CLOSE ACCESS

Introduction to BADDECISION

December 15-16, 2010

[redacted]

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)

Section Overview

CLOSE ACCESS

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

At The End…

You should be able to….

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

CLOSE ACCESS

BADDECISION Overview

- ➢ 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!

CLOSE ACCESS

BADDECISION Prerequisites

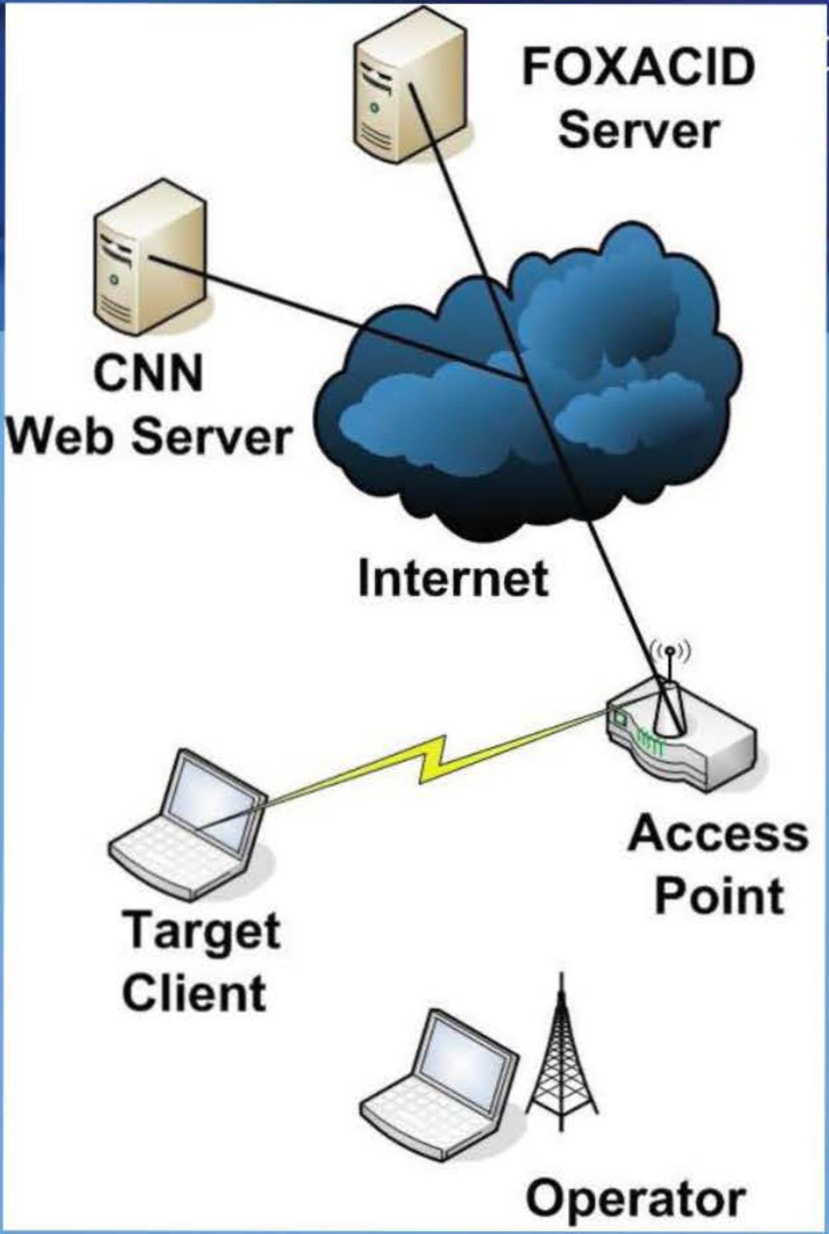
- **Working BLINDDATE Survey!**
- **Client on the Target network**
- **Security Level: WPA / WPA2**
- **Ability to maintain a reliable connection to a target network.**
- **Don't forget FOXACID Tag!**

BADDECISION Components

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

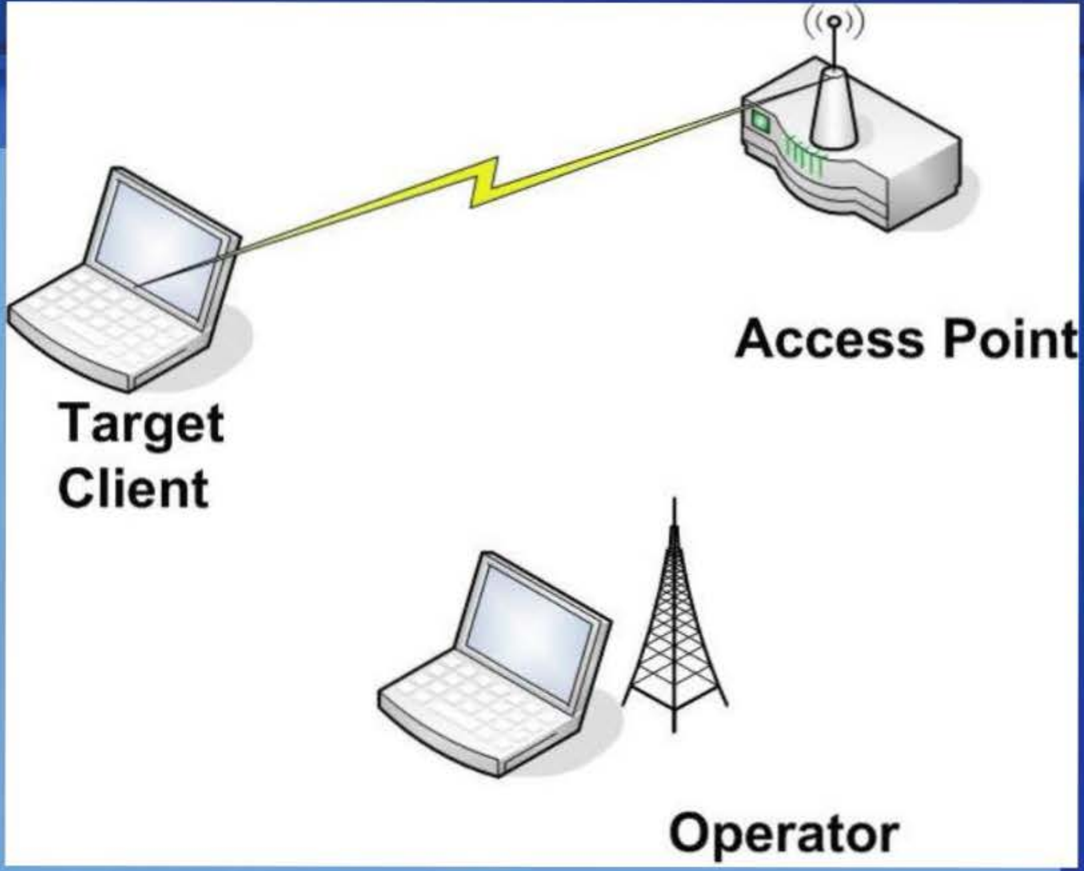
BADDECISION
Preparation

[redacted]



