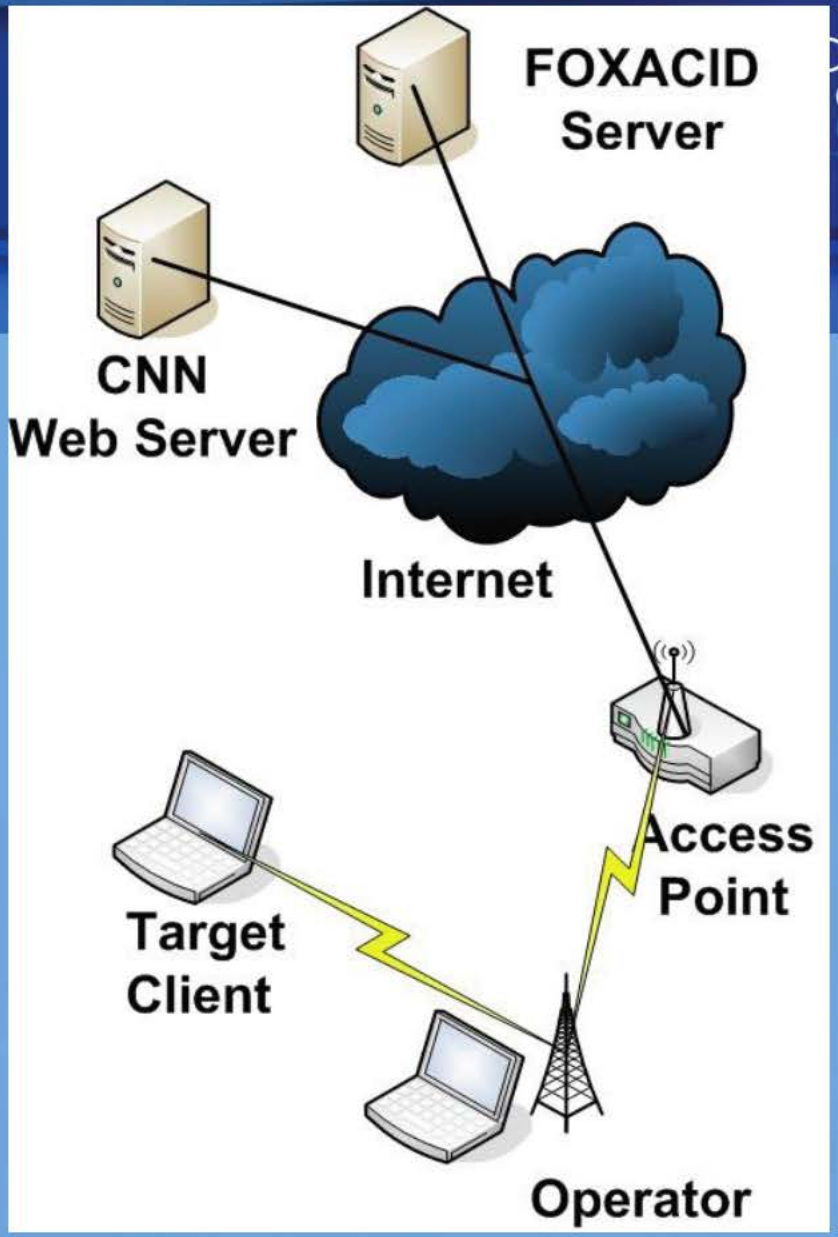
CLOSE ACCESS

BADDECISION
Preparation



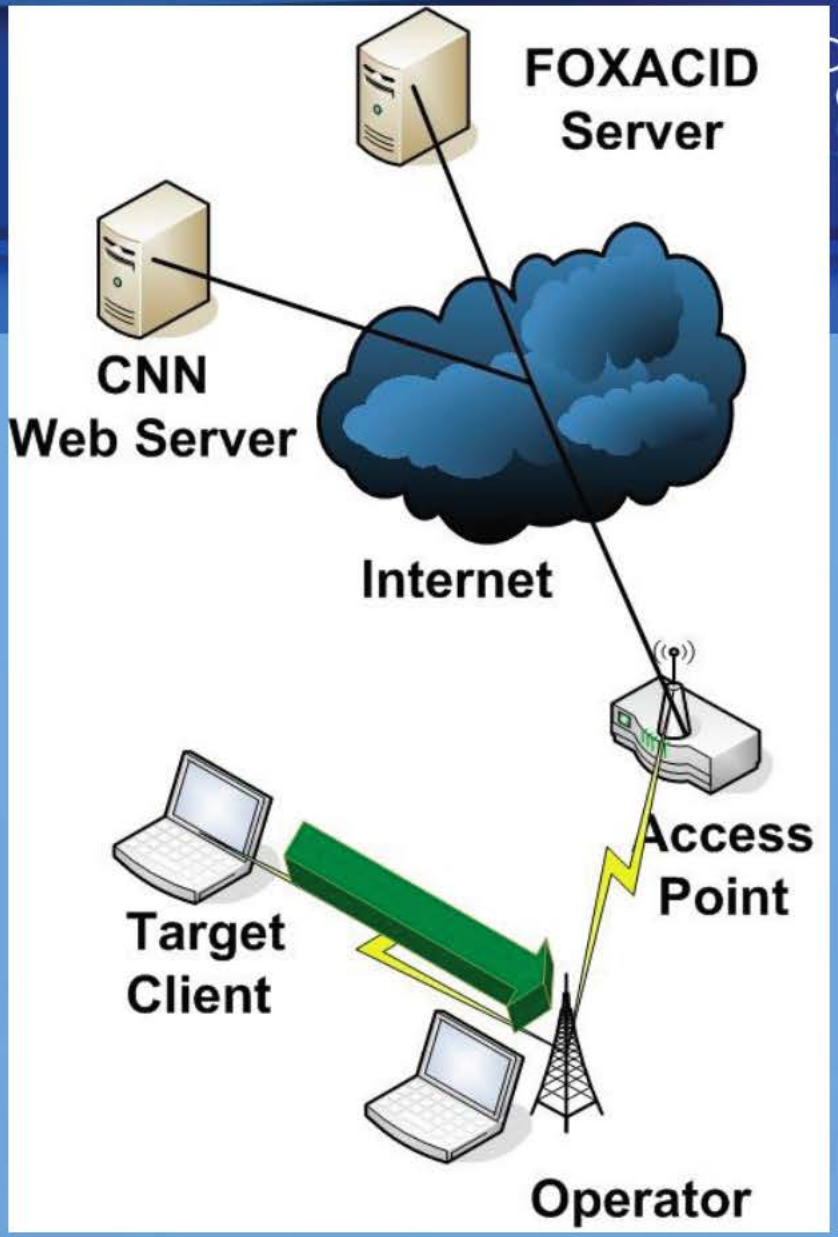
Overview of Operational Scenario

- Operator with BLINDDATE System.
- FOXACID Tag issued for Target.
- Target Client browsing the Internet via web browser ☺



