DGTIC UNAM CERT

2do Coloquio de Proyectos de Becarios en Seguridad Informática

Detector de URLs y Honeypots HTTP, SMTP, IRC

Martínez Olivares Omar Daniel
omartinez@ciencias.unam.mx

Agenda

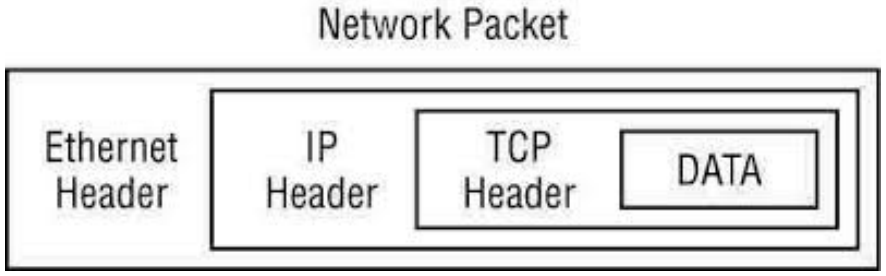
1. **Objetivo**
2. **Descripción**
3. **Componentes**
4. **Honeypots**
   - Alta Interacción
   - Baja Interacción
5. **Desarrollo**
   - Detector de URLs
   - Honeypot SMTP,HTTP,IRC
   - Parser
   - Incidentes SMTP,HTTP,IRC
6. **Reportes**

Objetivo

- Desarrollar un módulo de detección y procesamiento de tráfico malicioso para la UNAM-Darknet utilizando tecnologías honeypot para servicios de IRC,HTTP y SMTP.

Descripción

Para el desarrollo de esta herramienta se utiliza el lenguaje de programación PERL así como las librerías PCAP para la captura y análisis de tráfico.



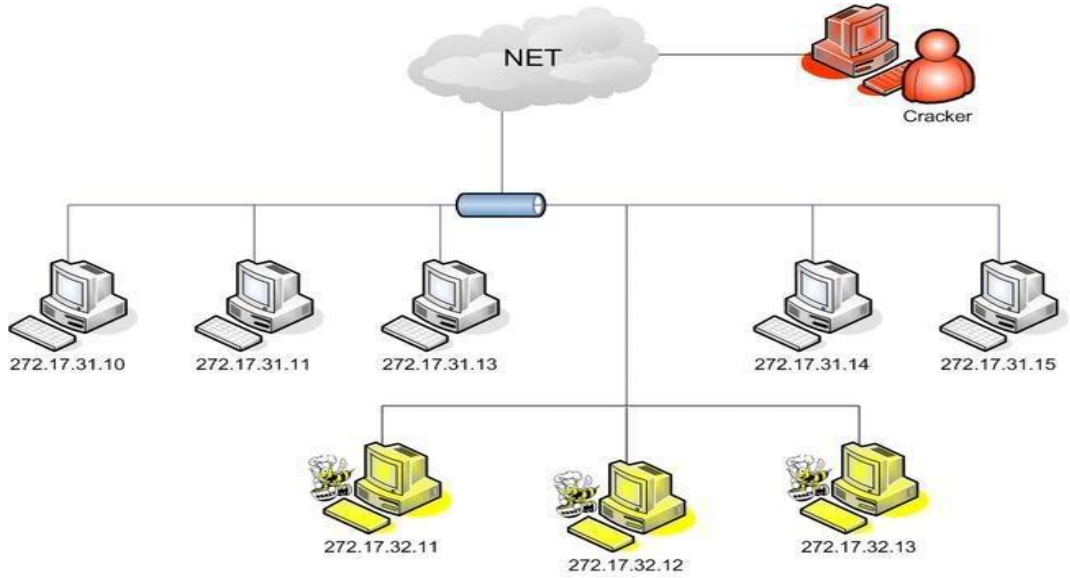
El sistema se compone de tres partes las cuales se complementan para poder lograr una correcta detección de amenazas en la red.

