**Datasets Sprint 6- Hito II**

1. **Objetivo Hito II**

El objetivo de este HITO II es documentar y disponibilizar 9 Datasets correspondientes a los ataques simulados que se efectuaron sobre la infraestructura del proyecto titulado como “**Propuesta de Infraestructura TI de bajo costo para proteger una RED CORPORATIVA de micro y pequeñas empresas**”.

Con esto se pretende tener una visión certera de la estructura de los ataques que se están realizando sobre la red.

1. **Tipos de ataque que se llevaran a cabo:**

A continuación, se presentan los diferentes tipos de ataques que se realizaran sobre la infraestructura planteada.

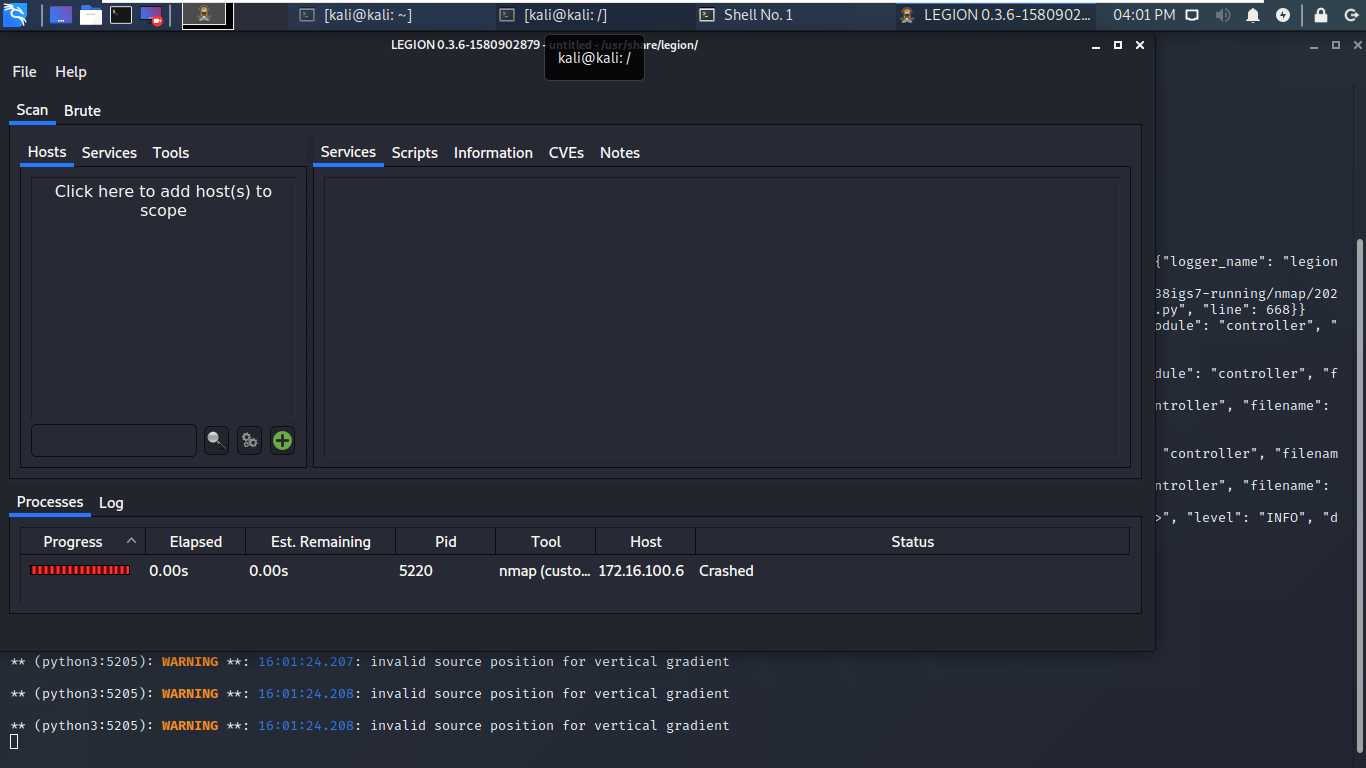
1. Analysis
2. Backdoor
3. Dos
4. Exploit
5. Fuzzer
6. Generic
7. Reconnaissance
8. Shellcode
9. Worm
10. **Dataset – Tipo de ataque:**
11. **Analysis**

En este primer ataque utilizamos la Kali Linux y a través de su herramienta “Legión” generamos un ataque considerado de tipo Analysis, de acuerdo al siguiente detalle:

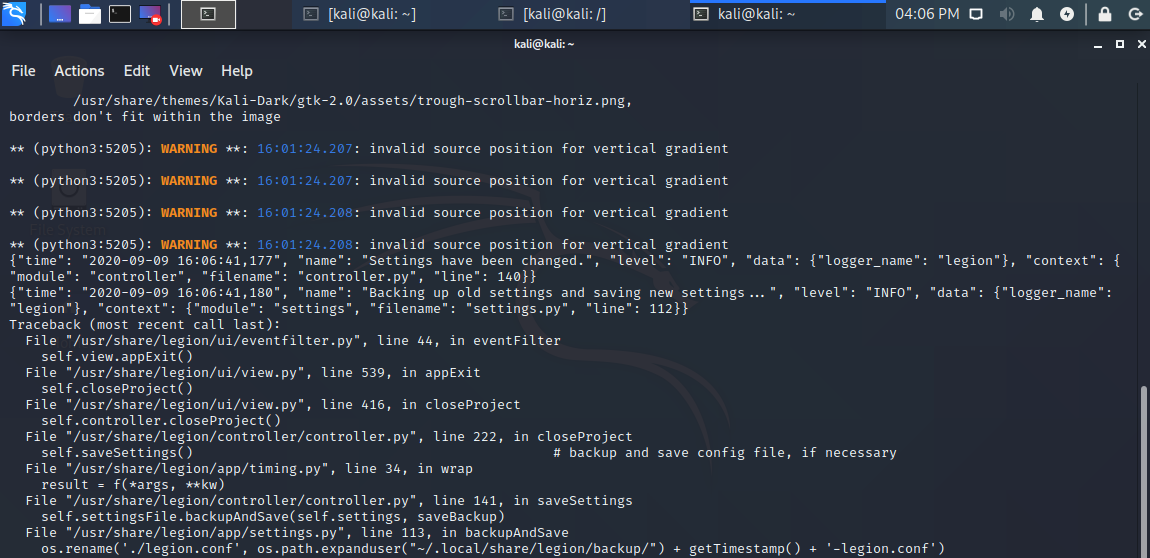
Atacante: Herramienta “Legión”

Victima: 172.16.100.6 (Modulo\_Unab)

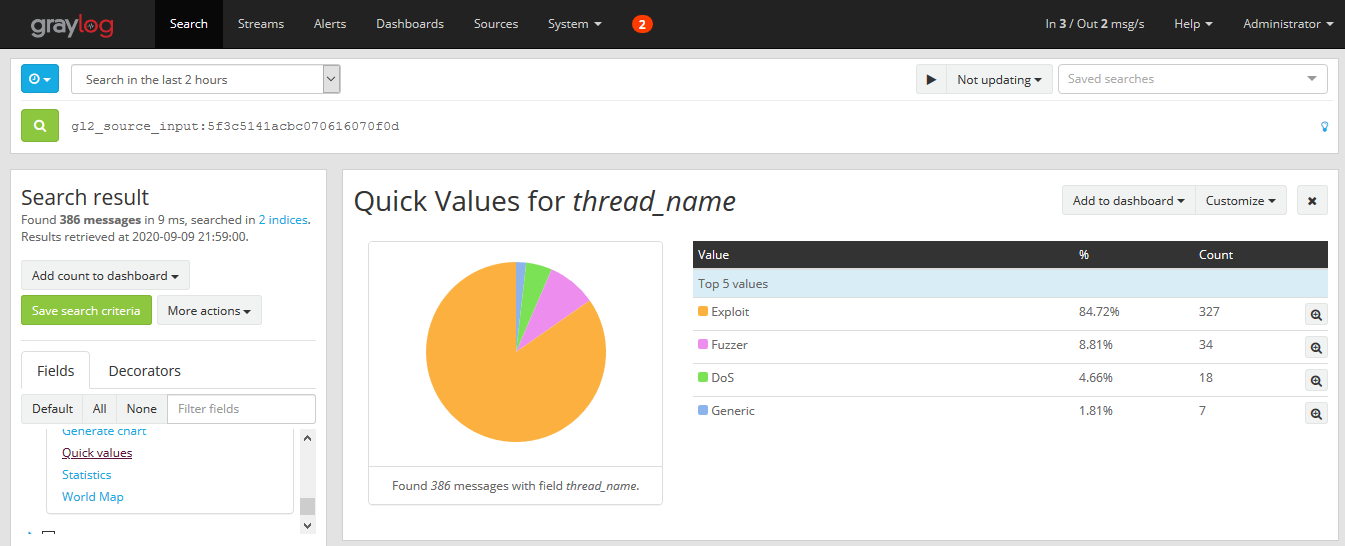
Duración: 5 min.