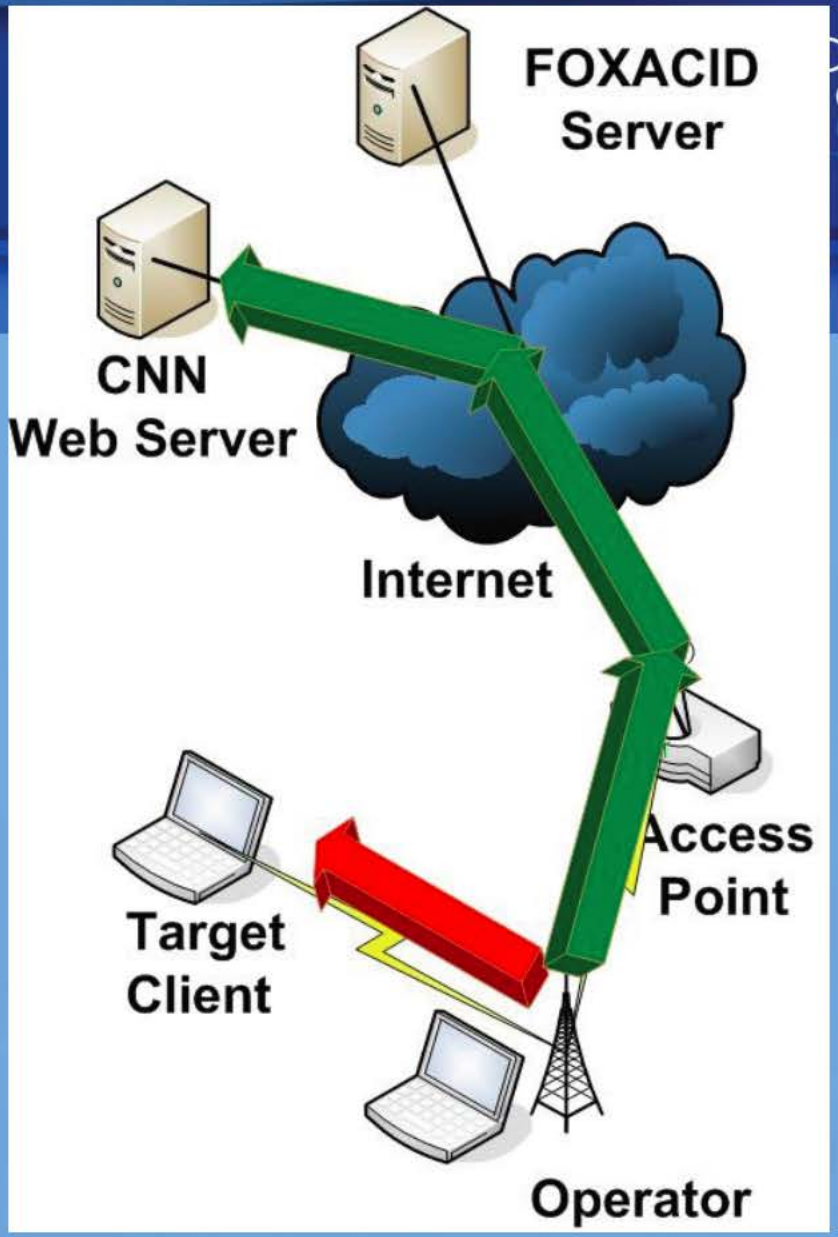
Webpage Request

- Target issues HTTP GET Request to webpage of interest (cnn.com)