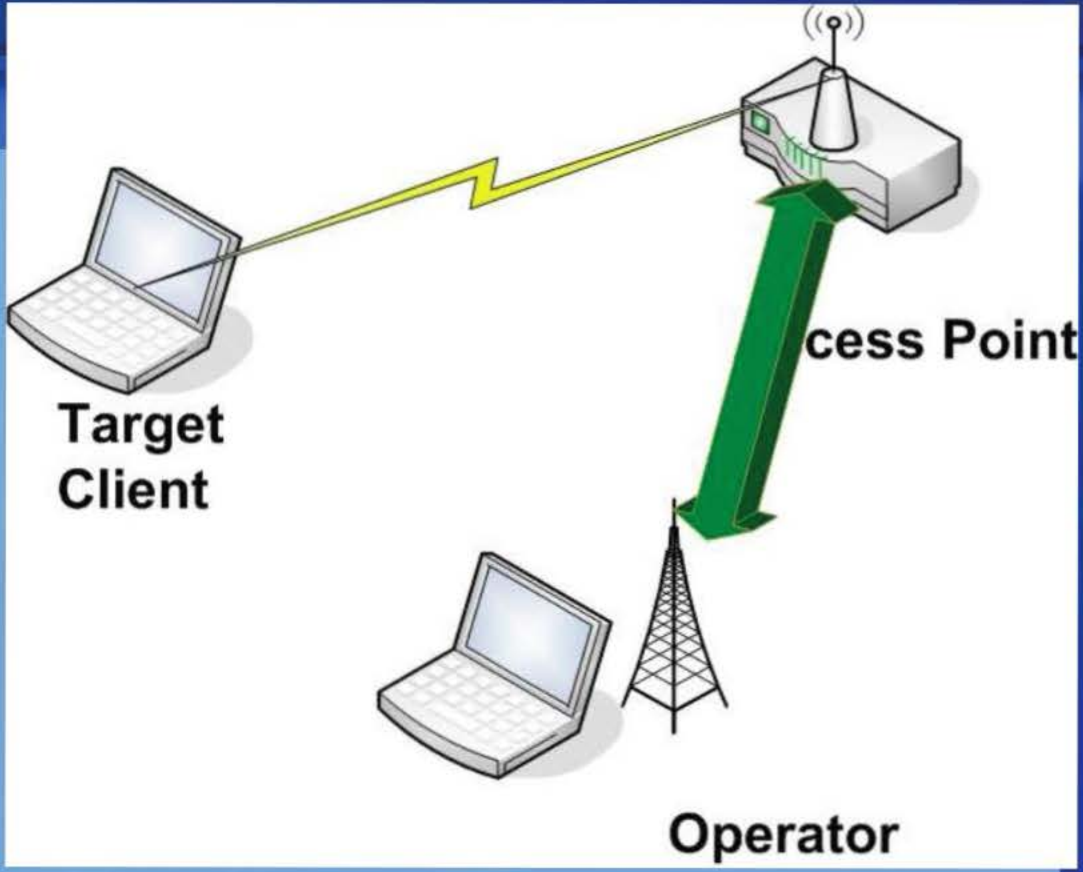
BADDECISION
Preparation

[redacted]



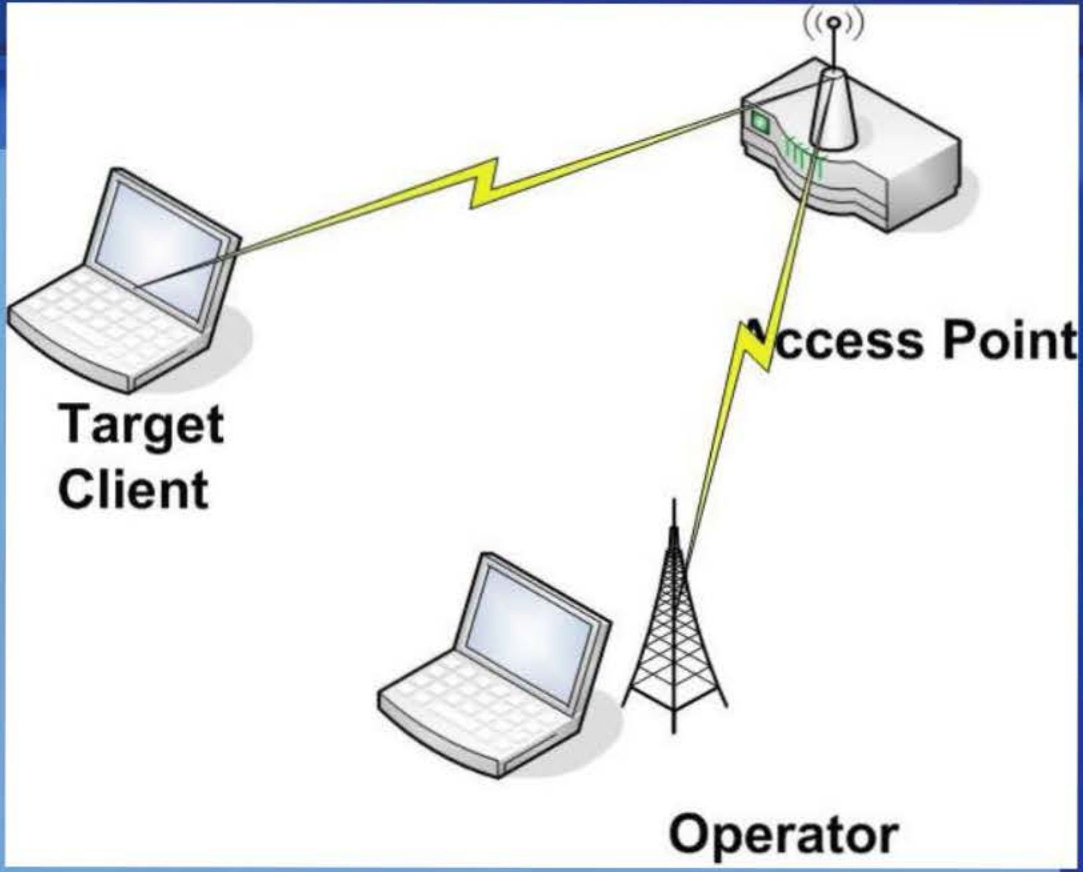
BADDECISION
Preparation

[redacted]



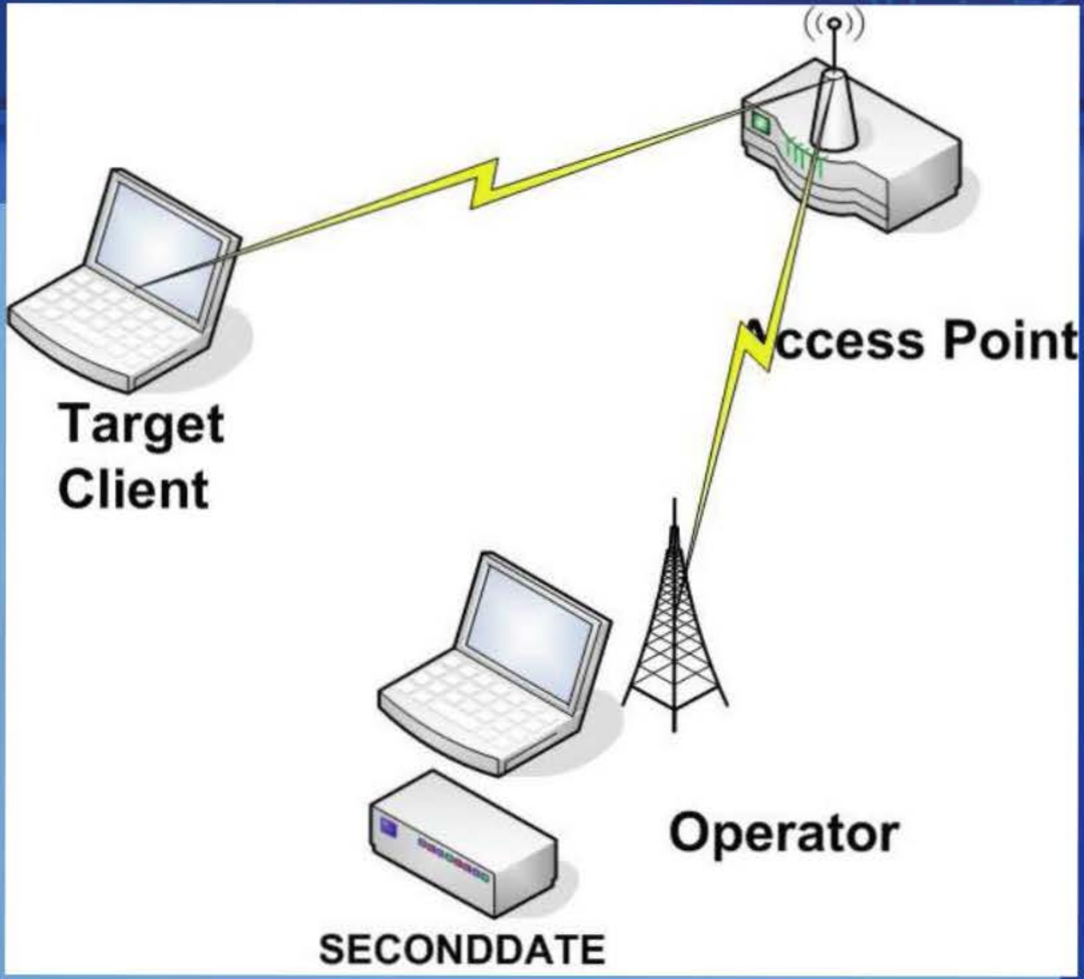
BADDECISION
Preparation

[redacted]