**Fig. 1 Progreso ataque Legión**



**Fig. 2 Termino del ataque**



**Fig. 3 Categorización de Ataque “Analysis” en Graylog**

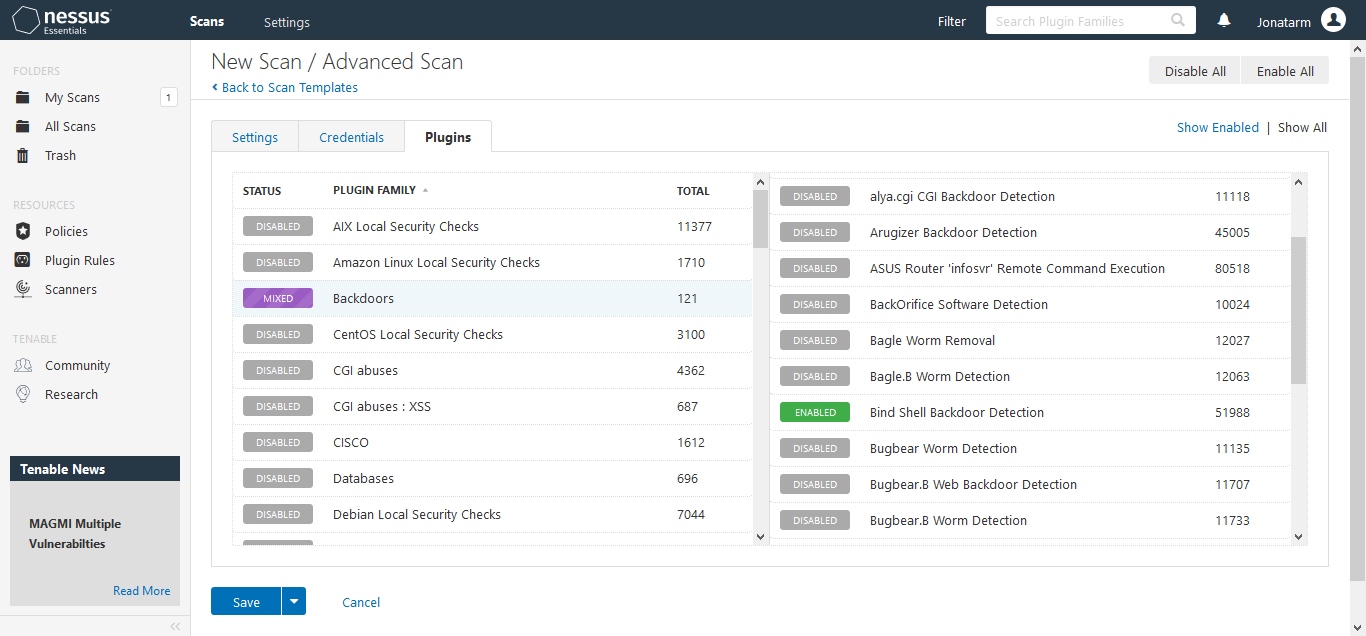
1. **Backdoor**

En este tipo de ataque y tomando en cuenta que el modulo de categorización, realiza una captura de trafico en donde esta conectado el equipo “victima”, se opto por utilizar la Herramienta Nessus con su plugin de Backdoor, se acuerdo a siguiente detalle:

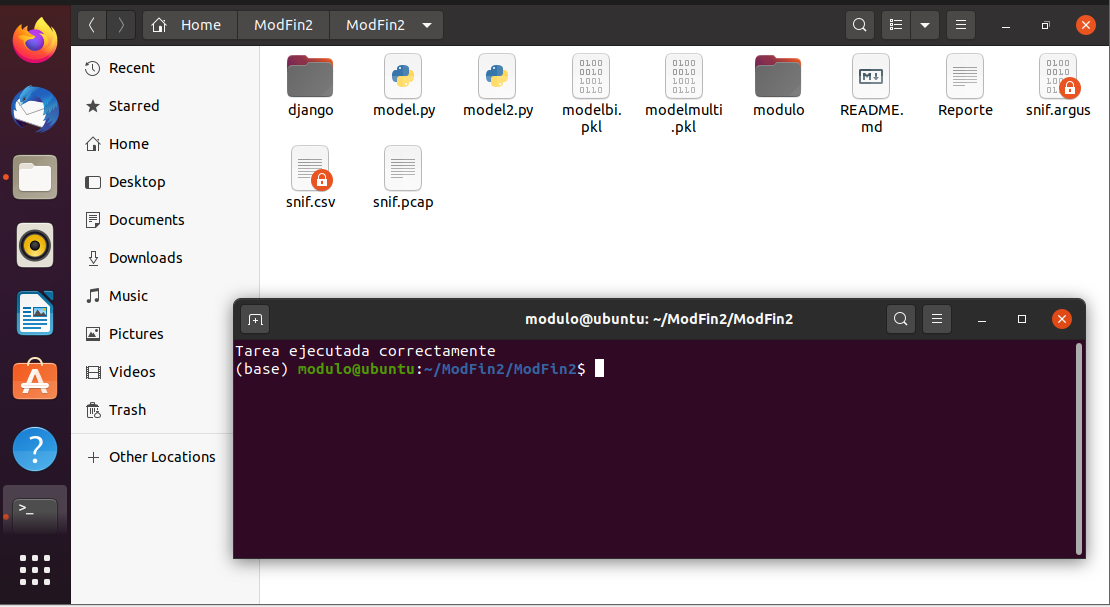
Atacante: Nessus “Plugin Backdoor”

Victima: 172.16.100.6 (Modulo\_Unab)

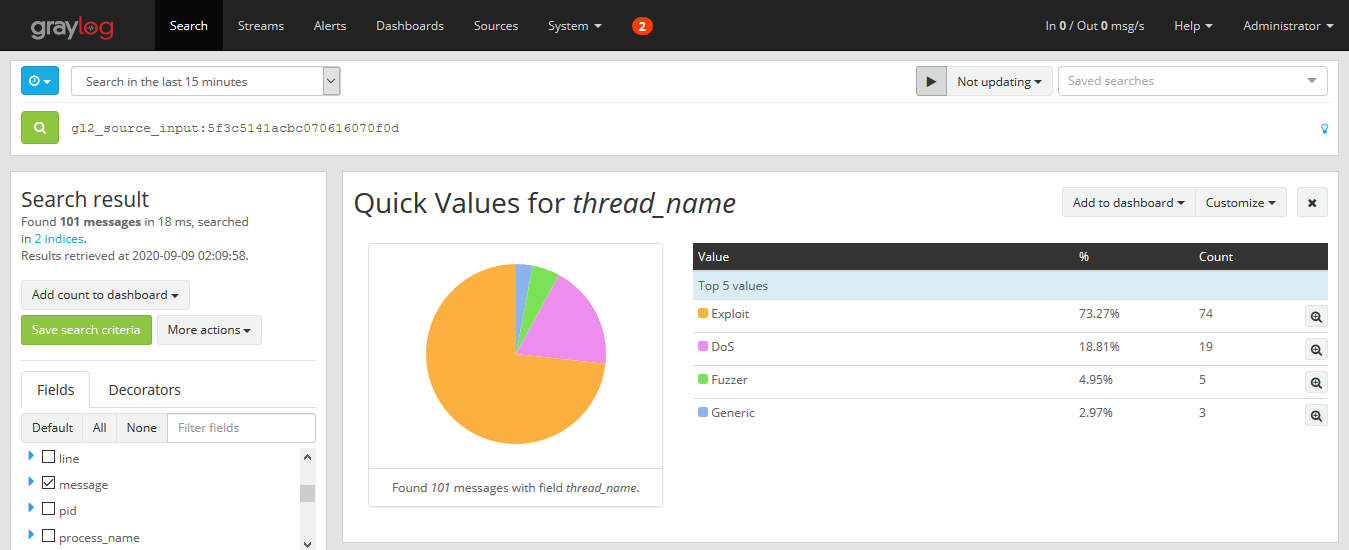
Duración: 5 min.



**Fig. 4 Nessus – Plugin Backdoor**



**Fig. 5 Modulo de categorización - Datasets**



**Fig. 6 Categorización de Ataque “Backdoor” en Graylog**

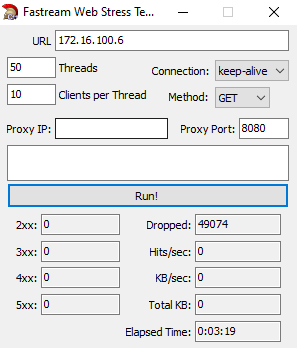
1. **Dos**

El ataque Dos será realizado a través de herramienta “Web Stress Tester”, de acuerdo a siguientes parámetros:

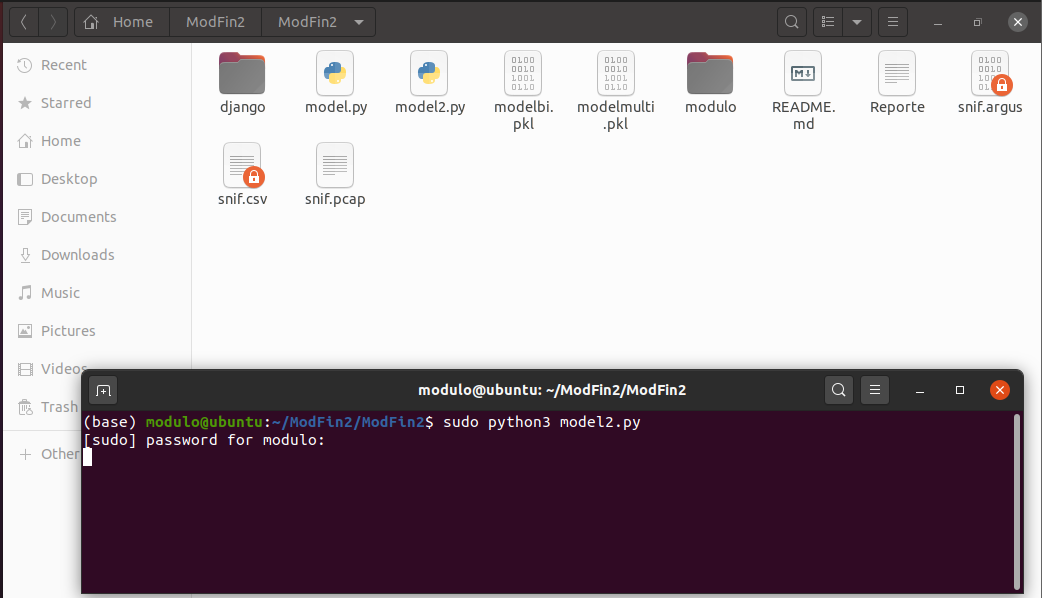
Atacante: Herramienta Web Stress Tester

Victima: 172.16.100.6 (Modulo\_Unab)

Duración: 3 min.