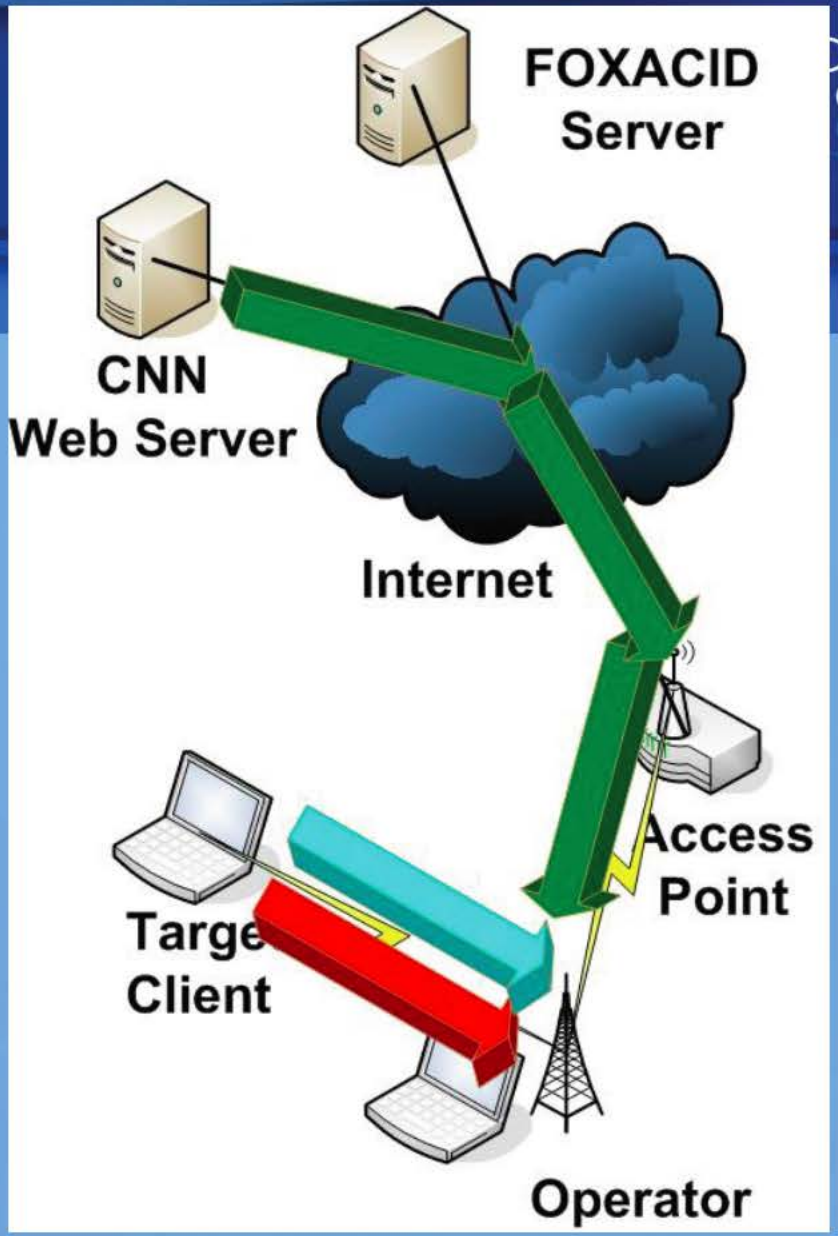
Injection

- Operate uses SECONDDATE to inject a redirection payload at Target Client.
- Target Client's original HTTP GET Request continues on it's normal path.