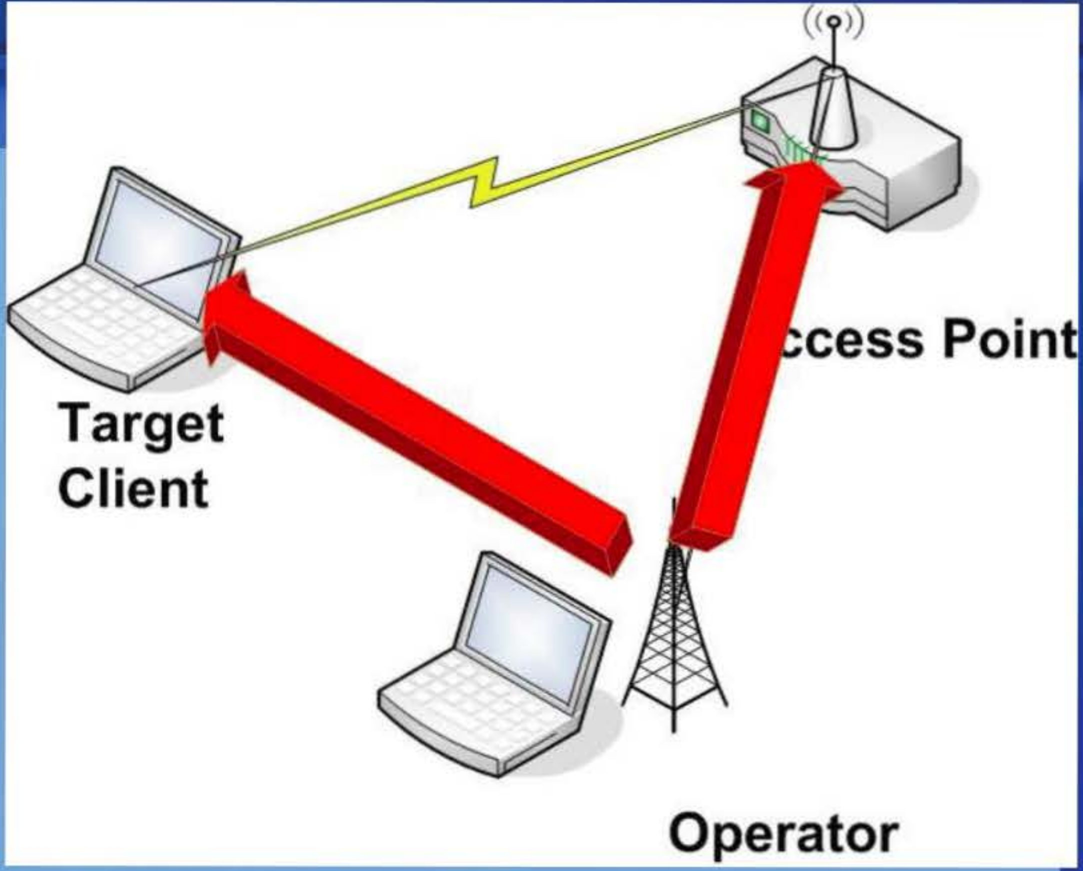
BADDECISION
Preparation

[redacted]



BADDECISION
Preparation

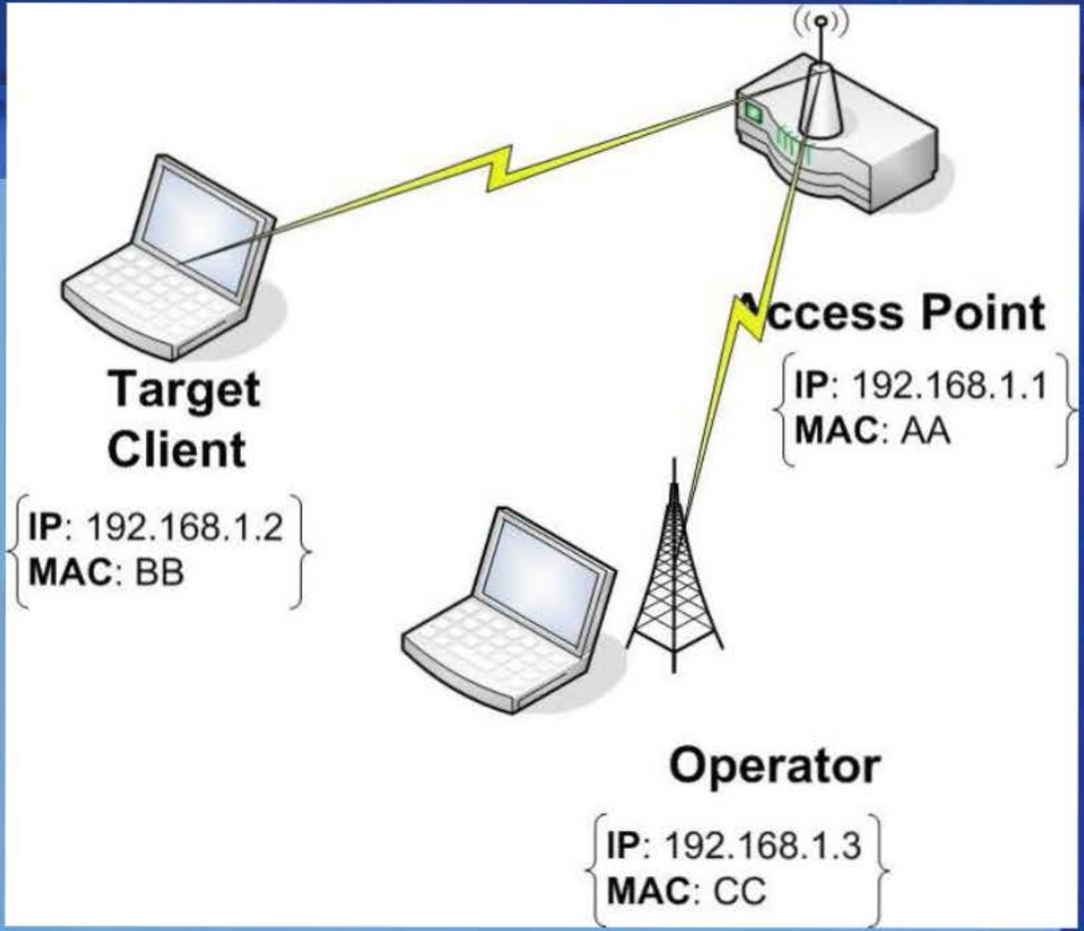
[redacted]



CLOSE ACCESS

BADDECISION
Preparation

[redacted]



