Capstone Incident Response Report (SANS Template)

Incident Title: SMB Brute-Force Attempt on Windows 10
Date: [Add your date here]
Reported by: Abhishek Tiwary
Tools Involved: CrowdSec Agent, CrowdSec Bouncer, Windows Event Viewer
Severity Level: High

---

1. Executive Summary

An active **SMB brute-force attack** was detected on the Windows 10 virtual machine.
The attack originated from **Attacker IP: 10.178.124.51** and was successfully identified by the **CrowdSec Agent**.
Within seconds, the system automatically contained the threat by banning the attacker's IP using the CrowdSec Bouncer.
No system compromise occurred.

---

2. Timeline of Events

Time	Event Description
T0	**Metasploit SMB Brute-Force initiated** from Attacker VM (10.178.124.51).
T0 + 15s	**Windows Agent** detects multiple failed logins (Event ID 4625) and alerts the **CrowdSec LAPI**.
T0 + 30s	**CrowdSec Server** issues a **BAN decision** against attacker IP.
T0 + 45s	**Ping test from attacker VM fails**, confirming network-level containment.

---

3. Impact Analysis

- **Impact Level:** Low / Minimal
- No credentials were compromised.

- No lateral movement or privilege escalation observed.
- The **CrowdSec Bouncer** effectively prevented unauthorized access attempts.

---

4. Remediation Steps

1. **Containment:**
    - Attacker IP **10.178.124.51** was banned automatically by CrowdSec.
2. **Eradication:**
    - **Windows Event Logs** reviewed for failed logins and confirmation of defense action.
3. **Recovery:**
    - **Account Lockout Policy** reviewed and strengthened to mitigate future brute-force attempts.