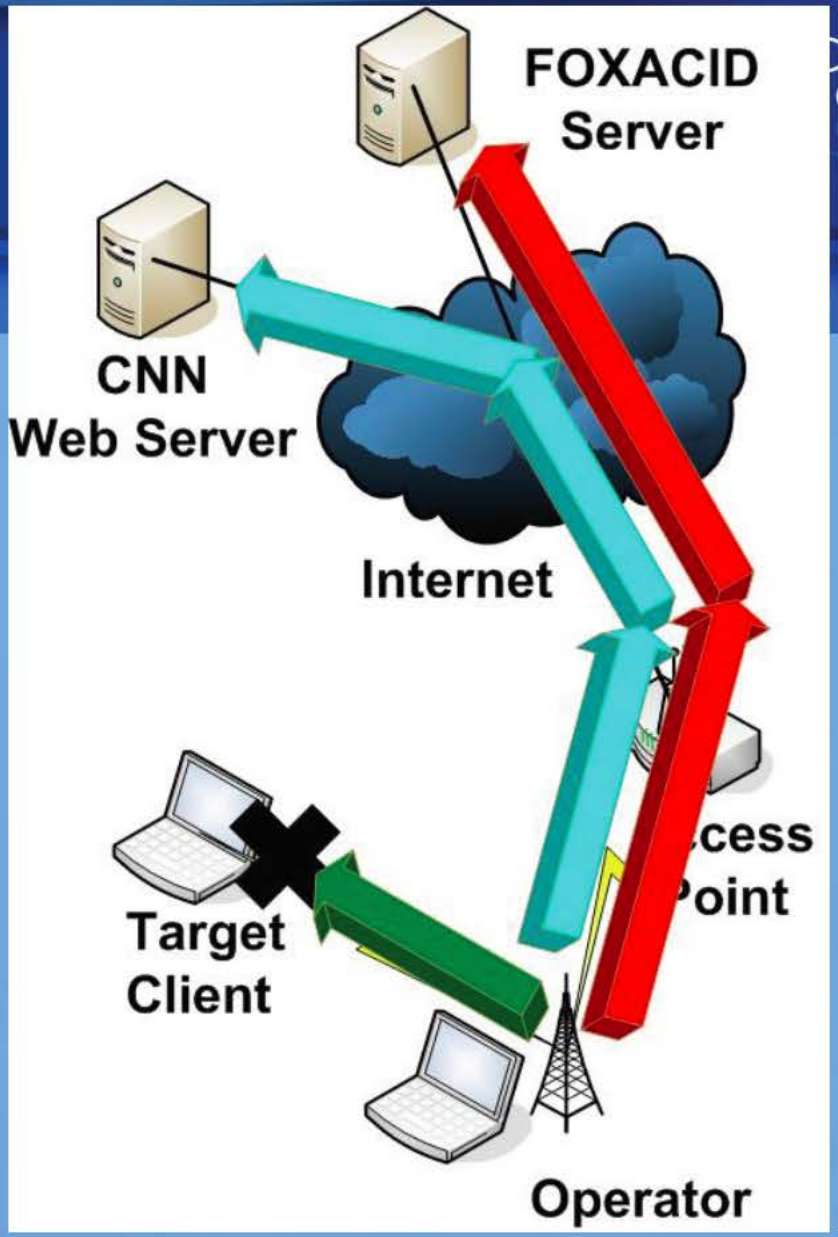
Refresh and Covert Request

- Injected payload forces Target Client to refresh and send another HTTP GET Request to desired webpage.
- Covert Request is issued by Target Client to FOXACID Server.