Access Point

IP: 192.168.1.1
MAC: AA

Target Client

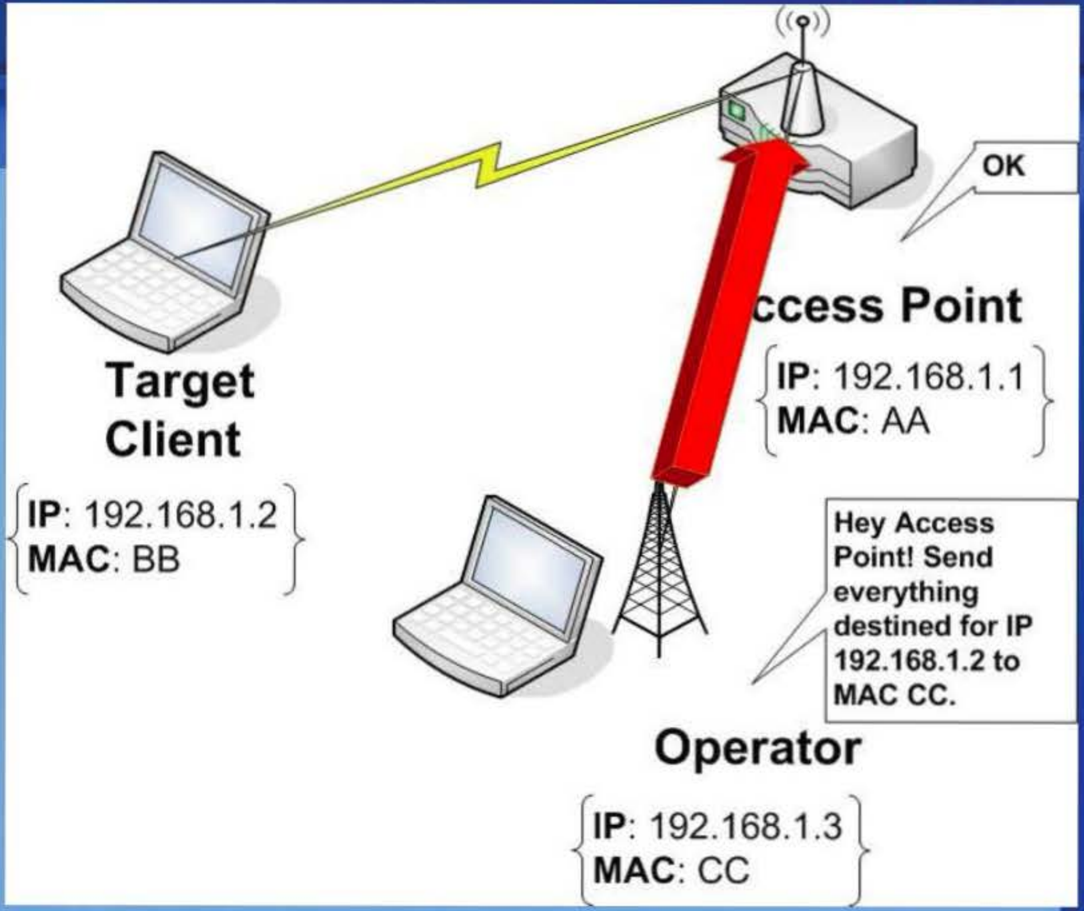
IP: 192.168.1.2
MAC: BB

Operator

IP: 192.168.1.3
MAC: CC

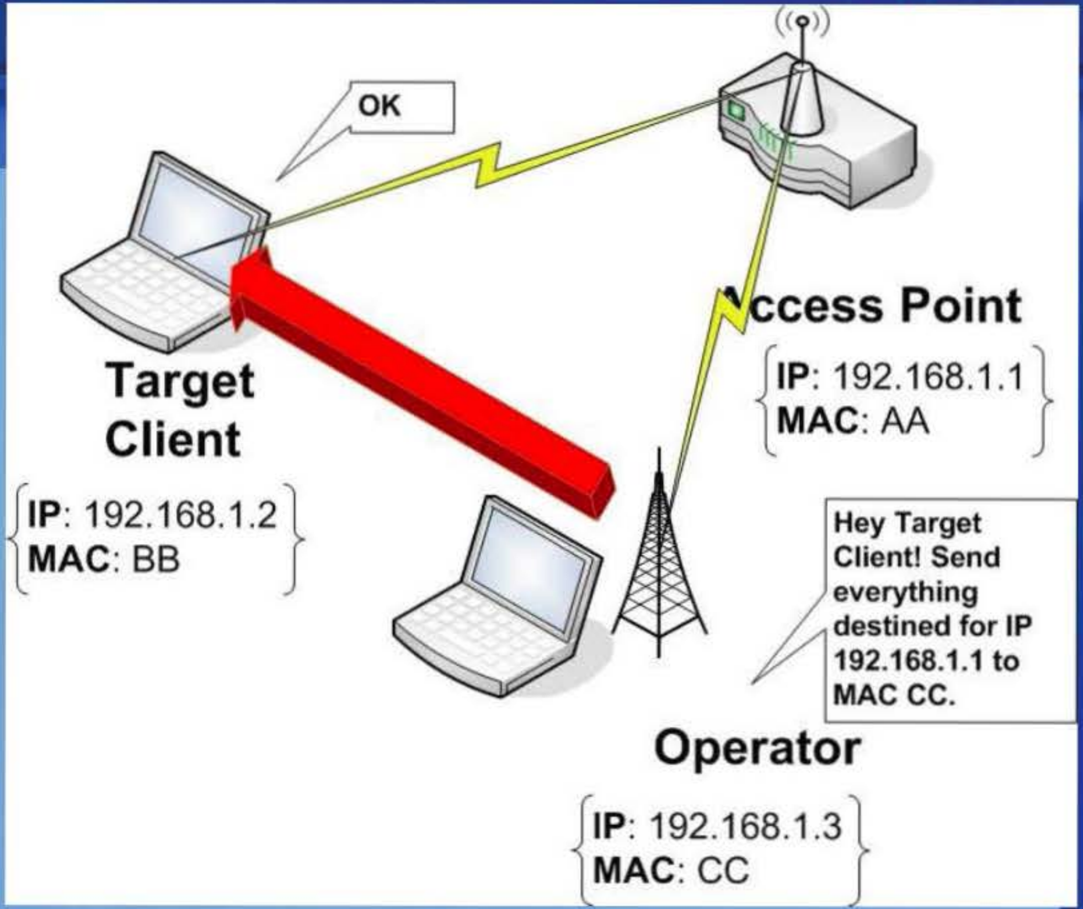
BADDECISION
Preparation

[redacted]



BADDECISION
Preparation

[redacted]



OK

Target Client

IP: 192.168.1.2
MAC: BB

Access Point

IP: 192.168.1.1
MAC: AA

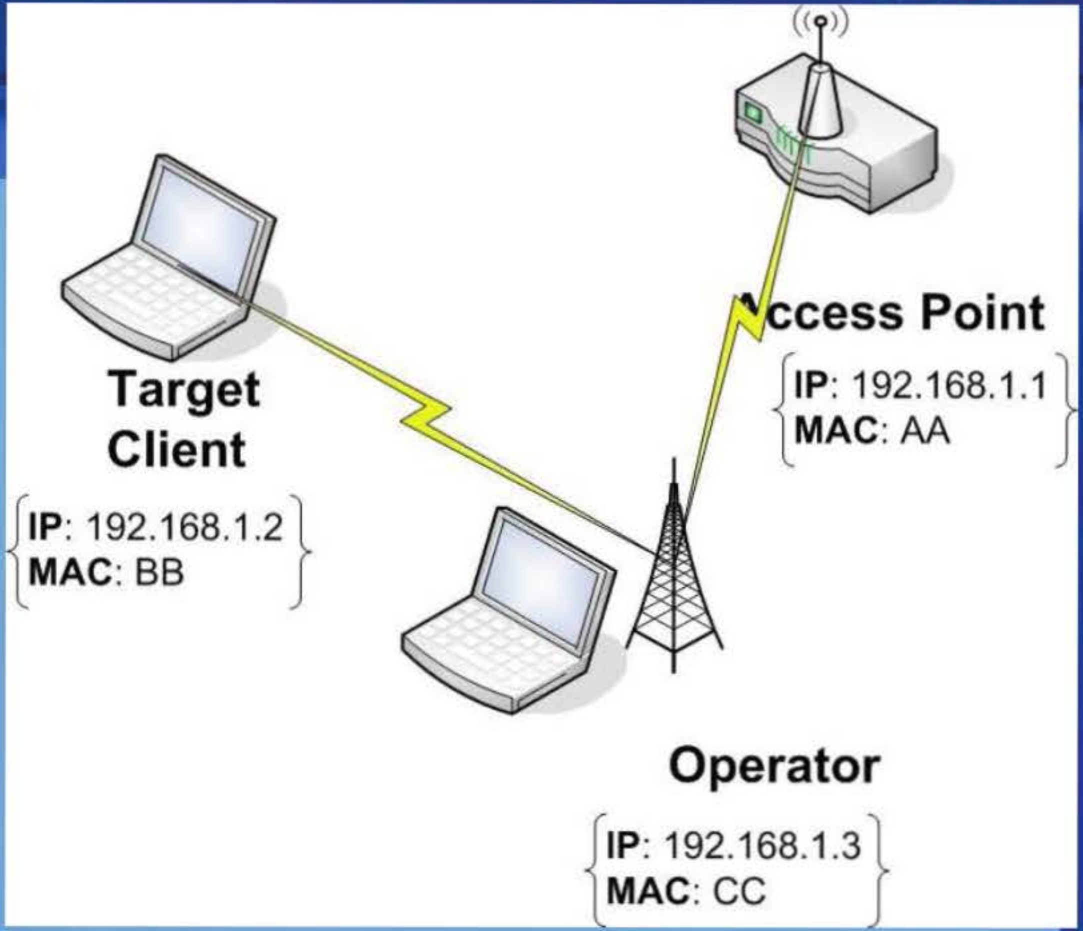
Hey Target Client! Send everything destined for IP 192.168.1.1 to MAC CC.