**Fig. 7 Web Stress tester**



**Fig. 8 Modulo de categorización - Datasets**

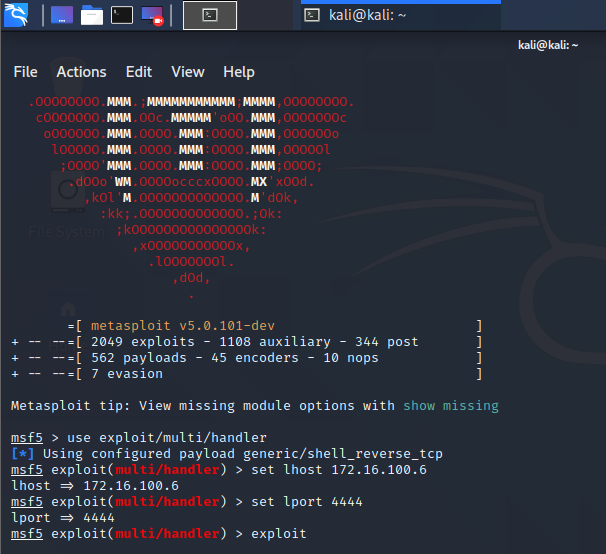
1. **Exploit**

En este siguiente ataque se utilizará Metasploit desde Kali Linux, en el cual se empleara “Exploit Handler”, de acuerdo a siguiente detalle:

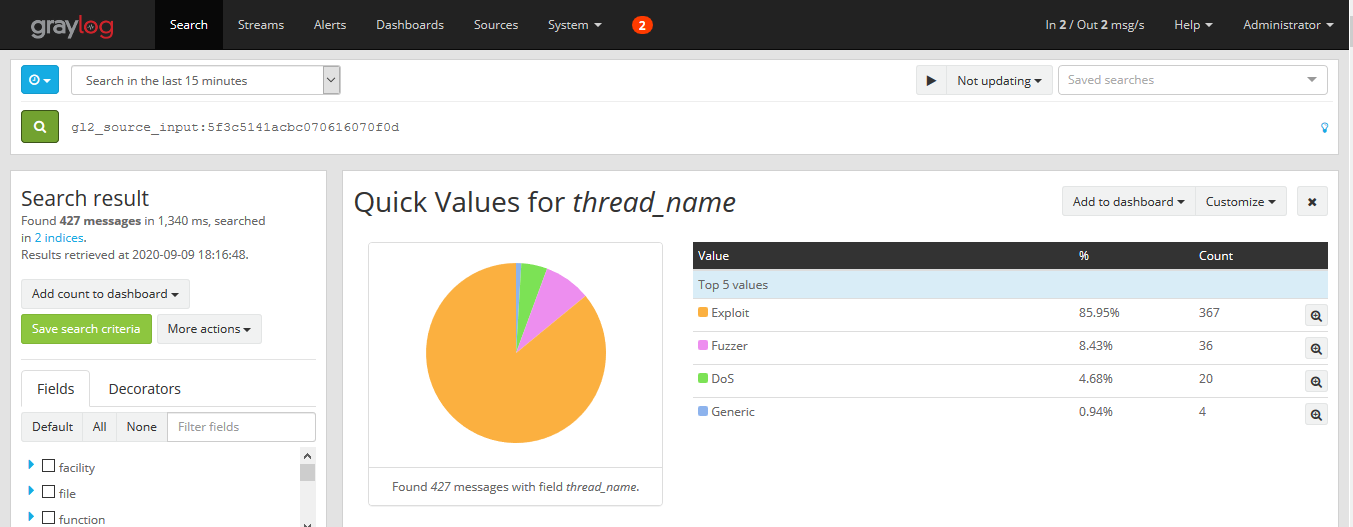
Atacante: Exploit Handler

Victima: 172.16.100.6 (Modulo\_Unab)

Duración: 3 min.



**Fig. 9 Metasploit - Exploit**



**Fig. 10 Categorización de Ataque “Exploit” en Graylog**

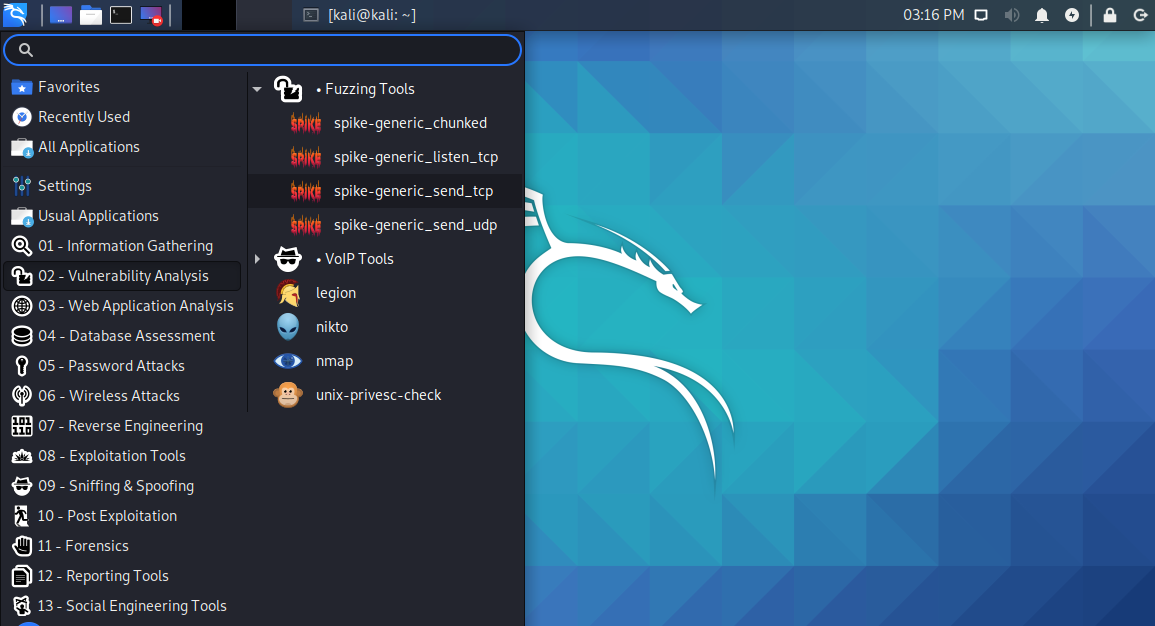
1. **Fuzzer**

A continuación para lleva a cabo este ataque del tipo “Fuzzer” se utilizara el modulo de “Spike-generic\_send\_tcp” de Fuzzing Tools, de acuerdo a siguiente detalle:

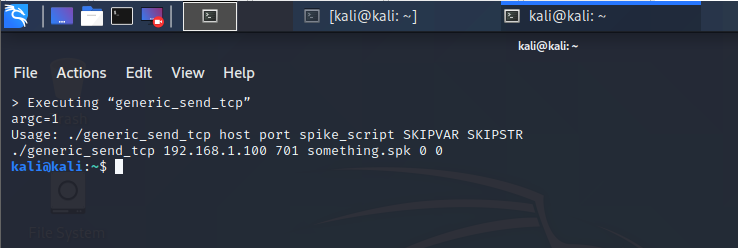
Atacante: Spike-generic\_send\_tcp

Victima: 172.16.100.6 (Modulo\_Unab)

Duración: 5 min.



