CLOSE ACCESS

Introduction to WLAN / 802.11 Active CNE Operations

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)

Section Overview

- Passive to Active Operations
- WLAN CNE Criteria / Assessment
- Active CNE Operations
- Introduction to FOXACID

At The End…

CLOSE ACCESS

You should be able to….

- Identify Criteria for CNE Assessment.
- List the Active CNE Operational Process
- Describe the purpose of FOXACID.

Passive to Active Operations

CLOSE ACCESS

- **Primary Goal:** To enable on-net access to target networks via off-net capabilities.
- **Prerequisite:** We need to find the network of interest in order to target it.
- **Procedure:** Conduct passive survey to locate network, then perform active op.
- **Solution:** Utilize BLINDDATE and the appropriate plug-in solution(s).

Passive to Active Operations

CLOSE ACCESS

- Successful operation of BLINDDATE is essential to correct usage of plug-ins.
- Two types of plug-ins exist:
  - Analysis Tool Aids
  - Active CNE Tools
- We will focus on Active CNE Tools:
  - NIGHTSTAND
  - HAPPYHOUR

Active CNE Assessment

CLOSE ACCESS

- BLINDDATE used as both a survey and vulnerability analysis tool for 802.11 networks.
- Operator needs to know what vulnerabilities, or criteria, to look for in order to utilize the correct Active CNE Tool (if any)
- We will focus primarily on criteria necessary to carry out NIGHTSTAND (NS) and BADDECISION (BDN) operations.

CLOSE ACCESS

Major Assessment Criteria

- **Clients**
  - A client is a prerequisite: If no clients are on the target network, there's nothing to do yet.
- **Security**
  - Encryption setting (Open, WEP, WPA, WPA2) dictates which capability can be used (if any).
- **Signal Strength**
  - SNR dictates whether we can perform a successful active CNE operation.

Active CNE Operations

CLOSE ACCESS

- What is our end goal?
  - Provide on-net access via off-net means.
- How do we do that?
  - **Redirect the target** to the TAO infrastructure.
- How do we do that?
  - **Inject payload** destined for the target client.

Active CNE Operations

CLOSE ACCESS

- What does that do exactly?
  - Forces the target to **covertly contact** a FOXACID server.
- What is FOXACID suppose to do?
  - Perform **vulnerability analysis and exploitation** of the target (if possible).

Introduction to FOXACID

CLOSE ACCESS

- FOXACID is the cover term for a DNT/ROC project to deliver content based exploits (CBE) to web browsers.
- The greatest vulnerability to your computer: your web browser.

Introduction to FOXACID

CLOSE ACCESS

- FOXACID Servers sit on Internet.
  - Publicly addressable, DNS resolved.
  - Utilizes whitelist for security, filtering.
- Requires specially crafted URL tag to contact FA Servers (FOXACID Tag).

Example Tag

http://Domain/PluginName/PluginName2/ListBegin/Group/ListEnd/DeploymentIDTLN_MSGID.html

http://baseball2.2ndhalfplays.com/nested/attribs/bins/1/define/forms9952_z1zzz.html

FOXACID Tags

CLOSE ACCESS

- Designed to look ambiguous.
- Unique for a particular target / operation.
- All fields in the tag denote something special…

Redirection to FOXACID

CLOSE ACCESS

- A FOXACID Tag is a special URL pointing to a particular FOXACID Server.
- Contacting the FA Server will (hopefully) result in the contactor being exploited.
- We want the target to be exploited.
- How do we redirect the target to the FOXACID Server without being noticed.
  - Use NIGHTSTAND or BADDECISION

CLOSE ACCESS

The End.

Questions?