Operator

IP: 192.168.1.3
MAC: CC

BADDECISION
Preparation

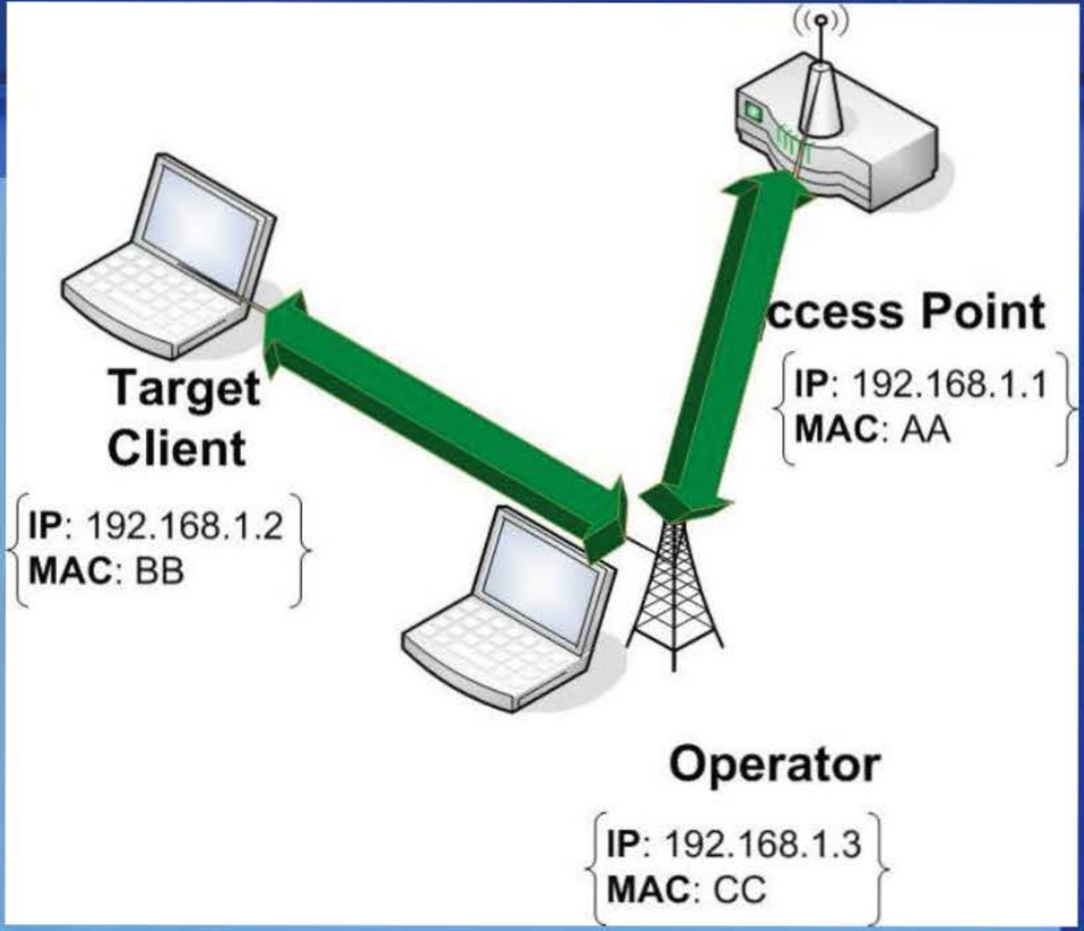
[redacted]



CLOSE ACCESS

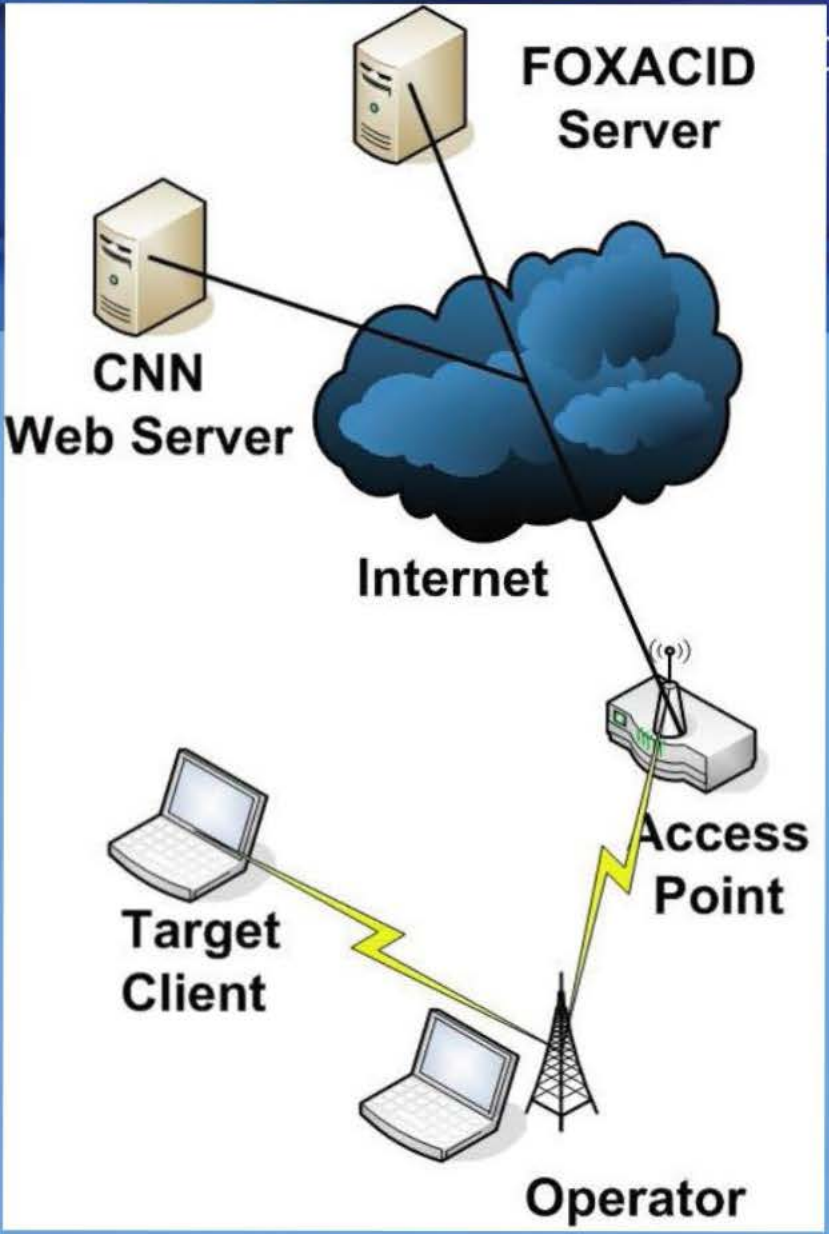
BADDECISION
Preparation

[redacted]