**Fig. 11 Metasploit – Fuzzing Tools**



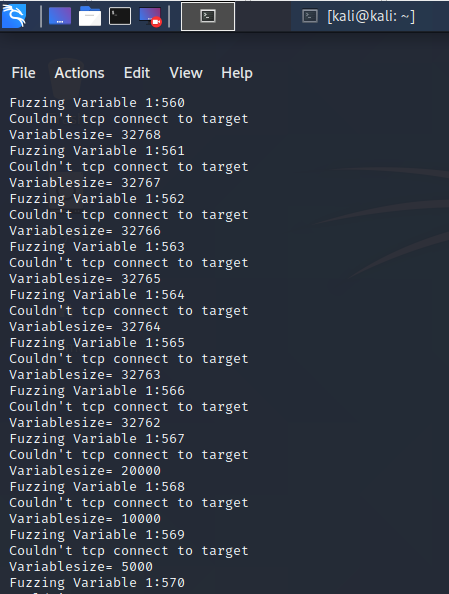
**Fig. 12 Ejecución generic send tcp**

Como podemos ver en la figura 12, cuando ejecutamos este comando, devuelve una pantalla de ayuda básica. Debemos tener en cuenta que para ejecutar este comando, simplemente necesitamos proporcionar:

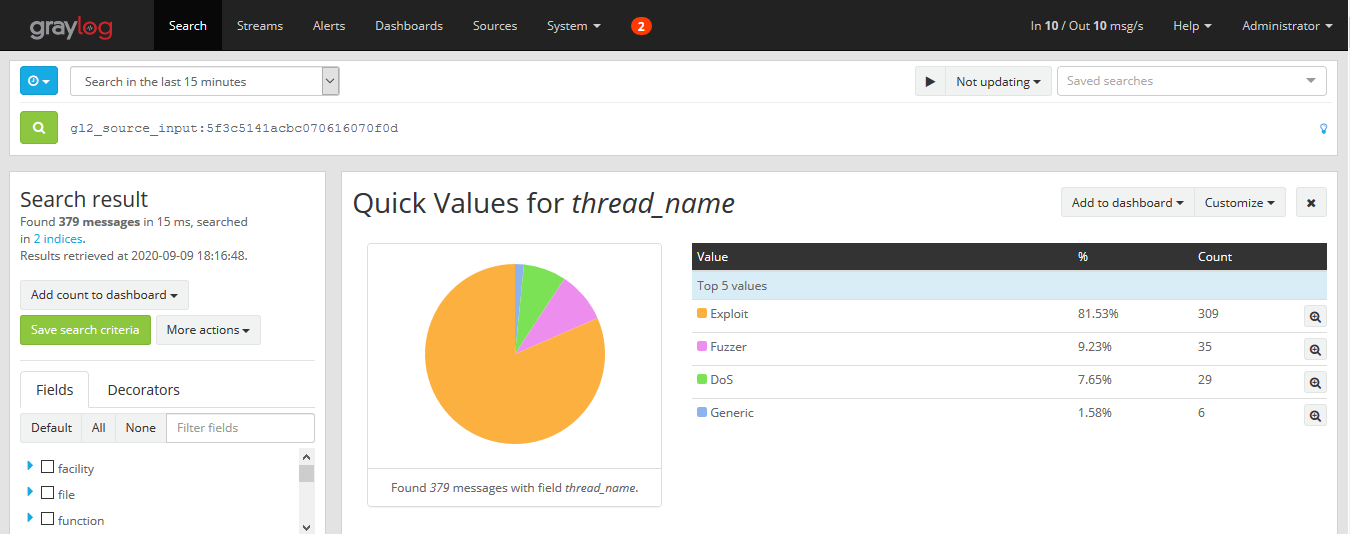
* Dirección IP de destino
* Número de puerto
* Una secuencia de comandos de pico y
* SKIPVAR y SKIPSTR

Ejemplo:

**kali> generic\_send\_tcp 172.16.100.16 9999** **/usr/share/spike/audits/SMTP/smtp1.spk 0 0**



**Fig. 13 Ataque Fuzzing**



**Fig. 14 Categorización de Ataque “Fuzzer” en Graylog**

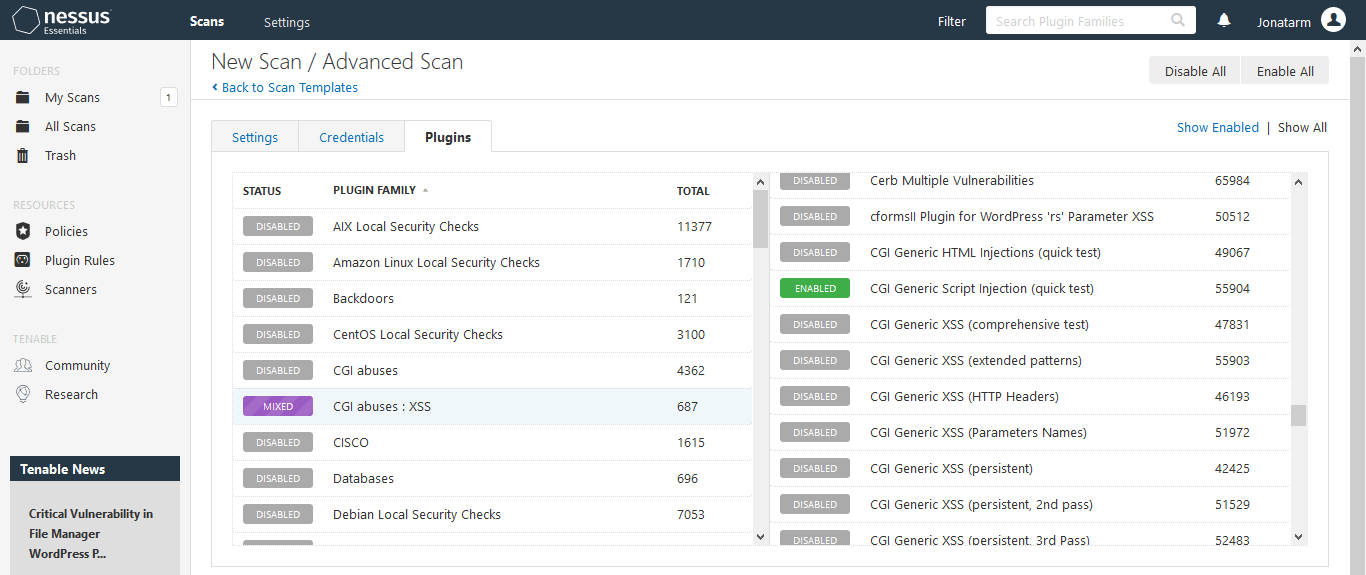
1. **Generic**

Para este tipo de ataque utilizaremos el Plugin “CGI Generic Script Injection” de Nessus, de acuerdo a siguiente detalle:

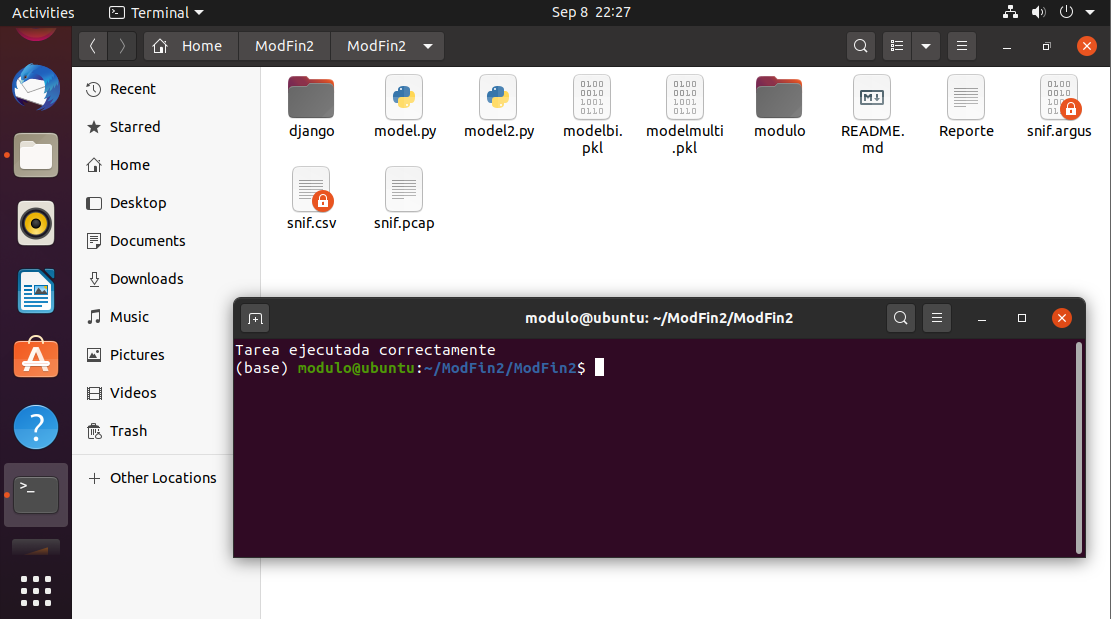
Atacante: CGI Generic Script Injection

Victima: 172.16.100.6 (Modulo\_Unab)

