פרויקט BlizShield

מנחה: אמיר קירש

מספר פרוייקט: 220104

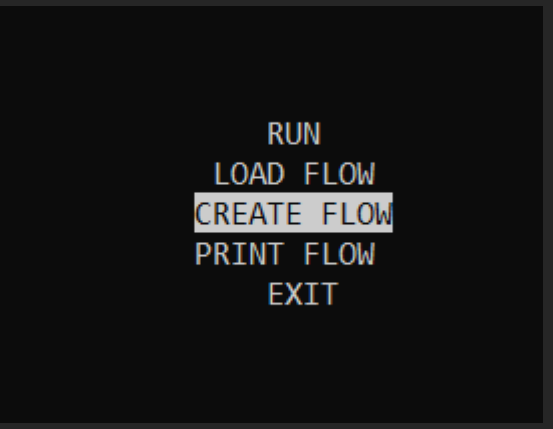
מגישים: יפים אשכנזי, אלמוג רבינוביץ ועידן אלבוים

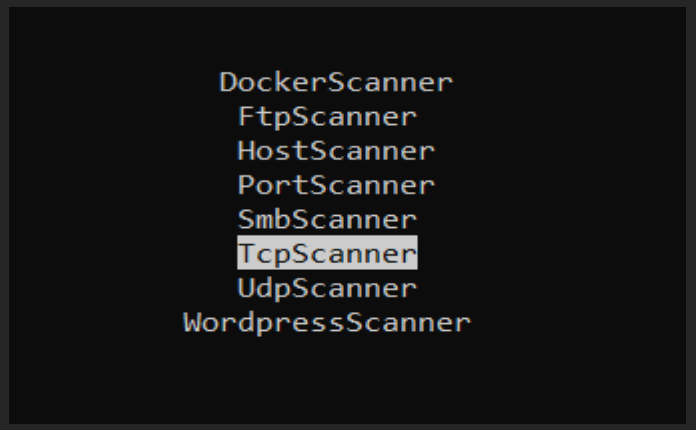
- רשתות enterprise מכילות מספר הולך וגובר של שירותים ואפליקציות .

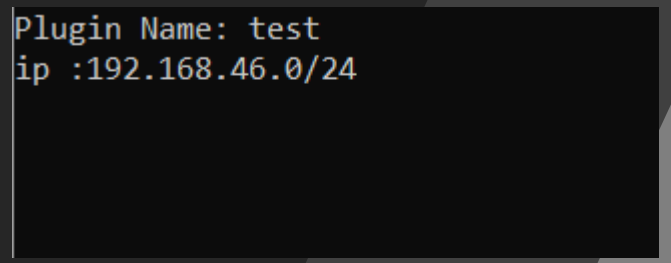
- במקביל נדרש להחזיק מיפוי של שירותים אלו, בדיקות סטטוס מהירות, בפרט בעת גילוי חולשה משמעותית.

BlizShield הוא פרויקט סריקות Opensource המאפשר לייצר תמונת מצב של הרשת בצורה מונגשת ונוחה

- מודולריות – סריקות מבוססי לוגיקות ותוצאות סריקות קודמות להחלטת המשתמש
- תאימות – מערכת גנרית תומכת בפשטות בהוספת יכולות נוספות
- הצגת תוצאות הסטטוס בדשבורדים סיכומים המספקים תמונת מצב אבטחתית של הרשת


RUN
LOAD FLOW
CREATE FLOW
PRINT FLOW
EXIT


DockerScanner
FtpScanner
HostScanner
PortScanner
SmbScanner
TcpScanner
UdpScanner
WordpressScanner