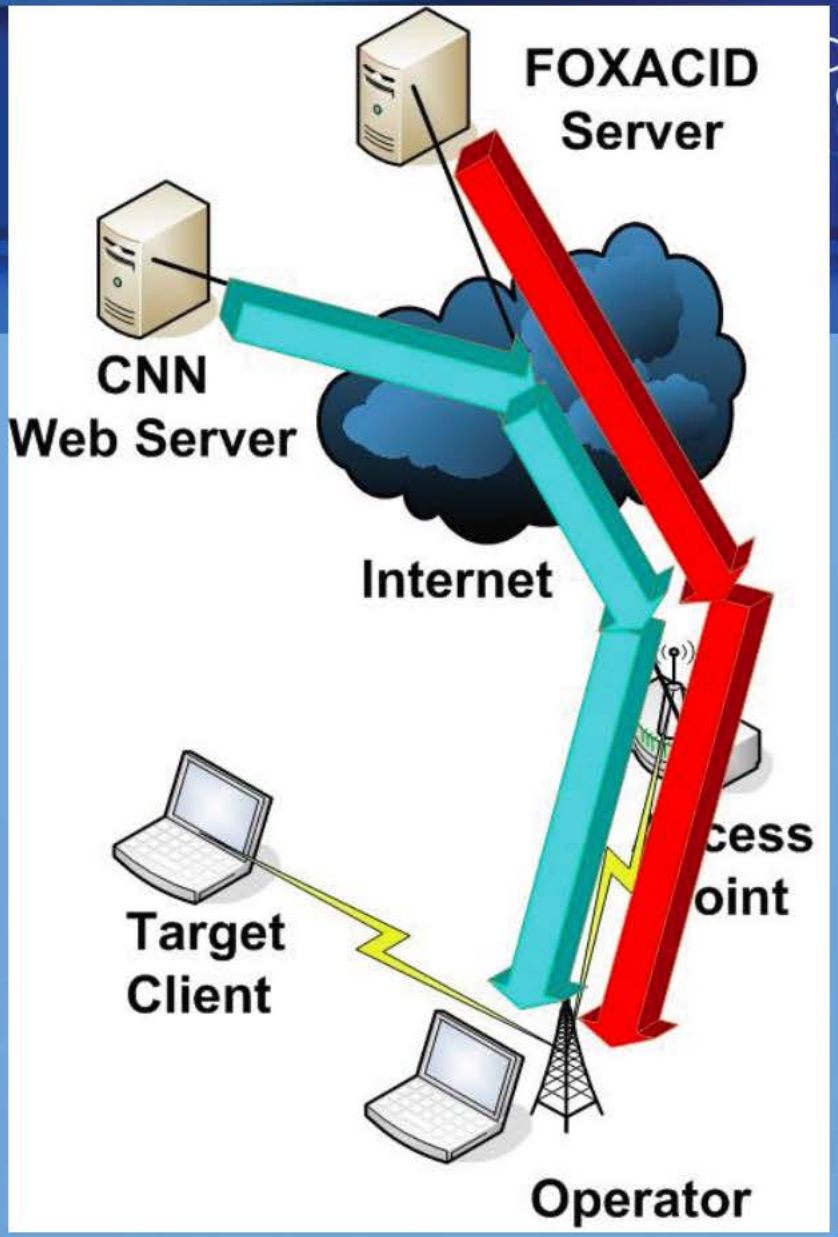
FOXACID
Request Received

- FOXACID receives request from entity.
- Entity is validated as Target Client by FOXACID Tag.
- Response to original HTTP GET Request