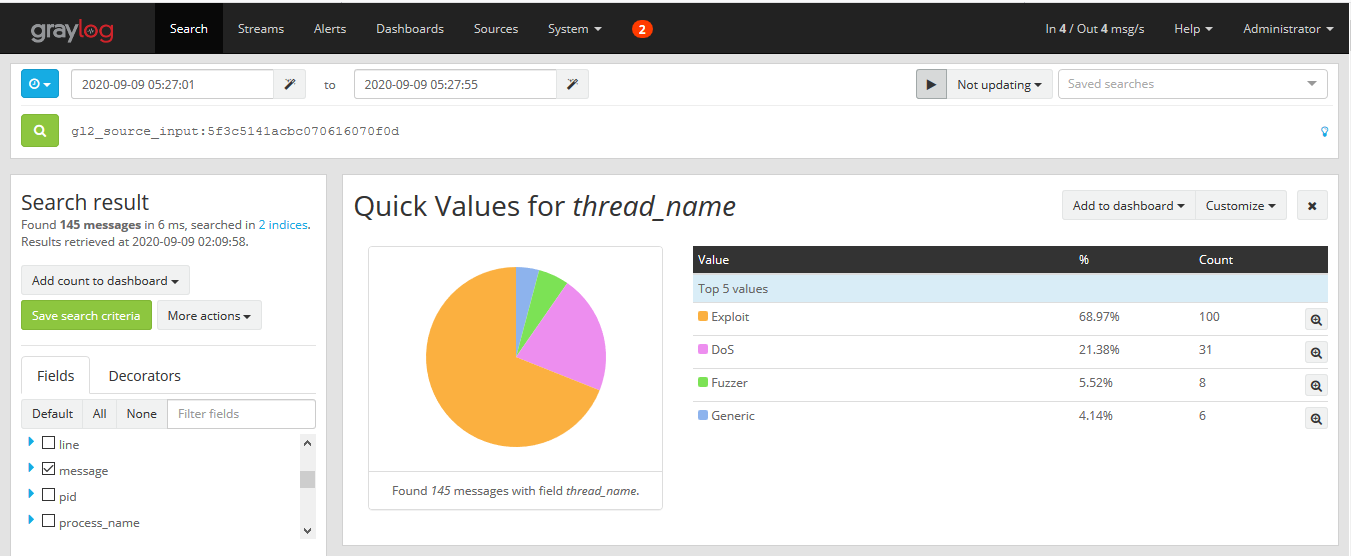
Duración: 5 min.



**Fig. 15 Nessus - CGI Generic Script Injection**



**Fig. 16 Modulo de categorización - Datasets**



**Fig. 17 Categorización de Ataque “Generic” en Graylog**

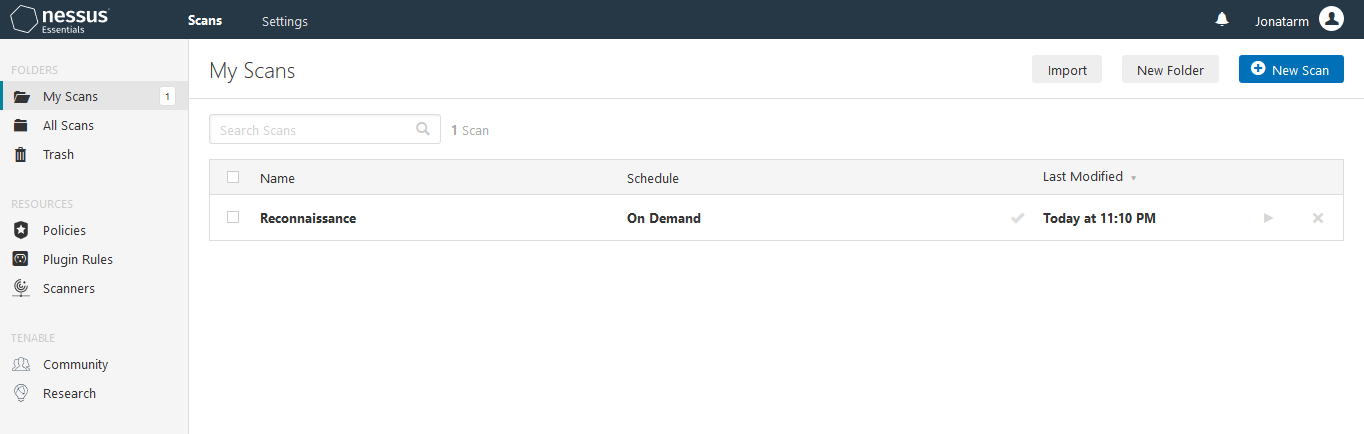
1. **Reconnaissance**

En este ataque utilizaremos un Plugin de Escaneo de Nessus, de acuerdo a siguiente detalle:

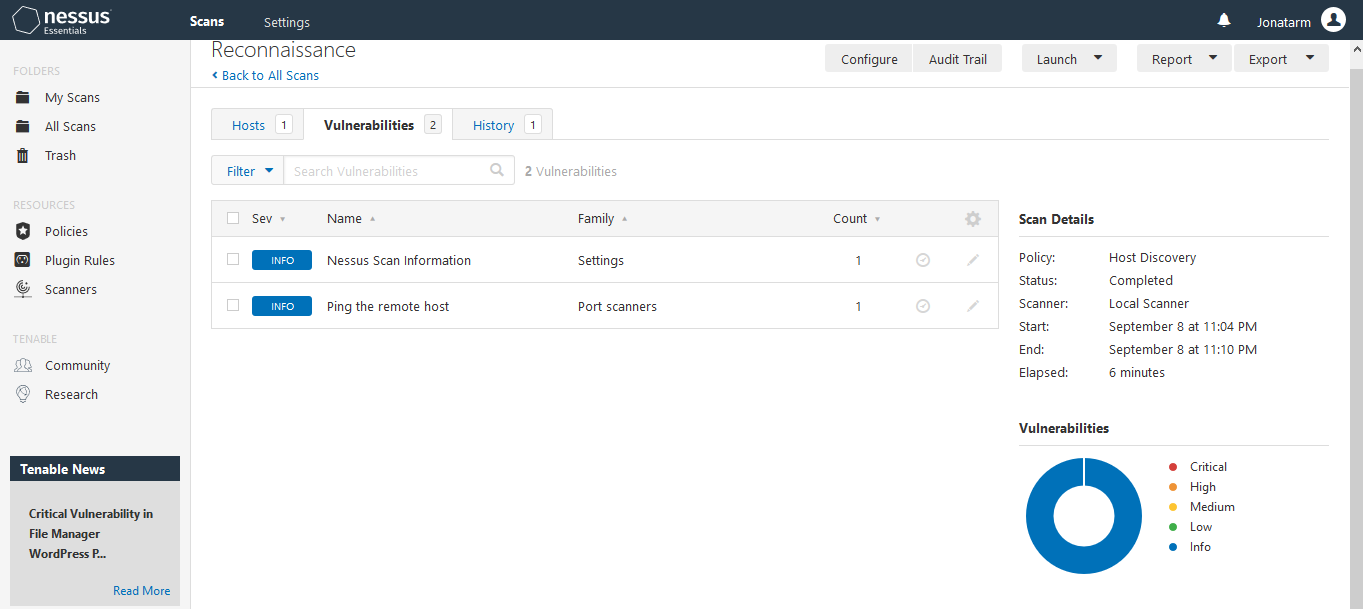
Atacante: Nessus

Victima: 172.16.100.6 (Modulo\_Unab)

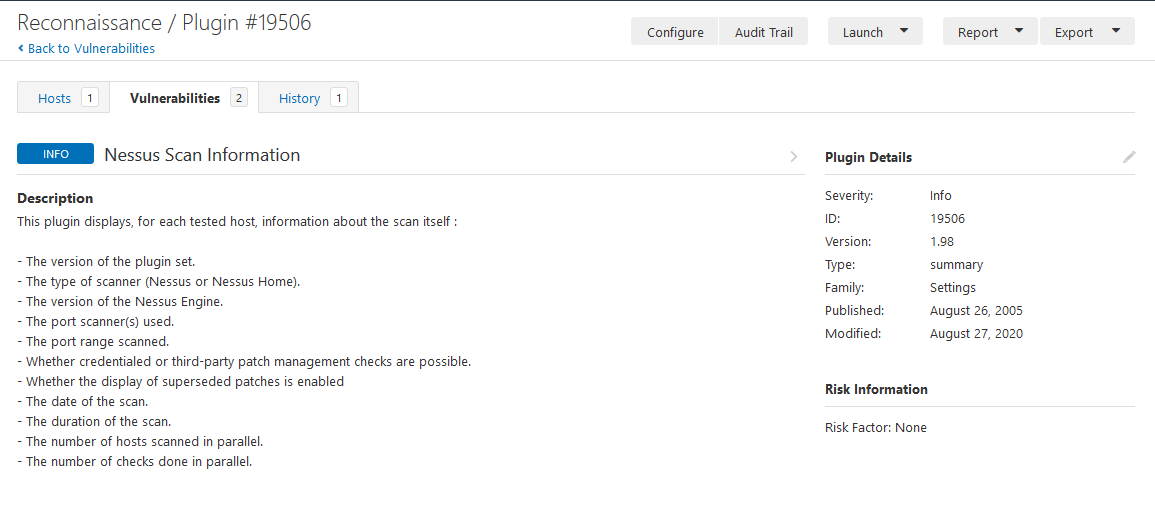
Duración: 5 min.