Componentes

- Analizador y detector de URLs
- Honeypots de baja interacción
- Analizador(parser)
- Interfaz Web para Reportes

Honeypot

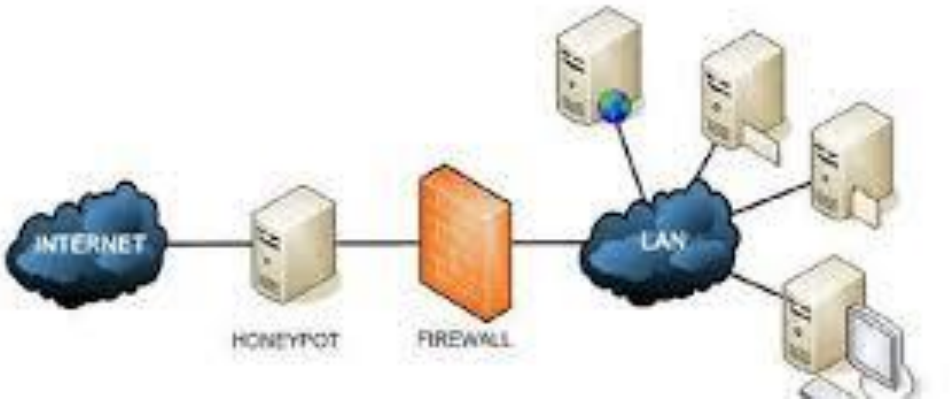
Es un software o sistema diseñado para atraer a los atacantes, simulando ser sistemas vulnerables o débiles a los ataques, para analizar como los intrusos emplean sus herramientas para intentar ganar acceso a un sistema.



- Por medio del aprendizaje de sus herramientas y métodos de intrusión se puede proteger mejor los sistemas.

Honeypot de Alta Interacción

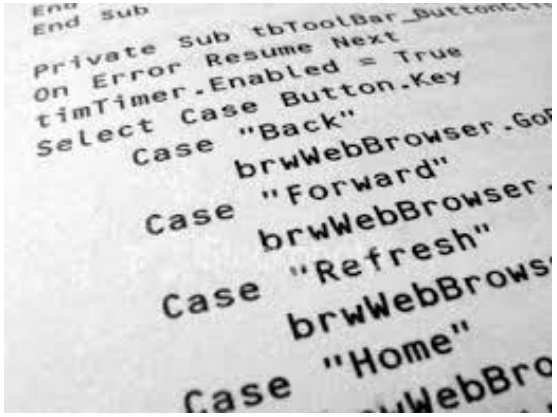
Honeypots que trabajan sobre sistemas reales y son capaces de reunir más información que los de baja interacción.



Sin embargo representan un mayor riesgo de seguridad debido a que se deja el sistema al alcance de la red pública para exponerlo a atacantes informáticos.

Honeypot de Baja Interacción

Son programas que se limitan a simular sistemas operativos o servicios no existentes en realidad en el equipo.

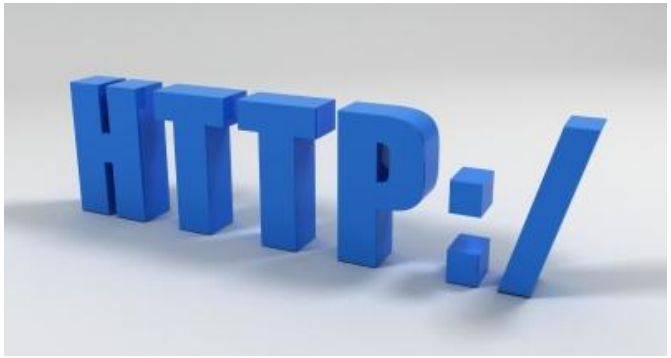


Su objetivo es brindar la sensación de estar interactuando como un servicio real y vulnerable, mientras se recaba información de métodos de ataques e intrusión.

Desarrollo

Analizador y detector de URLs

Módulo que realiza un análisis del tráfico de la red mediante el uso de un **archivo de captura PCAP** o la utilización de un **portmirror** realizando un tracking del payload de las sesiones.



Se recaba información con la finalidad de detectar patrones maliciosos relacionados con peticiones de posible malware en la red, con base en un **diccionario**.

El resultado de este proceso es la obtención de un **archivo de listas negras** que nos definen posibles direcciones IP con actividades maliciosas.