is dropped (but don't worry, that's good)



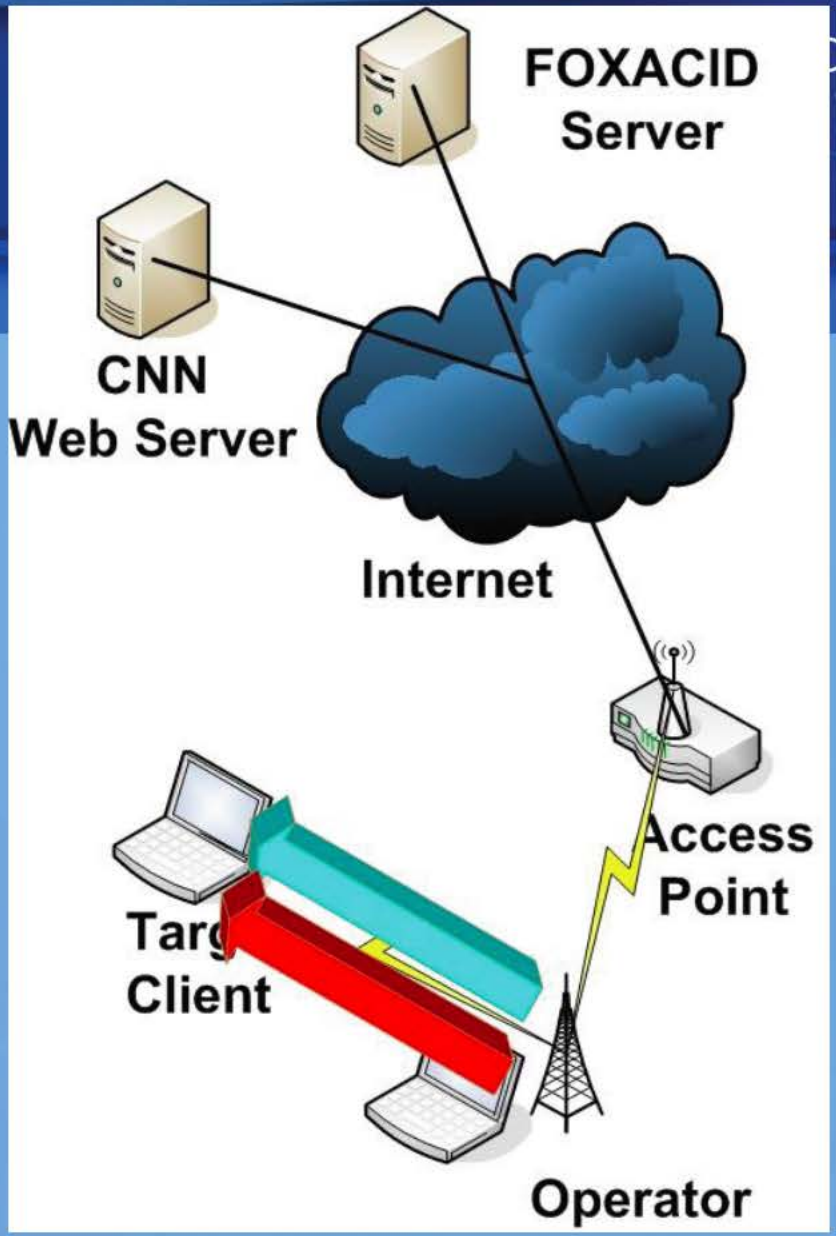
FOXACID
Browser Survey

- FOXACID Server instantiates browser survey on Target Client to detect vulnerabilities.