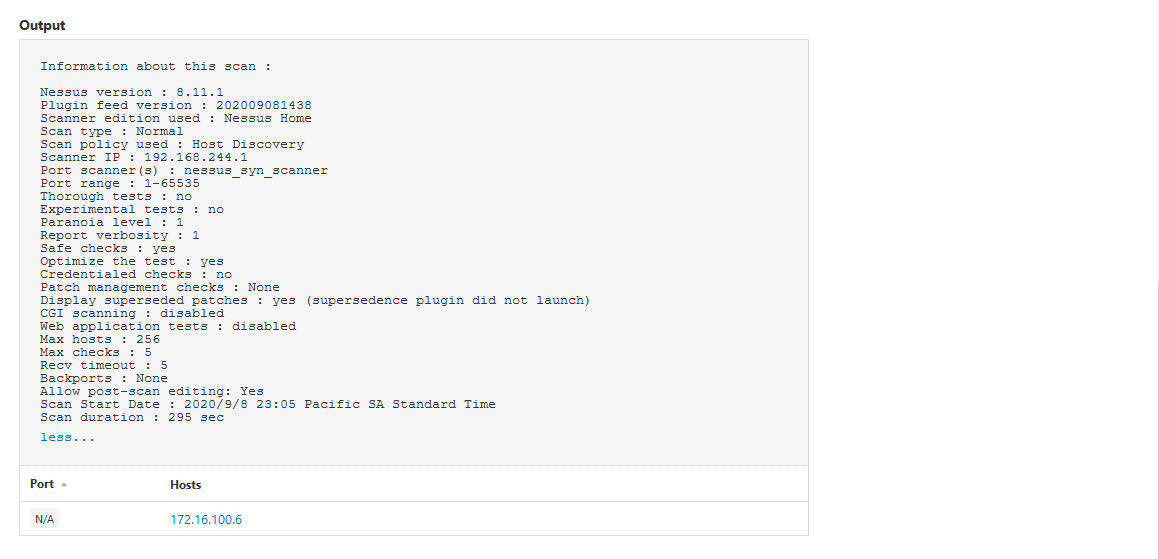
**Fig. 18 Nessus – Recconnaisse 1**



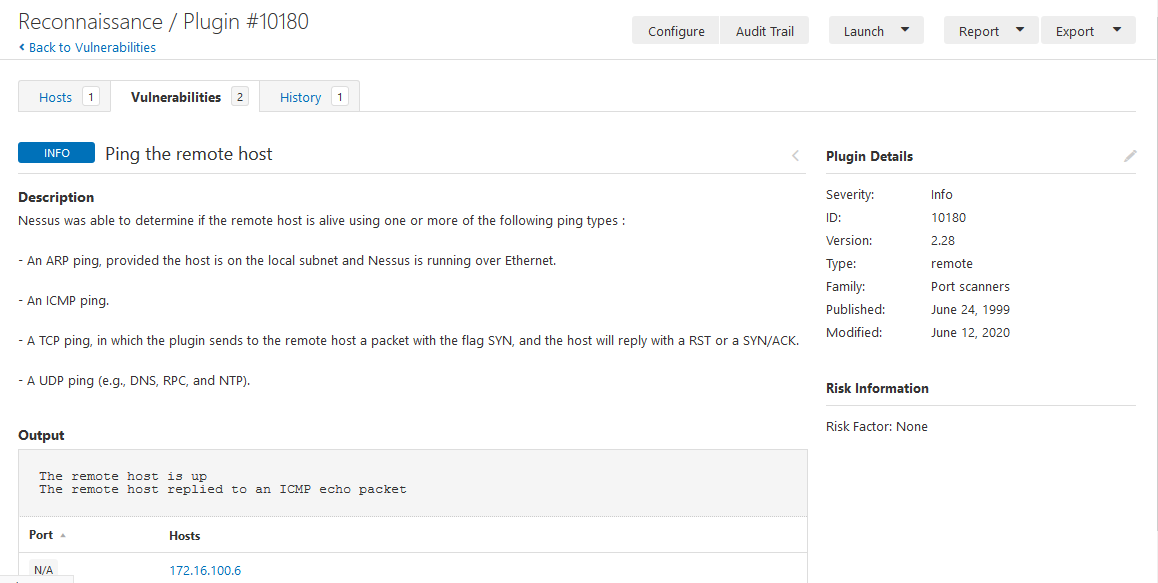
**Fig. 19 Nessus – Recconnaisse 2**



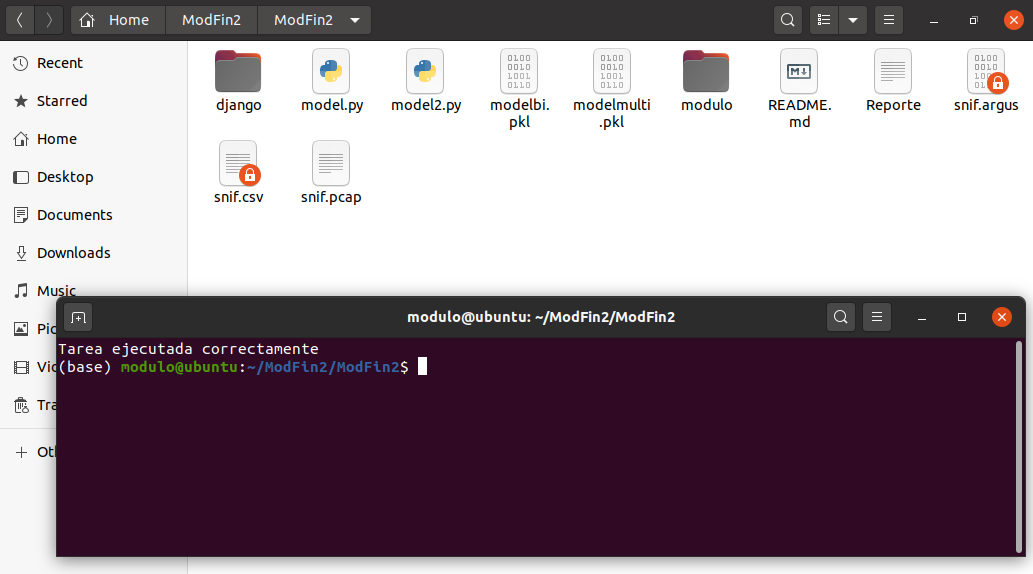
**Fig. 20 Nessus - Information**



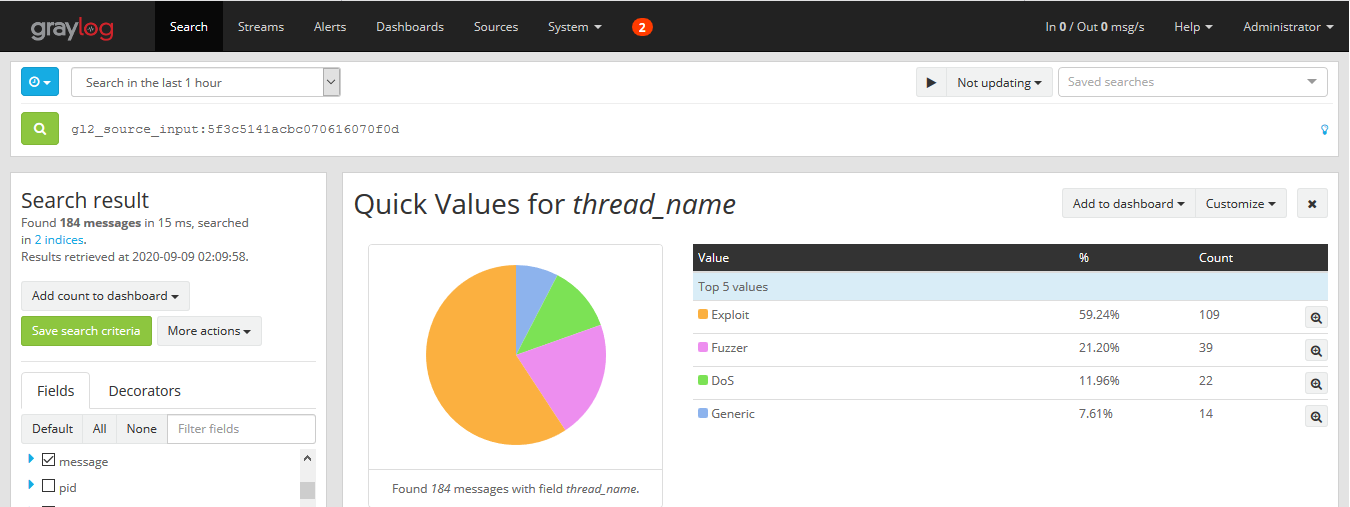
**Fig. 21 Nessus - Salida**



**Fig. 22 Nessus – Ping Remote Host**



**Fig. 23 Modulo de Categorización - Datasets**



**Fig. 24 Categorización de Ataque “Reconnaissance” en graylog**

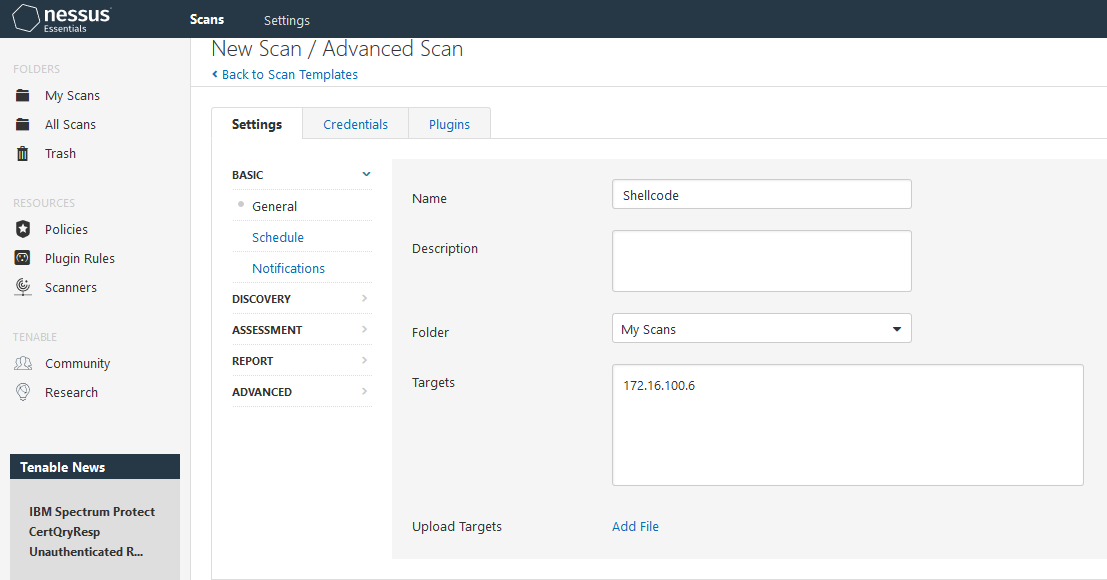
1. **Shellcode**

Para este ataque utilizaremos el Plugin “Bash Remote Code Execution” de Nessus, de acuerdo a siguiente detalle:

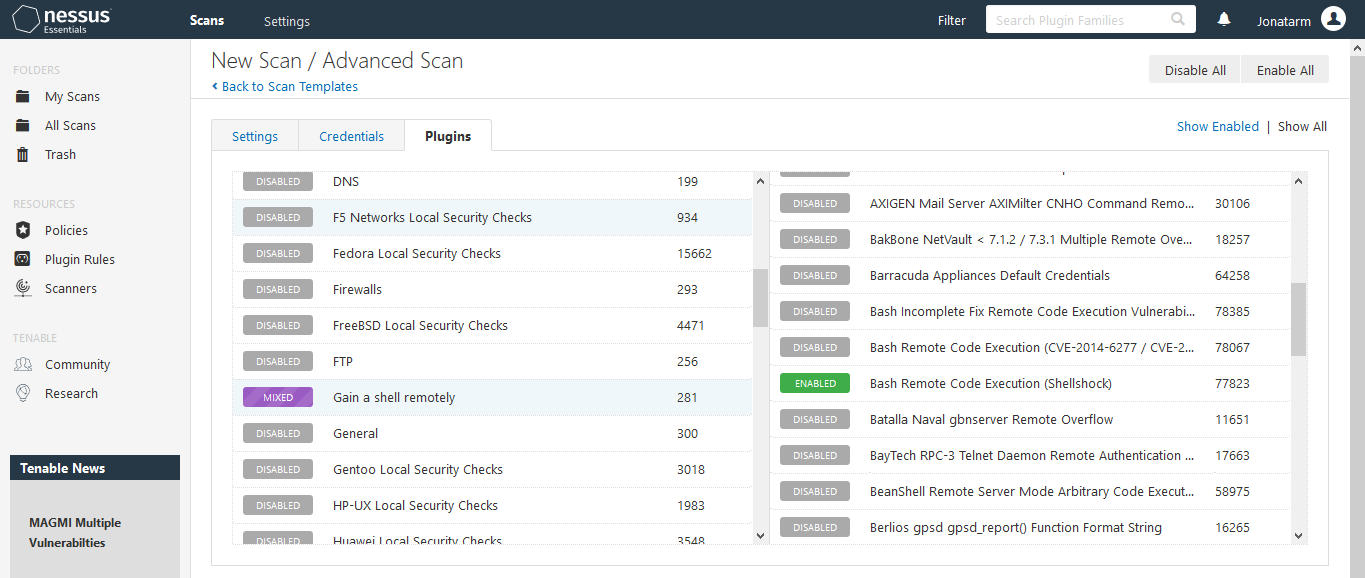
Atacante: Nessus

Victima: 172.16.100.6 (Modulo\_Unab)

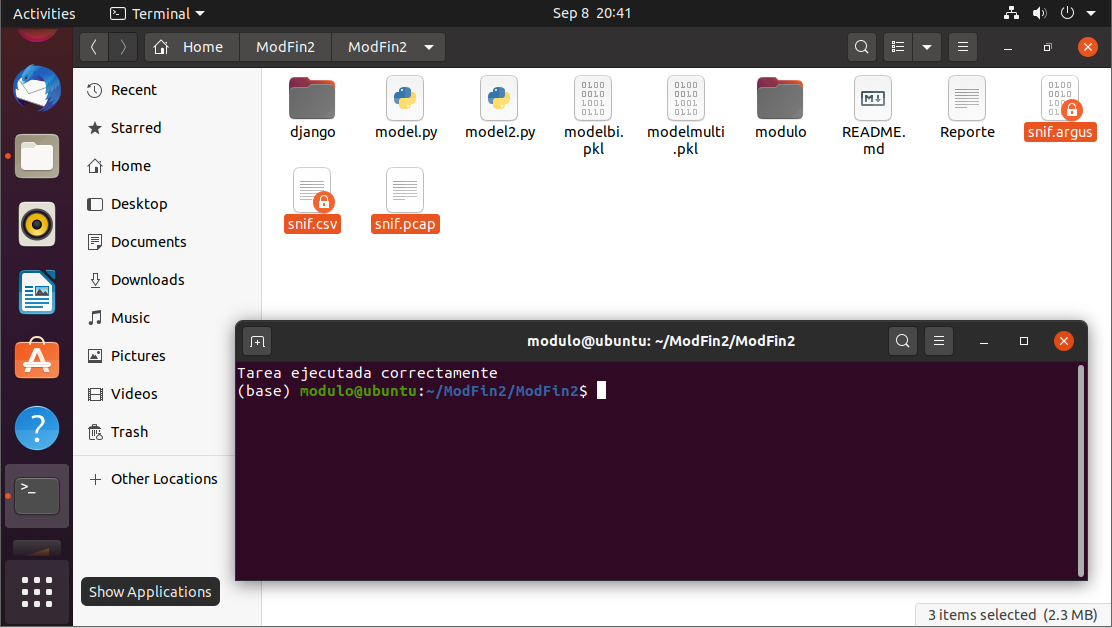
Duración: 5 min.