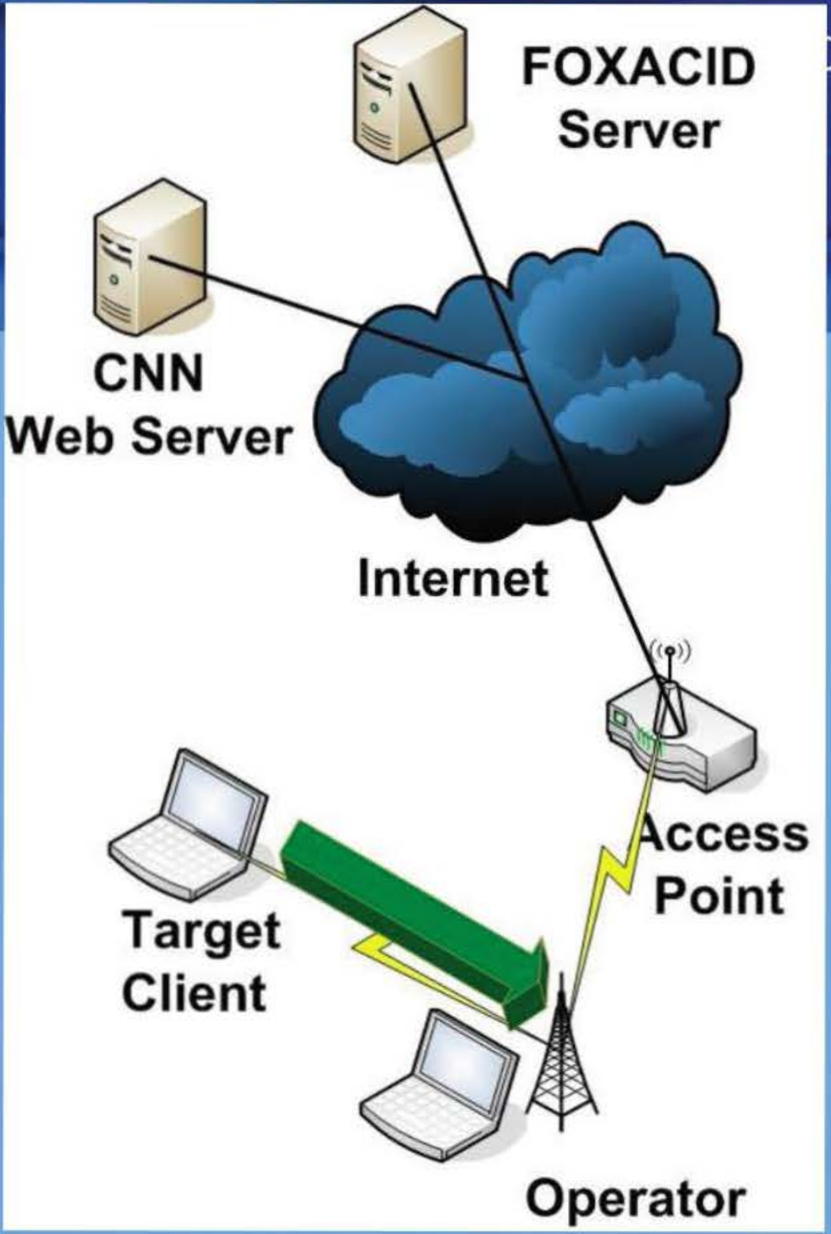
Overview of Operational Scenario

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



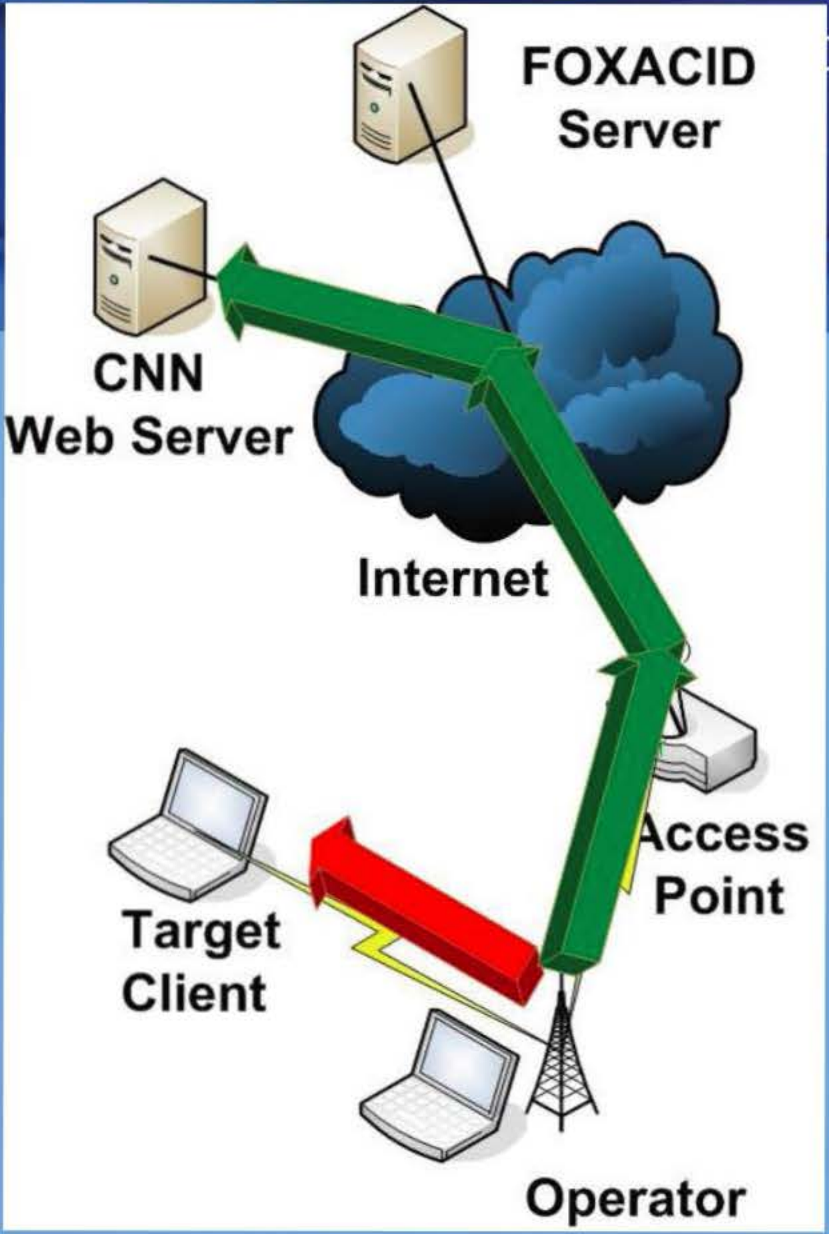
Webpage Request

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



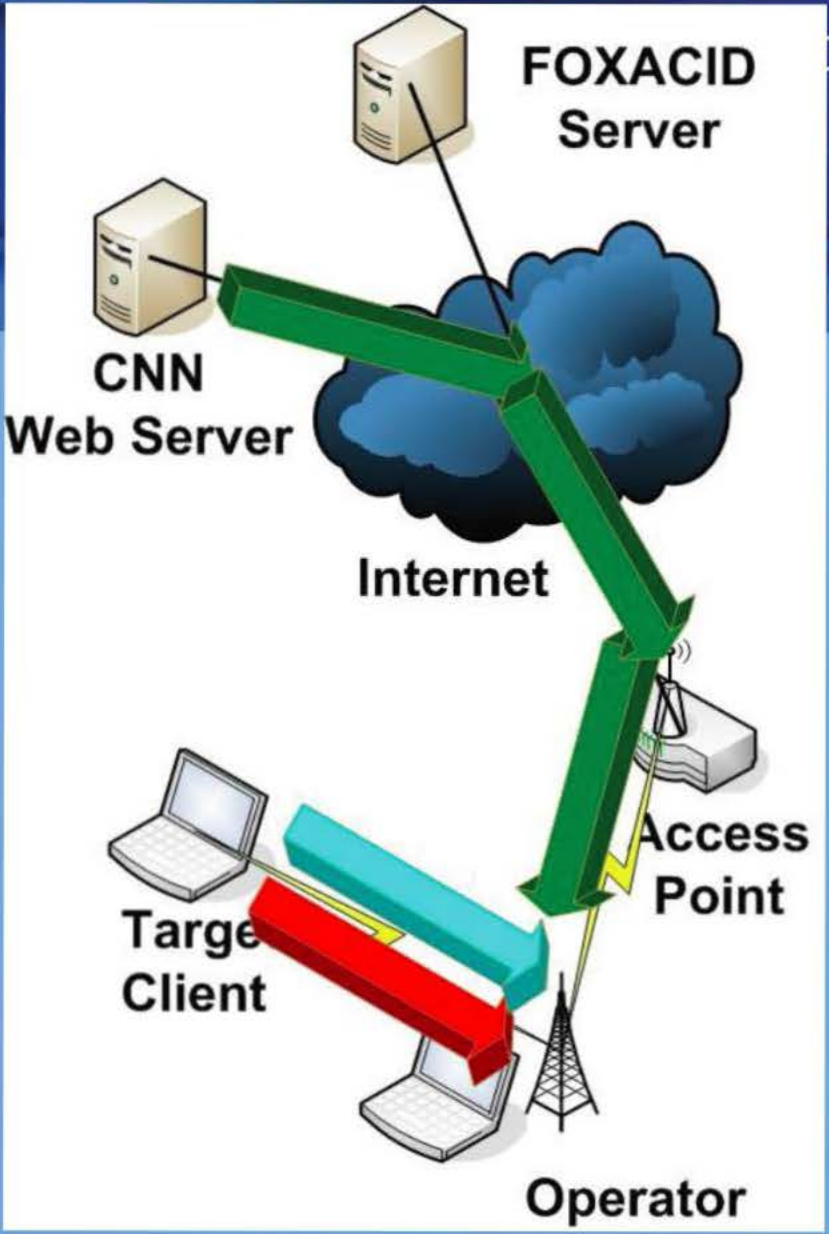
Injection

