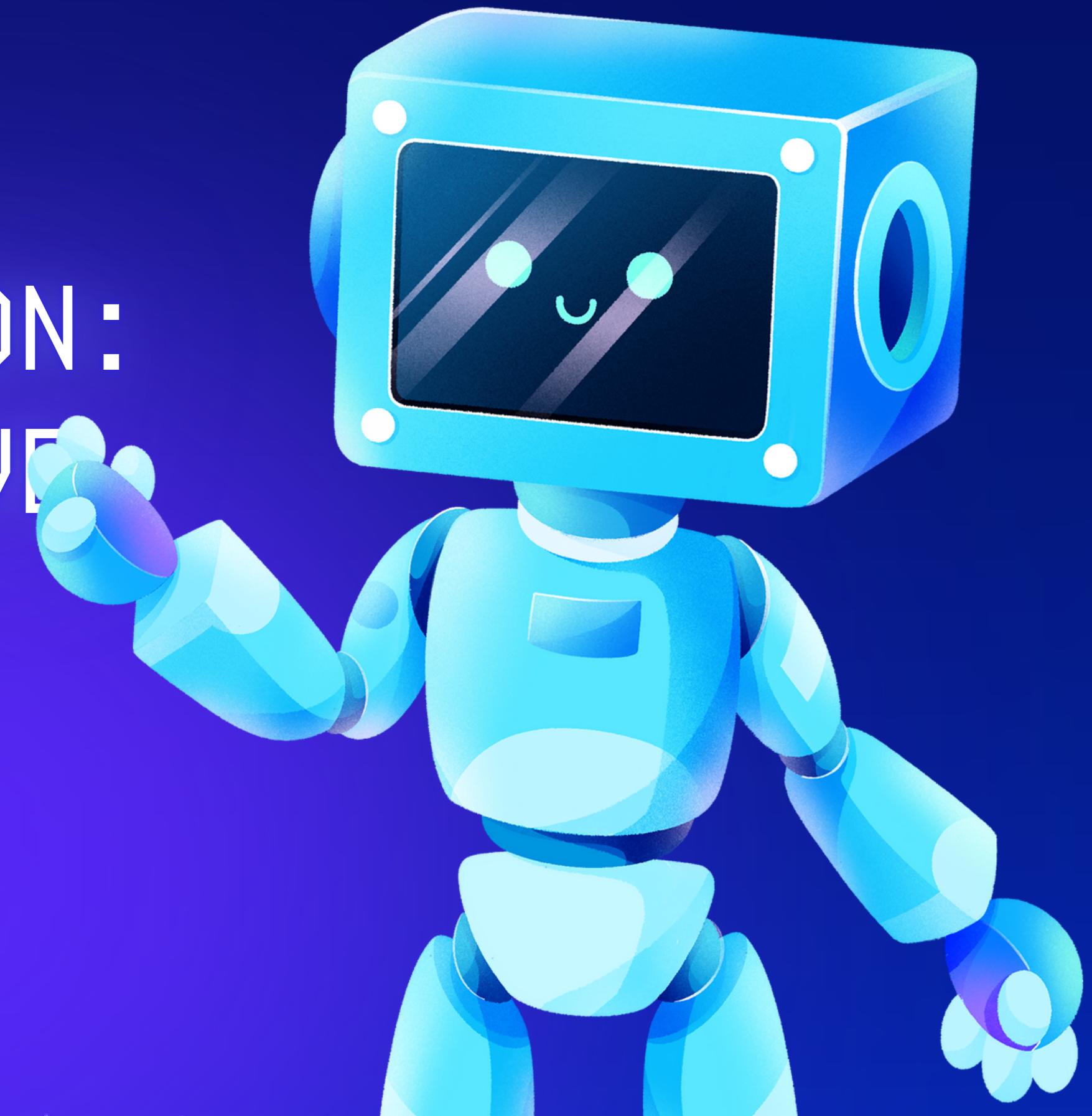


SECURITY OPERATION: AZIONI PREVENTIVE

Ernesto Robles



DISPOSITIVI COINVOLTI



Macchina Kali ip: 192.168.1.63

Macchina Windows- XP ip: 192.168.1.62



STRUMENTI UTILIZZATI

Nmap strumento open-source utilizzato per la scansione di reti e l'individuazione di dispositivi connessi a una rete, analisi delle porte e rilevazione di servizi in esecuzione su tali porte.

Sulla macchina Wind-XP è stato disabilitato il firewall, da Kali con l'uso di nmap viene effettuata una scansione volta ad individuare la versione del software sulla macchina Wind-XP.

Il risultato è la visualizzazione della versione del software sulla macchina target ovvero Wind-XP e alcuni dei servizi di questo.

```
(kali㉿kali)-[~]
└─$ nmap -Pn -sV 192.168.1.62
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 14:58 CET
Nmap scan report for 192.168.1.62
Host is up (0.00038s latency).

Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org
/submit/
Nmap done: 1 IP address (1 host up) scanned in 7.40 seconds
```

Sulla macchina Wind-XP è stato riabilitato il firewall, da Kali con l'uso di nmap viene effettuata una scansione volta ad individuare la versione del software sulla macchina Wind-XP.

Come risultato però non otteniamo la visualizzazione della versione del software sulla macchina target ovvero Wind-XP.

Il firewall blocca l'uso del protocollo ICMP e dunque del ping, ostacolo che si aggira usando una connessione 3 way hand shake. viene bloccata anche la rilevazione del software in attivo sulla macchina target, come illustrato qua vediamo che l'host è attivo ma non ne vediamo la versione software.

```
(kali㉿kali3)-[~]
└─$ nmap -sV 192.168.1.62
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 14:48 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds

(kali㉿kali3)-[~]
└─$ nmap -Pn -sV 192.168.1.62
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 14:49 CET
Nmap scan report for 192.168.1.62
Host is up.
All 1000 scanned ports on 192.168.1.62 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 203.22 seconds
```