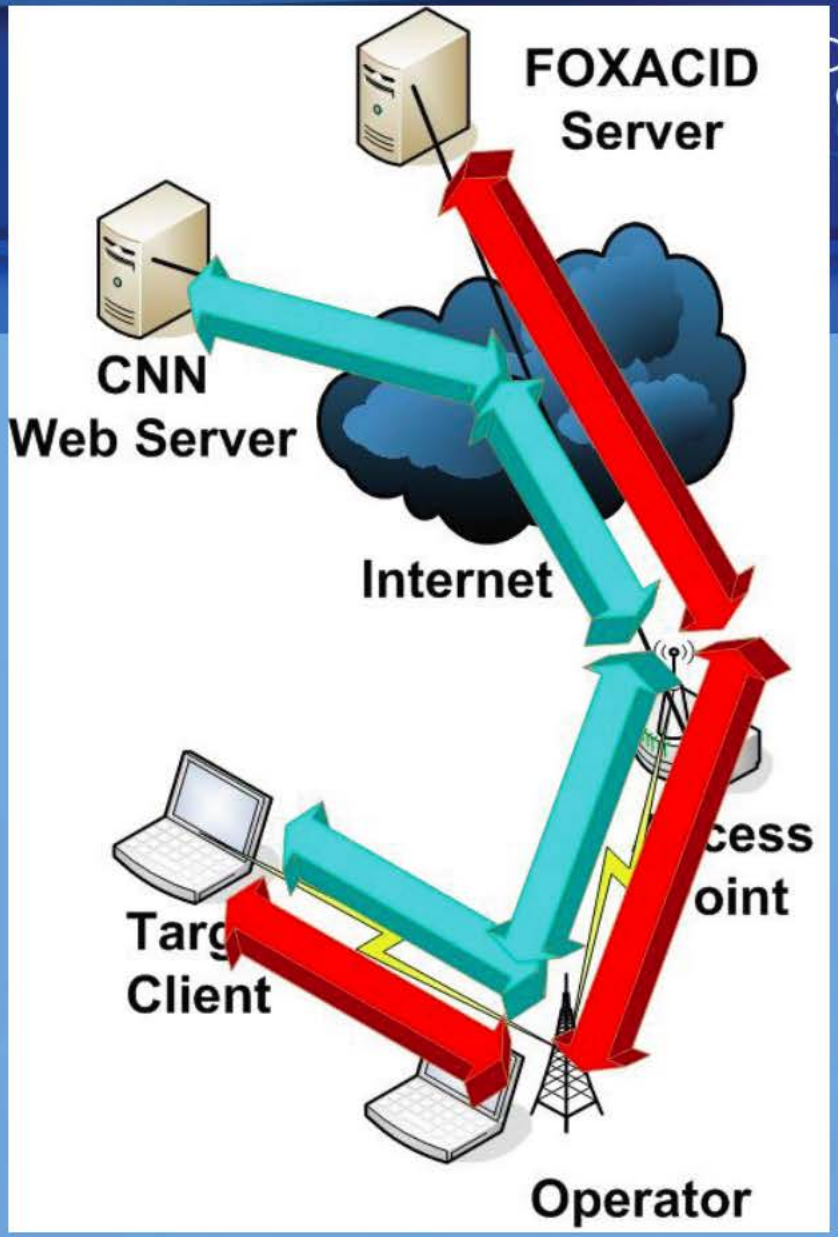
FOXACID
Browser Survey

- FOXACID Server instantiates browser survey on Target Client to detect vulnerabilities.