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



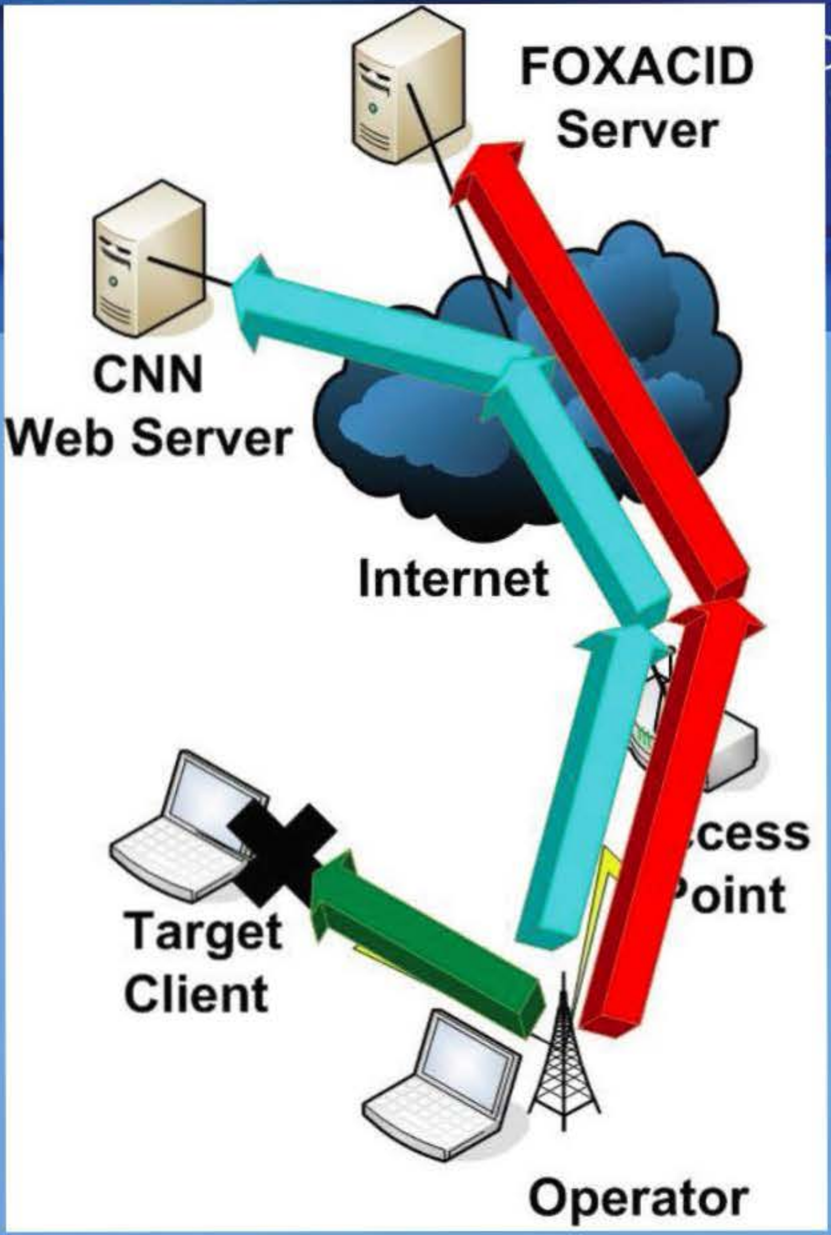
Refresh and Covert Request

- ➢ 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.



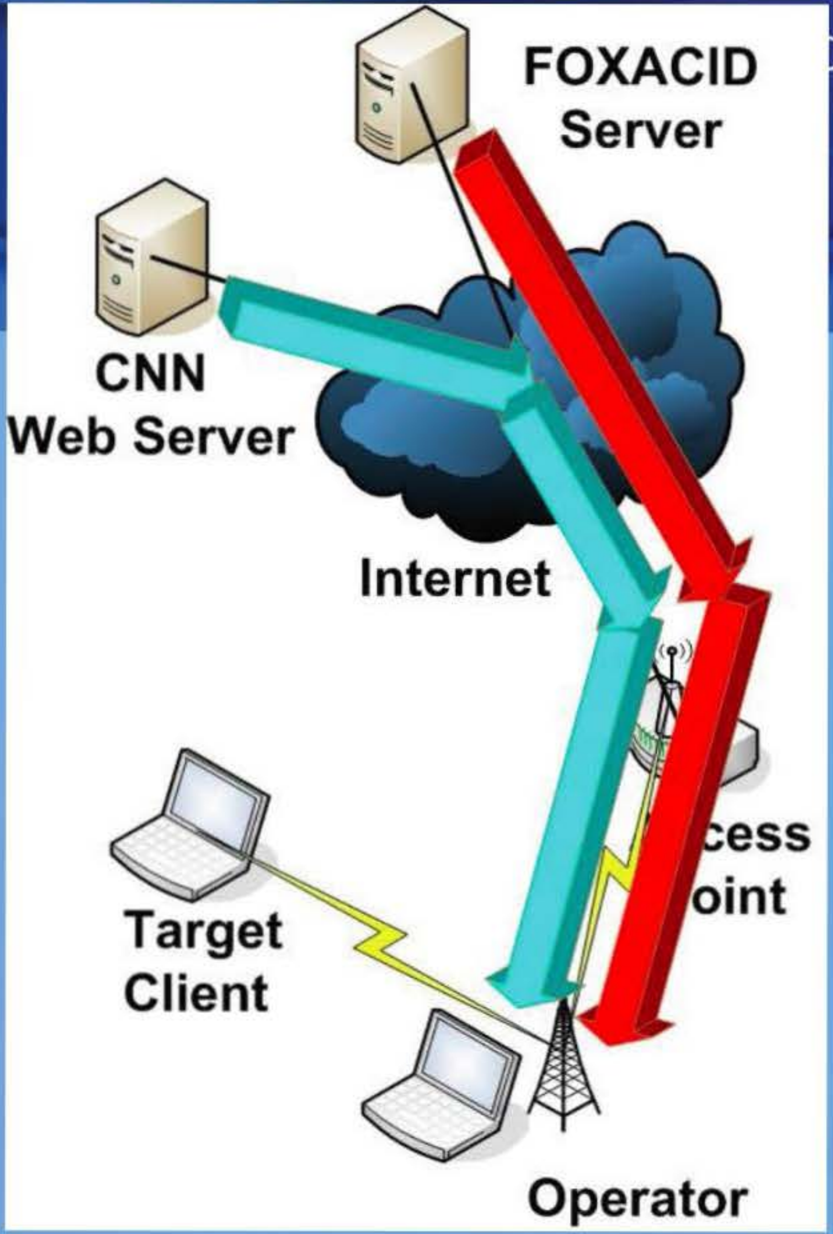
FOXACID Request Received

- ➢ 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)