Honeypot del Servicio SMTP

Honeypot de baja interacción del servicio SMTP, cuyo objetivo es la identificación de

- **URLs maliciosas**
- **Spammers**
- **Malware**

Funciones Simuladas SMTP

- **EHLO/HELO**
- **MAIL FROM**
- **RCPT TO**
- **RESET**
- **DATA**
- **QUIT**

Honeypot Servicio IRC

- Este módulo se encarga de simular un servidor de Internet Relay Chat (IRC) para poder recabar información acerca de:

- Actividades sospechosas hechas en la red del blackhole.
- Equipos con comportamiento de bot.
- Servidores C&C
- Herramientas utilizadas en botnets

Funciones Simuladas IRC

- **/privmsg**
- **/msg**
- **/part**
- **/whois**
- **/list**
- **/join**
- **/ping**
- **/help**
- **/names**

Honeypot Servicio HTTP

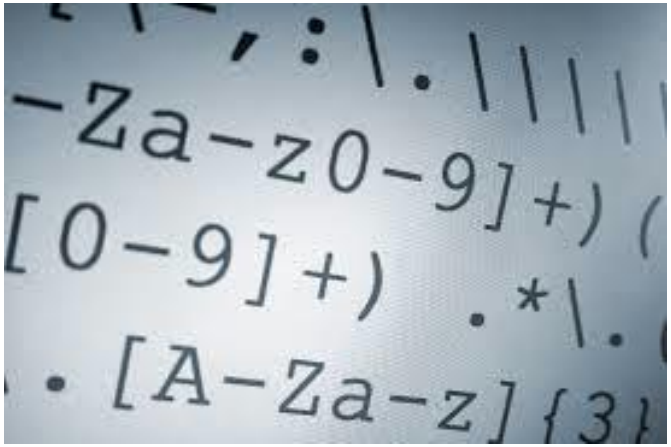
Este módulo se encarga de detectar posibles peticiones hechas por malware, así mismo identificar posibles URLs maliciosas que intenten vulnerar algún tipo de servicio WEB.

Funciones Simuladas HTTP

- GET
- POST
- HEAD

Módulo de Detección (Parser)

Es el encargado de procesar toda la información adquirida por los diferentes servicios honeypots y almacenarla en la base de datos del TSU.



Parser

- IRC
  - Direcciones IP con C&C
  - Dominios de C&C
  - Canales maliciosos
  - Url de Herramientas
  - Comandos IRC utilizados
- HTTP
  - Urls maliciosas
  - Direcciones IP en listas negras
- SMTP
  - Urls maliciosas
  - Direcciones IP fuente de SPAM
  - Malware

Incidentes Honeypot SMTP

- Dirección IP fuente de SPAM
- Incidentes por URL en SPAM
- Incidentes por Malware adjunto al correo (base64).

Incidentes Honeypot IRC

- **Botnets:** Equipos comprometidos con comportamiento de bot
- **C&Cs:** Servidores que envían ordenes a equipos comprometidos.
- **Ordenes C&C:** Comandos que permiten controlar a equipos bots.
- **Canales maliciosos:** Conexión de equipos comprometidos a canales sospechosos

Incidentes Honeypot HTTP

- Peticiones URLs hechas por malware
  - Direcciones IP en listas negras
  - Match de patrón malicioso en diccionario

Reportes

- Se cuenta con una interfaz Web que permite visualizar los incidentes generados por los diferentes servicios.
- URL https://[equipo]:[puerto]
- Ejemplo:
  - https://localhost:8080

Esquema del Proyecto

- Blackhole.conf: Definición de configuraciones y variables
- Blackhole.pl
  - ❖ Obtención de direcciones IP en Blacklist(SPAMHAUS)
  - ❖ Lectura de Patrones Maliciosos
  - ❖ Captura de Tráfico
  - ❖ Inicialización de Honeypots
- Interfaz Web(CGI perl)

- Captura de Tráfico(PacketCapture.pm):
  - ✓Lectura desde PortMirror
  - ✓Lectura desde Archivo PCAP
- Inicialización de Honeypots
  - Services.pm (Alta y Baja Interacción)
  - ProcessService.pm
  - Honeyparser.pm

HoneyParser.pm

- Parser HTTP
  - Urls Maliciosas(Direcciones IP en Listas Negras ó Patrones Maliciosos)
- Parser SMTP
  - Direcciones IP Fuentes de SPAM
  - Archivos Adjuntos Maliciosos(Reporte de VirusTotal).

- Urls Maliciosas(Direcciones IP en Listas Negras ó Patrones Maliciosos)
- Parser IRC
  - Canales maliciosos, comandos IRC, C&C ..