Plugin Name: test
ip :192.168.46.0/24

General / all scans by client

Last 90 days | 5s

Last run	Client	Testers	Scan Types	Runs
2022-09-13 13:30:52.780	client	["tester", "tester", "tester", "tester", "tester", "tester", "tester", "teste…	["PortScanner", "PortScanner", "PortScanner", "PortScanner", "PortScanner", "…	["d57dc1a8-94de-4223-b67d-afe5f…
2022-09-13 11:20:11.373	Yoni	["Asaf", "Asaf", "Asaf", "Asaf", "Asaf", "Asaf", "Asaf", "Asaf", "Asaf", "Asa…	["HostScanner", "HostScanner", "PortScanner", "PortScanner", "PortScanner", "…	["f48308bc-6921-4b09-8c63-bfc50…
2022-09-13 11:18:00.914	Idan	["Idan", "Idan", "Idan", "Idan", "Idan", "Idan", "Idan", "Idan", "Idan", "Ida…	["HostScanner", "WordpressScanner", "WordpressScanner", "WordpressScanner", "…	["a67c610d-e32c-4bff-8984-234e8…
2022-09-13 11:15:01.135	Zen	["Toly", "Toly", "Toly", "Toly", "Toly", "Toly", "Toly", "Toly", "Toly", "Tol…	["WordpressScanner", "WordpressScanner", "WordpressScanner", "WordpressScanne…	["c9db8264-b9ac-4b58-b034-65d40…
2022-09-13 11:05:43.987	ben	["almog", "almog", "almog", "almog", "almog", "almog", "almog", "almog", "alm…	["HostScanner", "WordpressScanner", "WordpressScanner", "WordpressScanner", "…	["188ea4dc-96f8-455d-8e83-ad9c0…
2022-09-10 21:35:08.961	client2	["tester", "tester", "tester", "tester", "tester", "tester", "tester", "tester", "tester", "tester", "tester", "tester"]	ner", "PortScanner", "PortScanner", "…	["f7bcfed9-441c-4e29-9354-b5836…

▾Array[12]
  0: "tester"
  1: "tester"

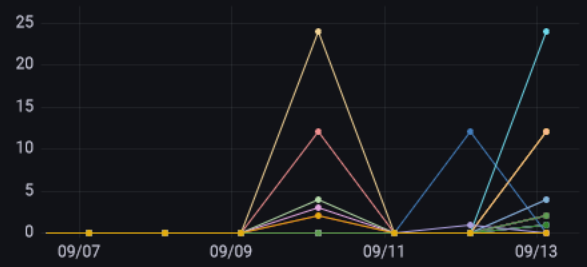
General / Bad Results Client Summary Dashboard Single Scan

Last 7 days

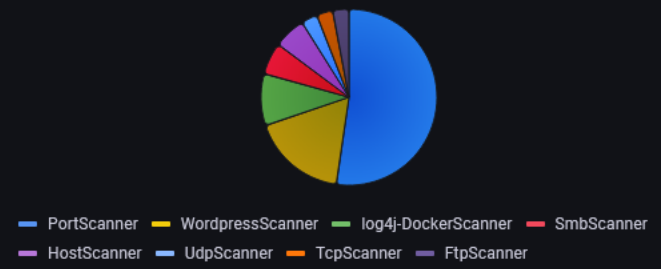
All Scans

Timestamp	Tester	Run ID	Scans
2022-09-13 13:30:52.780	tester	d57dc1a8-94de-4223-b67d-afe5f91ab565	["PortScanner", "PortScanner", …
2022-09-13 10:59:19.232	tester	a7c09241-0f39-49bb-9d6a-287302d797bb	["WordpressScanner", "Wordpress…
2022-09-13 10:54:40.610	tester	e5530c5e-b3df-41d7-8feb-e45a82ab59eb	["log4j-DockerScanner", "log4j-…
2022-09-13 10:46:14.785	tester	4f6b49f5-31c8-4928-beb0-d579c18a8900	["log4j-DockerScanner", "log4j-…
2022-09-13 10:45:25.873	tester	41e8bd28-32de-43f0-9a59-8cc3ebac56a4	["log4j-DockerScanner"]

Client's Scans over Time



Scan type distribution



Critical Results

vulnerable wordpress servers

scan time	host	description
2022-09-12 21:34:44.008	138.68.90.29	The external WP-Cron seems to be enabled: http://138.68.90.29/wp-cron.php
2022-09-12 21:34:44.008	138.68.90.29	
2022-09-12 21:34:44.008	138.68.90.29	WordPress readme found: http://138.68.90.29/readme.html

found hosts in subnet

last time scanned	subnet	found host	status
2022-09-13 10:57:07	rabinovit.ch	80.241.223.227	true
2022-09-10 21:16:13	138.68.90.29	138.68.90.29	true
2022-09-10 21:16:13	10.0.0.3	10.0.0.3	false

