

SOC ANALYST

PROJECT - CHECKER

STUDENT NAME: Tomer Dery

Unit: TMagen773637

Student Code: s5

Program Code: NX220

Lecturer: Eliran

Project Explanation

This document presents the automated SOC attack simulation tool developed for Project CHECKER. The tool helps SOC teams stay alert by simulating different types of network attacks including DOS, MITM, and Brute Force attacks. The system logs all activities for audit and training compliance purposes.

Key Features

- Network interface selection and IP discovery using Nmap
- Three attack types: DOS (Hping3), MITM (Arpspoof), Brute Force (Hydra)
- Target selection (specific or random) from discovered hosts
- Comprehensive attack logging with timestamps to /var/log
- Loop functionality for multiple attack simulations
- Input validation and error handling

Script Overview

The CHECKER tool is written in Bash and integrates industry-standard penetration testing tools. The script operates through a structured workflow: privilege verification, network discovery, attack selection, target selection, attack execution, and comprehensive logging. Each stage is clearly communicated to the user with color-coded output.

SYSTEM INITIALIZATION

The script begins by verifying root privileges, which are essential for running network attack tools. After confirmation, the system displays the CHECKER banner using figlet.

Network Interface Selection

The script automatically detects all active network interfaces on the host and displays them with their corresponding IP addresses. The user selects the appropriate interface for the attack simulation. The script validates the selection to ensure a valid interface is chosen.

Scan Configuration

After interface selection, the user chooses the type of network scan:

- **Fast Scan** - Quick reconnaissance of common ports.
- **Full Scan** - Comprehensive scan including service detection and OS detection.
- **Vulnerability Scan** - Deep analysis with NSE vulnerability scripts.

The scan excludes the attacker's own IP address to focus on target systems only.

```
(kali㉿kali)-[~/Desktop/ PROJECT: CHECKER]
$ sudo ./TMagen773637.s5.NX220.sh
[*] Available network interfaces in the host:
1) lo - 127.0.0.1
2) eth0 - 192.168.153.129
[?] please choose the network interface by number 2
[+] you have chosen eth0 with IP 192.168.153.129
[?] Please select the type of Nmap scanning to run:
1) Fast scan
2) Full scan
3) Vuln scanning
```

NETWORK DISCOVERY

The script uses Nmap to discover live hosts on the selected network. The scan results are parsed and displayed in a numbered list, making it easy for users to select targets for attack simulation.

Scan Execution

Depending on the selected scan type, Nmap runs with different parameters:

- **Fast Scan:** nmap -Pn -F --exclude [attacker_IP] [network]/24
- **Full Scan:** nmap -sS -Pn -O -A -sU -p- --exclude [attacker_IP] [network]/24
- **Vuln Scan:** nmap --script vuln -A -p- -Pn --exclude [attacker_IP] [network]/24

Host Discovery Results

The script extracts IP addresses from the Nmap output and displays them in a formatted list. Each discovered host is assigned a number for easy reference during target selection.

Example discovered hosts:

- 1) 192.168.153.1
- 2) 192.168.153.2
- 3) **192.168.153.161** (Metasploitable2 target)
- 4) 192.168.153.254

```
(kali㉿kali)-[~/Desktop/ PROJECT: CHECKER]
$ sudo ./TMagen773637.s5.NX220.sh
[?] Please select the type of Nmap scanning to run:
1) Fast scan
2) Full scan
3) Vuln scanning
[?] Choose your scan type (1-3): 1
[*] Running nmap scan... This may take a while
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-10 02:55 EST
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 62.94% done; ETC: 02:55 (0:00:01 remaining)
Nmap scan report for 192.168.153.1
Host is up (0.00027s latency).
All 100 scanned ports on 192.168.153.1 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.153.2
Host is up (0.00020s latency).
Not shown: 99 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F1:30:01 (VMware)

Nmap scan report for 192.168.153.161
Host is up (0.00038s latency).
Not shown: 82 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
```

```
(kali㉿kali)-[~/Desktop/ PROJECT: CHECKER]
$ sudo ./TMagen773637.s5.NX220.sh
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
MAC Address: 00:0C:29:4F:55:26 (VMware)

Nmap scan report for 192.168.153.254
Host is up (0.00012s latency).
All 100 scanned ports on 192.168.153.254 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
MAC Address: 00:50:56:EB:80:B9 (VMware)

Nmap done: 255 IP addresses (4 hosts up) scanned in 4.22 seconds
[+] Scan complete!
[*] Discovered hosts on the network:
1) 192.168.153.1
2) 192.168.153.2
3) 192.168.153.161
4) 192.168.153.254
```

ATTACK SELECTION

After discovering live hosts, the system presents an interactive attack menu with four options, each with a detailed description of its functionality.