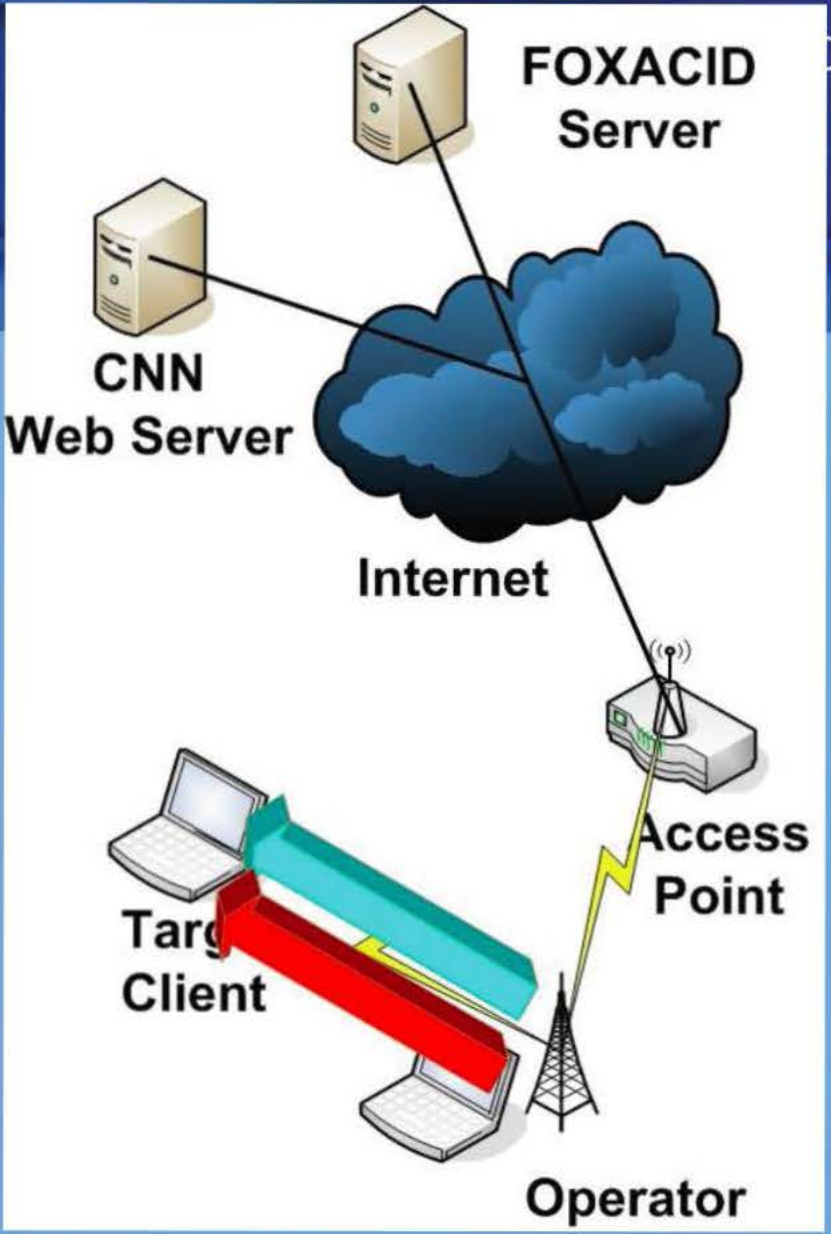
FOXACID Browser Survey

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



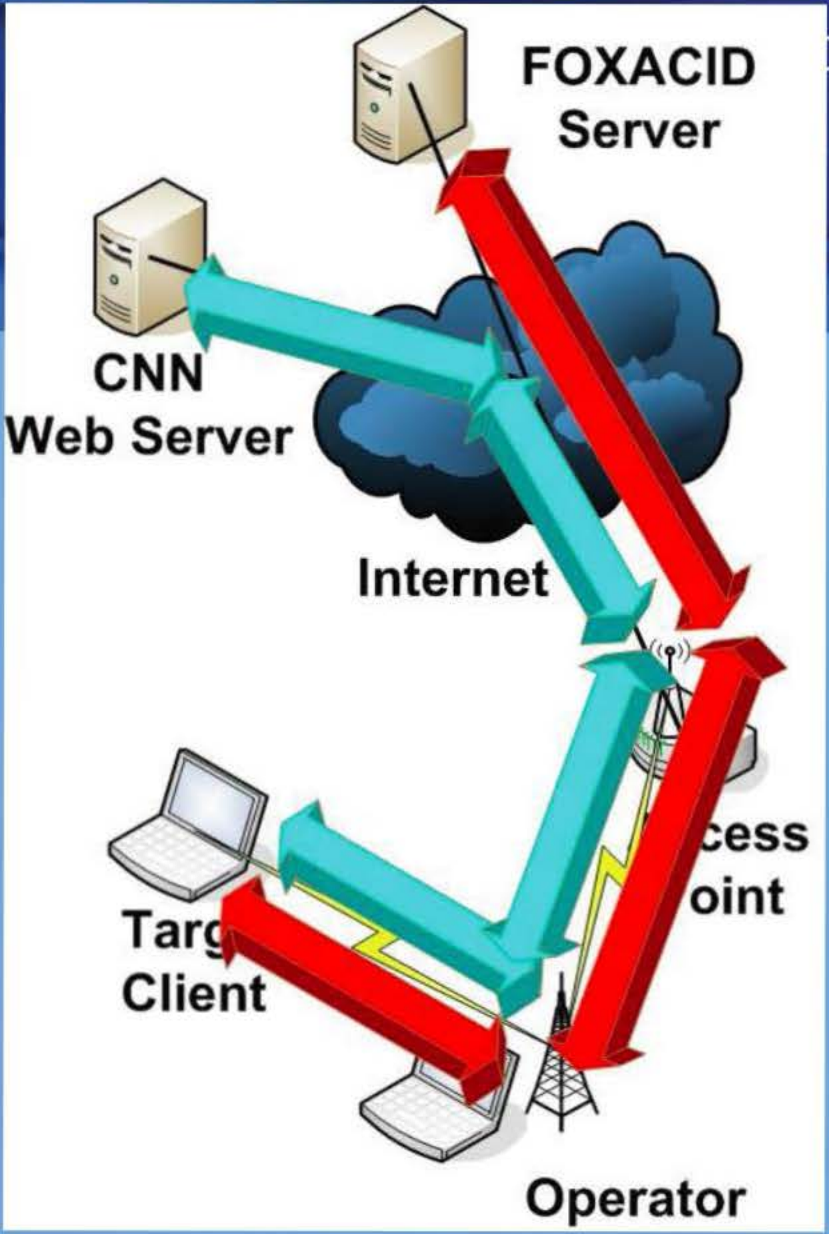
FOXACID Browser Survey

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



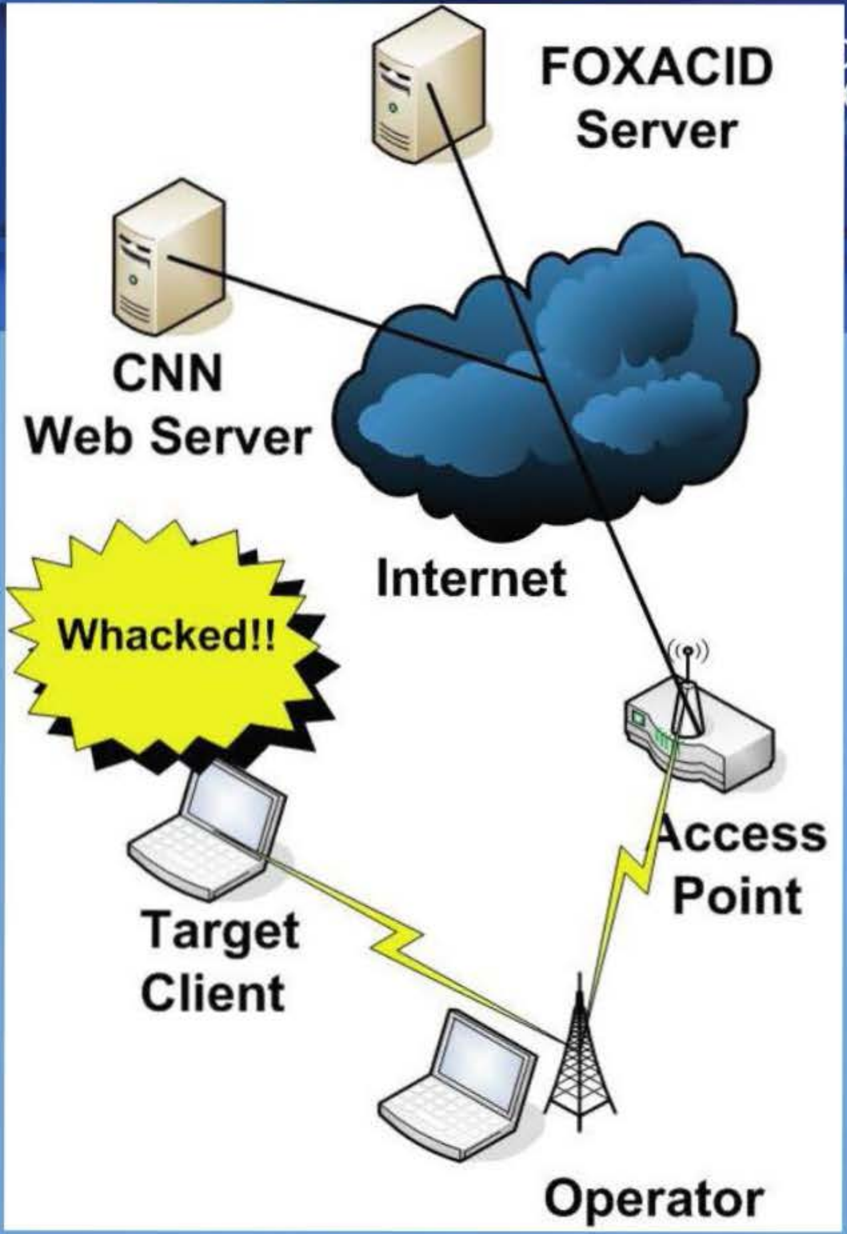
Survey, Payload, Exploitation

- ➢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!

BADDECISION Demos and Labs

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

BADDECISION Pros / Cons

- 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.

The End.

Questions?

[redacted]