All Open servers found for FTP protocol

last time scanned	ip	username	password
2022-09-10 21:14:02	138.68.90.29	anonymous	<no password>

vulnerable wordpress servers

scan time	service	is vulnerable
2022-09-13 10:42:21.187	-u http://rabinovit.ch:92…	false
2022-09-13 10:54:40.610	-u http://172.21.80.1:92…	true
2022-09-13 10:46:07.803	-u http://127.0.0.1:8000…	false
2022-09-13 10:44:40.179	-u http://192.168.195.2…	false
2022-09-13 10:42:21.187	-u http://172.21.80.1:92…	false
2022-09-13 10:30:50.673	-u http://192.168.195.2…	true

vunlerable for log4j

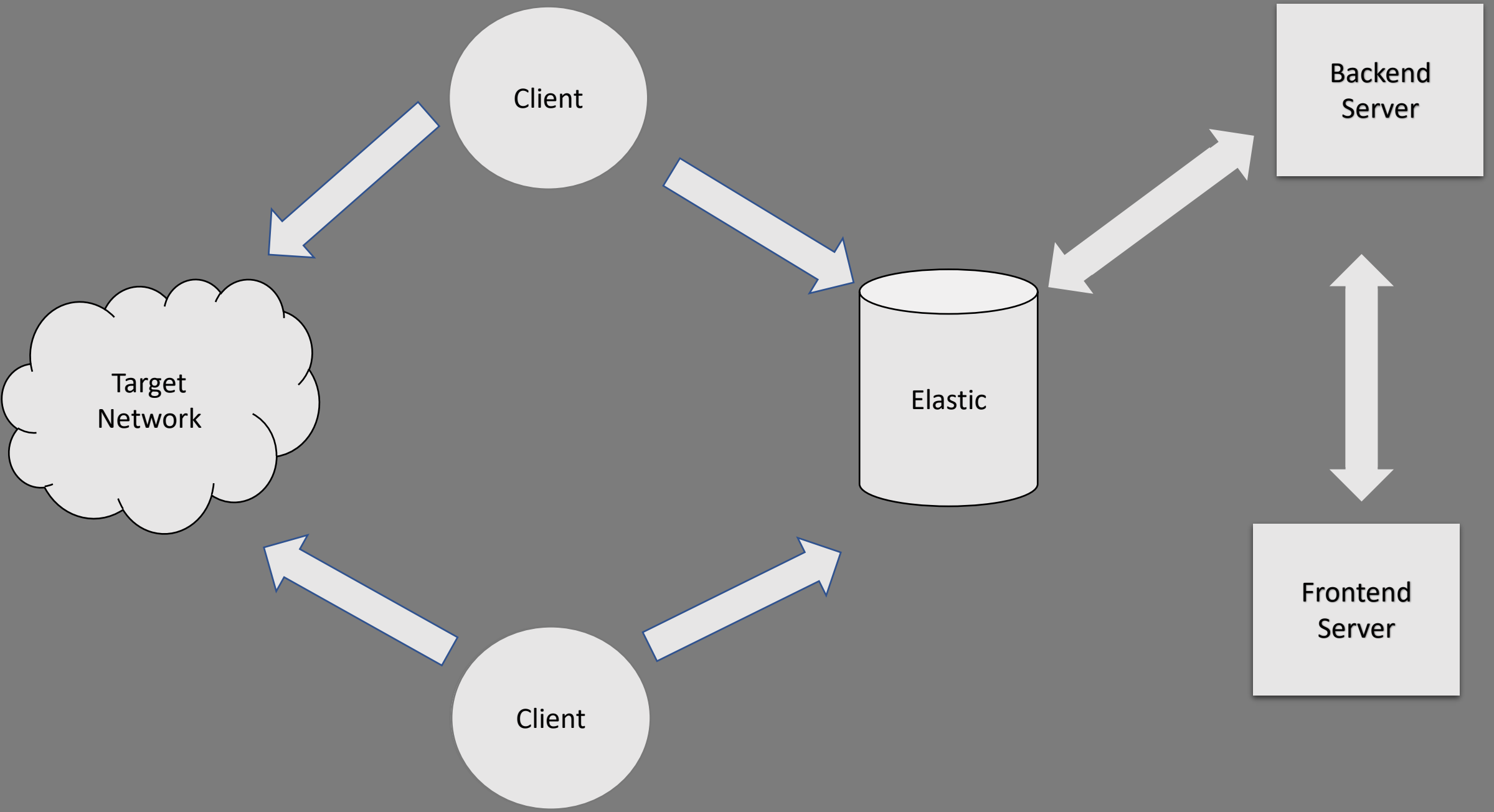
last time scanned	Server	is vulnerable
2022-09-13 10:54:40.610	-u http://172.21.80.1:9200/ --disable-…	true
2022-09-13 10:30:50.673	-u http://192.168.195.224:8000/ --dis…	true