Available Attack Option

1) DOS Attack (Hping3)

- Floods target SYN packets to overwhelm resources
- Simulates Denial of Service attack
- Uses hping3 with --flood mode for 10 seconds

2) MITM Attack (Arpspoof)

- ARP poisoning to intercept network traffic
- Enables IP forwarding for man-in-the-middle positioning
- Runs for 15 seconds with automatic cleanup

3) Brute Force Attack (Hydra)

- Attempts to crack SSH passwords
- Uses common password wordlist
- Tests SSH service on port 22 for 30 seconds

4) Random Attack

- Randomly selects one of the above attacks
- Useful for unpredictable SOC training scenarios

Input Validation

The script validates user input to ensure only valid attack types are selected (1-4). Invalid inputs trigger error messages and prompt the user to re-enter their choice.

```
[*] Available Attack Options:  
1) DOS Attack (Hping3) - Floods target with SYN packets to overwhelm resources  
2) MITM Attack (Arpspoof) - ARP poisoning to intercept network traffic  
3) Brute Force (Hydra) - Attempts to crack SSH passwords  
4) Random Attack - Randomly selects one of the above attacks  
[?] Choose attack type (1-4): 1
```

TARGET SELECTION & ATTACK EXECUTION

Once an attack type is selected, the system prompts for target selection.

Target Selection Methods

The user has two options for selecting attack targets:

1) Choose specific IP from list

- Displays of all discovered hosts again
- User selects by number
- Validates selection is within range

2) Random target from discovered IPs

- System automatically selects a random host
- Displays which target was chosen

Attack Execution Examples

DOS Attack Execution:

- Displays attack launch message.
- Sends 1000 SYN packets using hping3.
- Runs for maximum 10 seconds.
- Shows completion status.

Brute Force Attack Execution:

- Create temporary password wordlist if needed.
- Attempts SSH login with multiple passwords.
- Runs for maximum 30 seconds.
- Reports success or completion

MITM Attack Execution:

- Enables IP forwarding.
- Run ARP spoofing for 15 seconds.
- Cleans up by disabling IP forwarding.
- Reports completion

```
[*] Target Selection:  
1) Choose specific IP from list  
2) Random target from discovered IPs  
[?] Select target method (1-2): 1  
[*] Available targets:  
1) 192.168.153.1  
2) 192.168.153.2  
3) 192.168.153.161  
4) 192.168.153.254  
[?] Choose target number: 3  
[+] Target selected: 192.168.153.161  
  
[*] Executing attack...  
[!] Launching DOS Attack on 192.168.153.161  
[*] Sending SYN flood packets...  
[!] DOS Attack failed  
[+] Attack logged to /var/log/attack log files.txt  
  
1) 192.168.153.1  
2) 192.168.153.2  
3) 192.168.153.161  
4) 192.168.153.254  
[?] Choose target number: 3  
[+] Target selected: 192.168.153.161  
  
[*] Executing attack...  
[!] Launching Brute Force Attack on 192.168.153.161  
[*] Attempting SSH password cracking...  
[!] Brute Force Attack completed (no valid credentials found)  
[+] Attack logged to /var/log/attack log files.txt
```

ATTACK LOGGING & RESULTS

Every attack executed by the system is automatically logged with comprehensive details for audit and training purposes.

Log File Structure

Location: /var/log/attack log files.txt

Each log entry contains:

- Timestamp (YYYY-MM-DD HH:MM: SS)
- Attack Type (DOS Attack, MITM Attack, or Brute Force Attack)
- Target IP address
- Network Interface used
- Status (SUCCESS or FAILED)

```
(kali㉿kali)-[~/Desktop/ PROJECT: CHECKER]
└─$ cat /var/log/attack\ log\ files.txt
[2025-11-10 02:51:48] Attack Type: Brute Force Attack | Target IP: 192.168.153.161 | Interface: eth0 | Status: SUCCESS
[2025-11-10 02:55:58] Attack Type: DOS Attack | Target IP: 192.168.153.161 | Interface: eth0 | Status: FAILED
└─$
```

Main Loop & Continuation

After each attack execution and logging, the system prompts:

Do you want to run another attack?

- 1) Yes – Run another attack
- 2) No – Exit

This allows SOC managers to run multiple attack simulations in a single session without rescanning the network, making training more efficient.

```
[?] Do you want to run another attack?
1) Yes - Run another attack
2) No - Exit
[?] Your choice (1-2): 2
[+] Thank you for using CHECKER SOC Tool!
[*] Logs saved to: /var/log/attack log files.txt

└─$ cat /var/log/attack\ log\ files.txt
[2025-11-10 02:51:48] Attack Type: Brute Force Attack | Target IP: 192.168.153.161 | Interface: eth0 | Status: SUCCESS
[2025-11-10 02:55:58] Attack Type: DOS Attack | Target IP: 192.168.153.161 | Interface: eth0 | Status: FAILED
└─$
```

CONCLUSION

This automated SOC attack simulation tool successfully demonstrates the capability to help SOC teams stay alert through controlled attack scenarios. The tool integrates multiple professional security testing tools and provides comprehensive logging for training and compliance purposes.

Project Achievements

- Successfully automated SOC attack simulation workflow
- Integrated multiple professional security tools (Nmap, Hping3, Arpspoof, Hydra)
- Implemented user-friendly interface with color-coded output.
- Created comprehensive logging system with timestamps.
- Demonstrated three effective attack types: DOS, MITM, and Brute Force
- Provided flexible target selection (specific or random)
- Enabled loop functionality for multiple training scenarios.