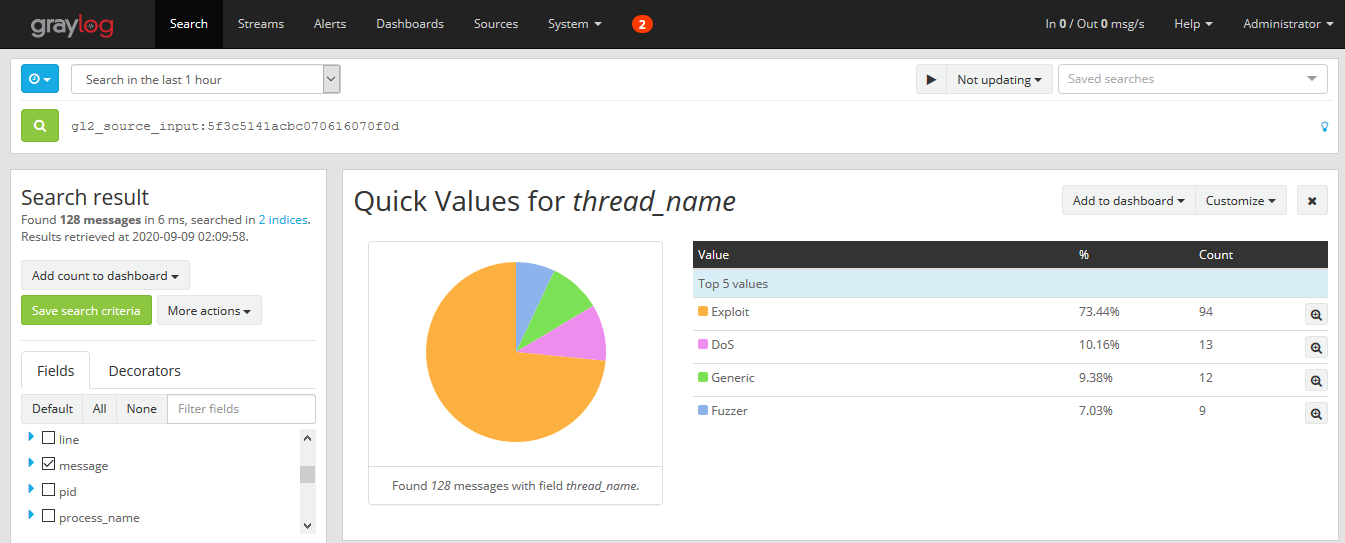
**Fig. 25 Nessus - Shellcode**



**Fig. 26 Nessus – Bash Remote Code Execution**



**Fig. 27 Modulo de Categorización - Datasets**



**Fig. 28 Categorización de Ataque “Shellcode” en Graylog**

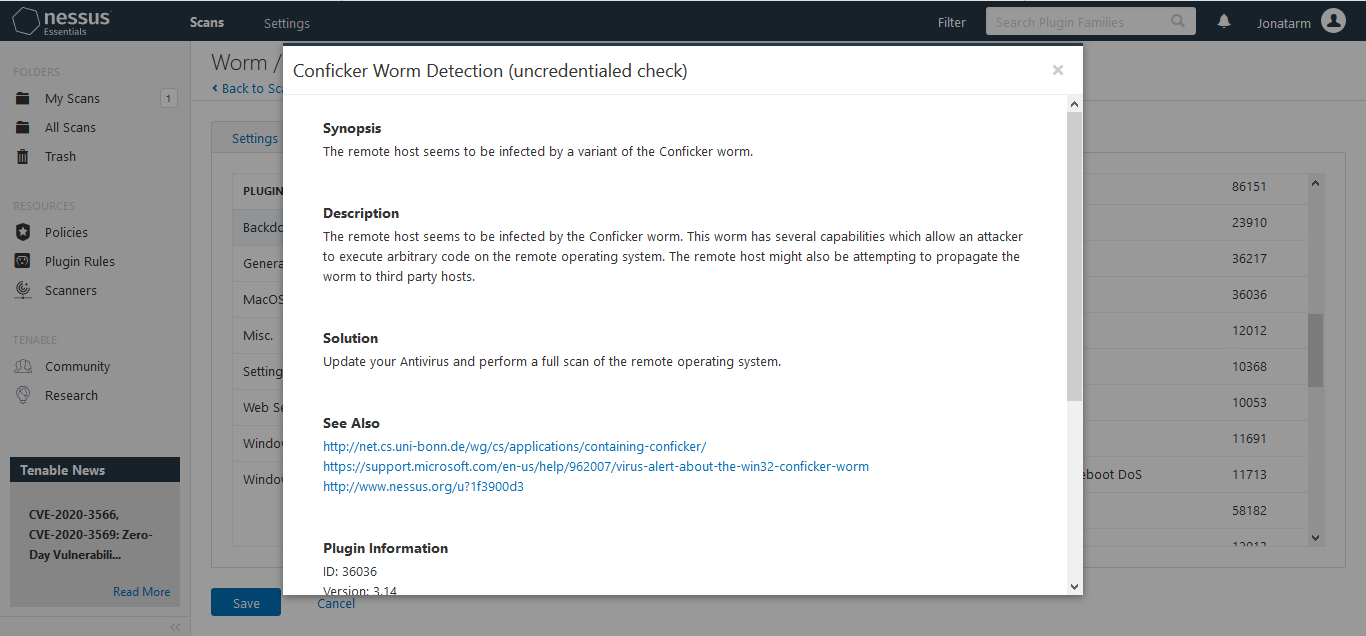
1. **Worm**

Aquí utilizaremos el Plugin “Conficker Worm” de Nessus, de acuerdo a siguiente detalle:

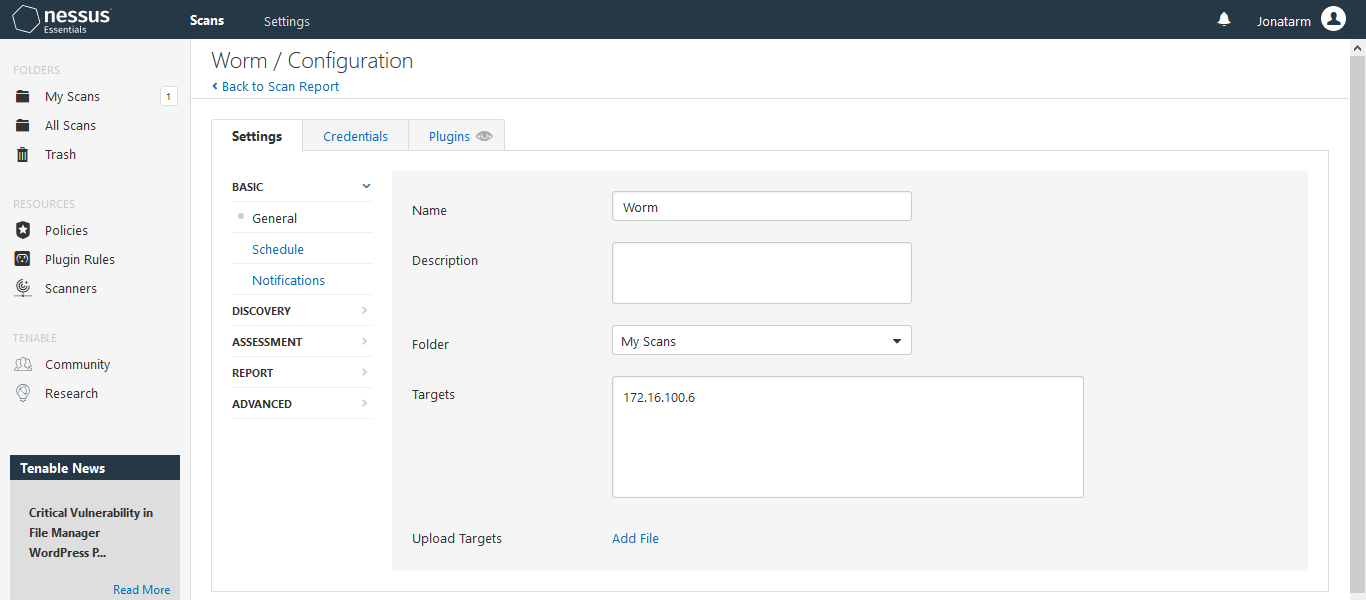
Atacante: Nessus

Victima: 172.16.100.6 (Modulo\_Unab)

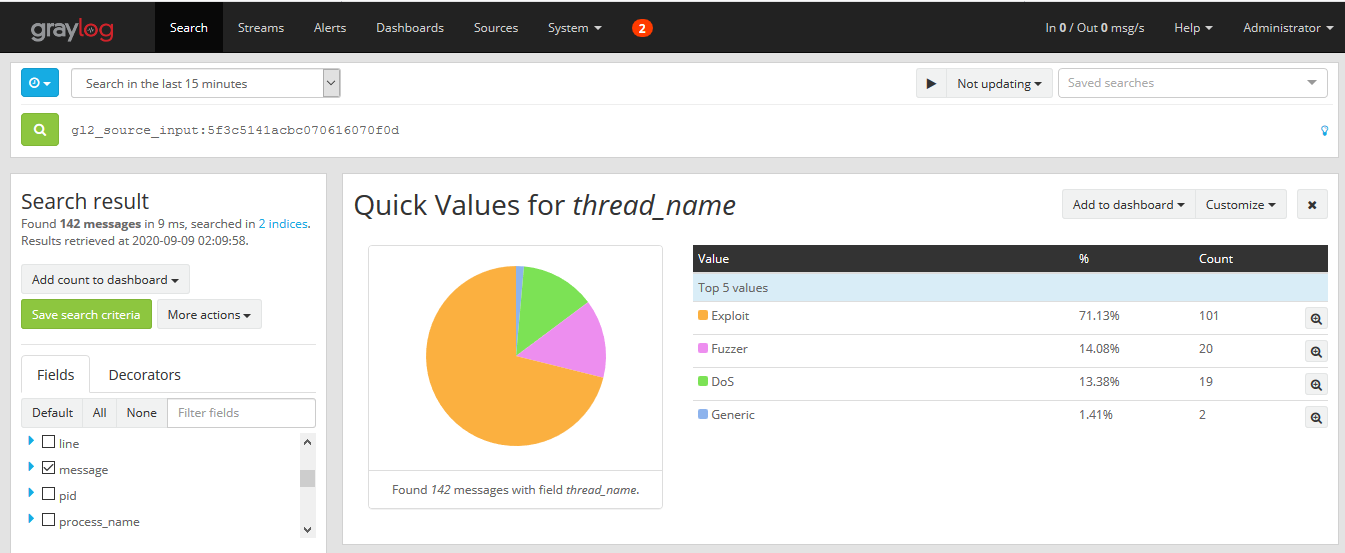
Duración: 5 min.



**Fig. 29 Nessus – Conficker Worm**



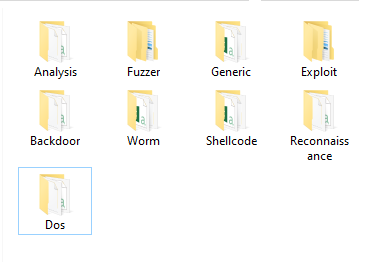
**Fig. 30 Nessus - Worm**



**Fig 31 Categorización de Ataque “Worm” en Graylog**

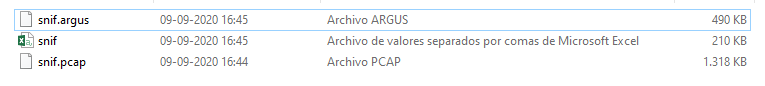
1. **Datasets:**

Respecto a los Datasets, estos se disponibilizaran en diferentes carpetas, de acuerdo a la Figura.



**Fig. 32 Carpetas con Datasets**

Dentro de cada carpeta se encontrara el Dataset de cada tipo de Ataque en los 3 formatos que trabaja el Modulo (**snif.pcap, snif.argus, snif.csv**), tal como se muestra en la Figura 33.



**Fig. 33 Dataset en formatos**

1. **Conclusión**

De acuerdo a los ataque realizados y a las maquinas virtuales que tuvieron que implementarse, se concluye que cada vez que se incluyen otros módulos o requerimientos, el consumo de recursos se incrementa en gran manera, principalmente en lo que respecta a Memoria RAM, Procesadores y Almacenamiento.

Por otra parte se detecto que el Modulo de Categorización, detecta en gran porcentaje (70 %) a los diferentes tipos de Ataques como “Exploit”, esto lo podemos revisar en las distintas figuras adjuntas en este documento.