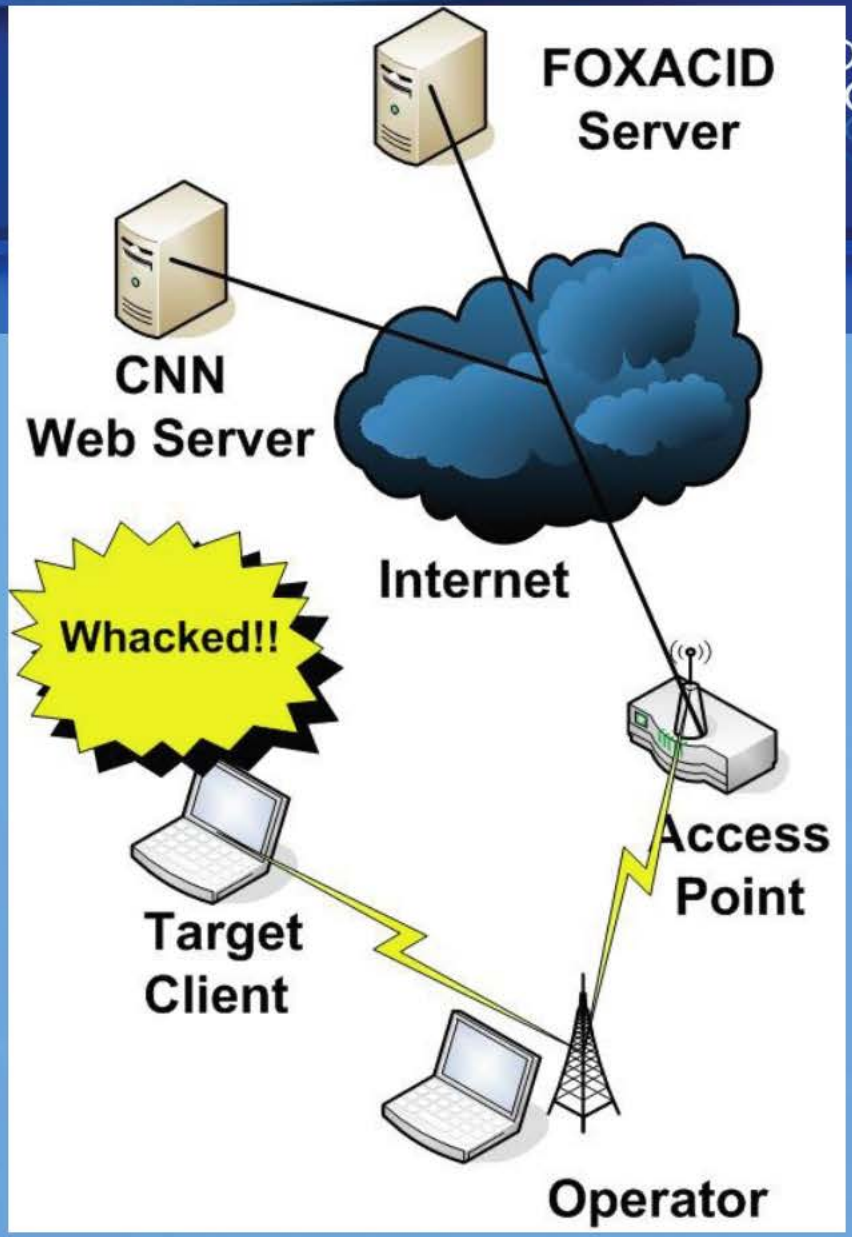
Survey, Payload, Exploitation

- Covert communicates continue between FOXACID and Target until found not vulnerabilities or exploited.
- Target Client continues normal webpage browsing, completely unaware ☺



WHACKED!

- That's the ultimate goal.



BADDECISION Step Through

CLOSE ACCESS

- Let's go through this together…
- … because there are many more pieces!

CLOSE ACCESS

BADDECISION Demos and Labs

- Grab a partner!
- One Target Client, one Operator.
- Have fun getting whacked!

BADDECISION Pros / Cons

CLOSE ACCESS

- Pros
  - Works for WPA / WPA2 networks.
  - Can reliability see all communications between target and FOXACID.
- Cons
  - Larger signature than NIGHTSTAND.
  - Requires higher SNR to maintain reliable communications between target and FOXACID.

CLOSE ACCESS

The End.

Questions?