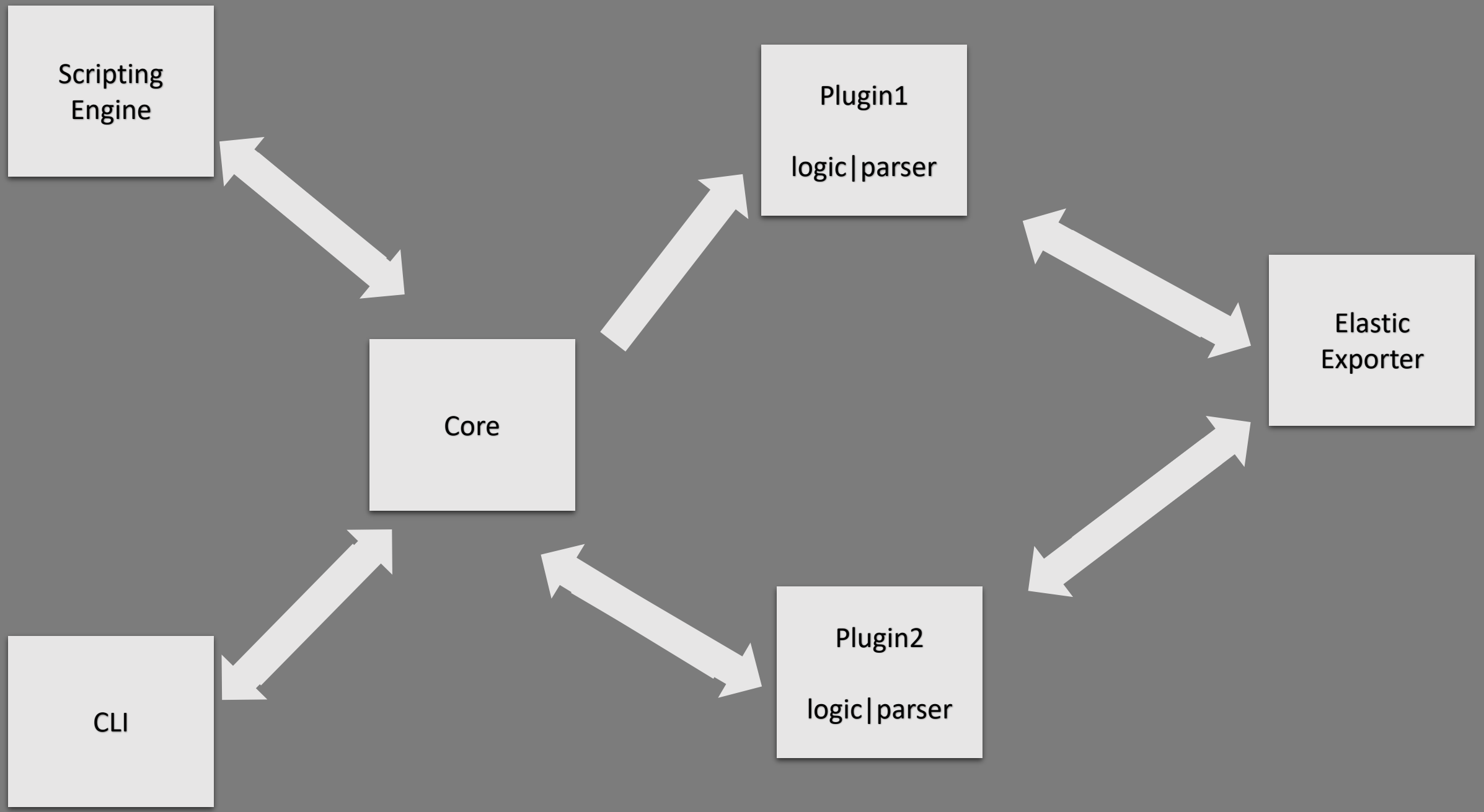
All Open shares found for SMB protocol

last time scanned	ip	password	username
2022-09-10 21:25:54	138.68.90.29	root	root

Open ports Found

last time scanned	ip	port	protocol	was the port open last time
2022-09-10 21:24:46	138.68.90.29	80	TCP	true


Client
Backend Server
Target Network
Elastic
Frontend Server
Client


Scripting Engine
Plugin1
logic|parser
Core
Elastic Exporter
CLI
Plugin2
logic|parser

elasticsearch

פתרונות אחרים בשוק:

- הטמעה הדורשת משאבים רבים
- מוצר blackbox ותלות ביצרנית ואינטגרטורים
- שליטה שאינה 100% ביכולות המוצר

תודה!