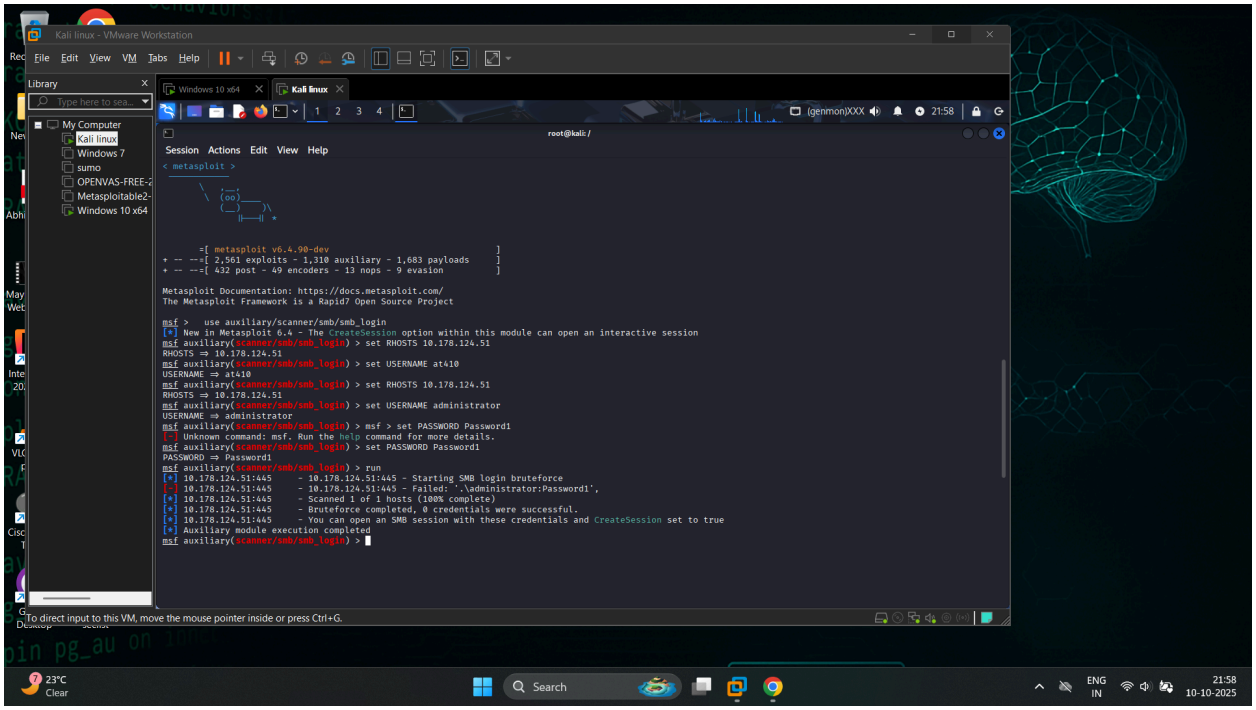
---

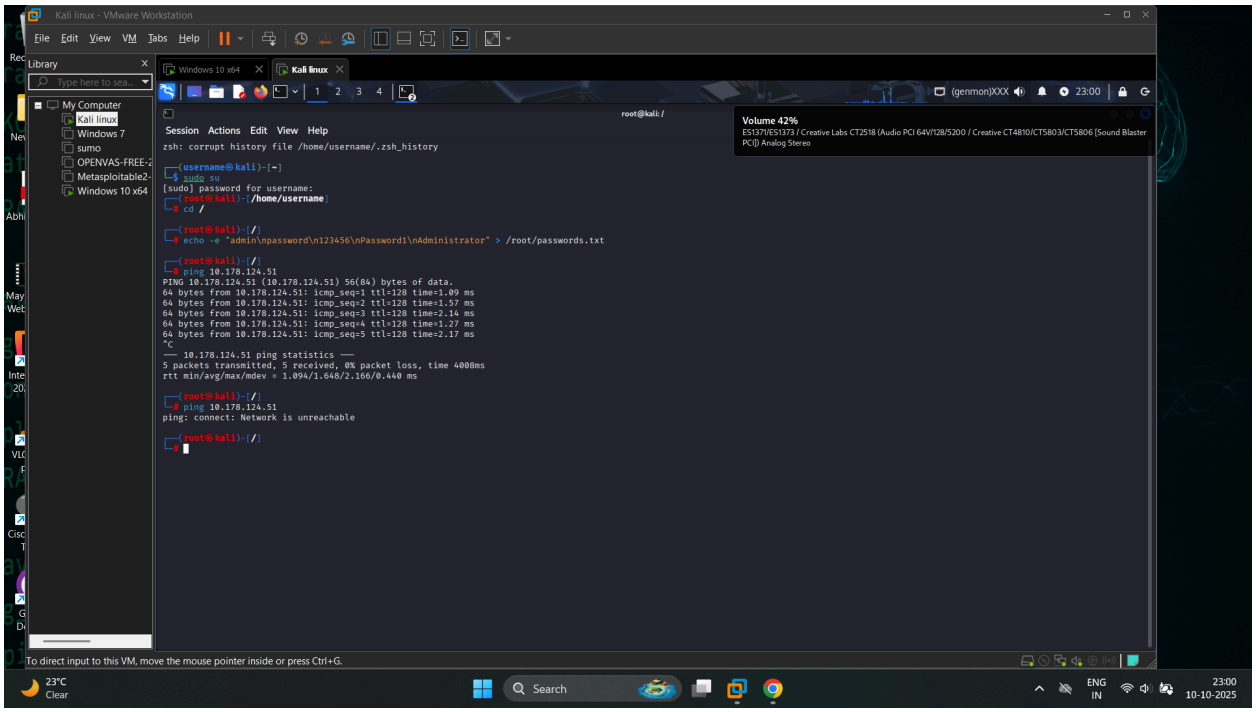
5. Lessons Learned

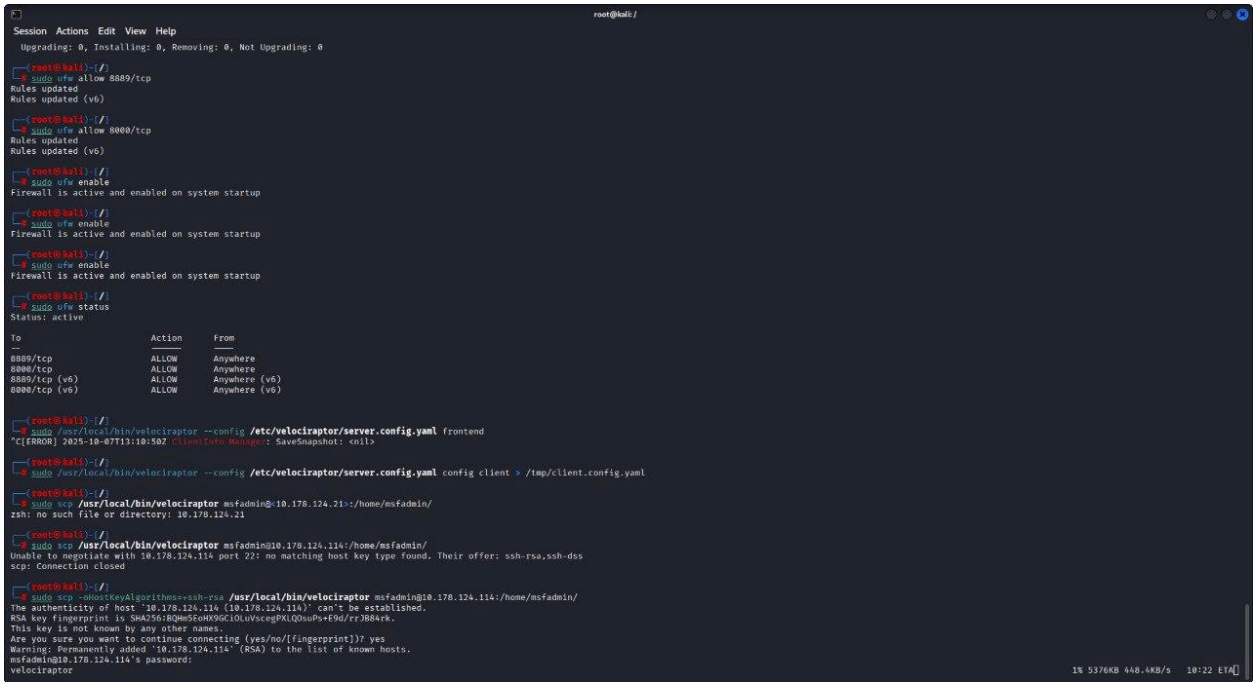
- Automated containment via **CrowdSec** proved highly effective.
- **Velociraptor forensic acquisition** failed due to kernel incompatibility, suggesting improved VM configuration and planning are needed.
- Future steps: automate log forwarding to **Wazuh** or **SIEM dashboard** for unified monitoring.

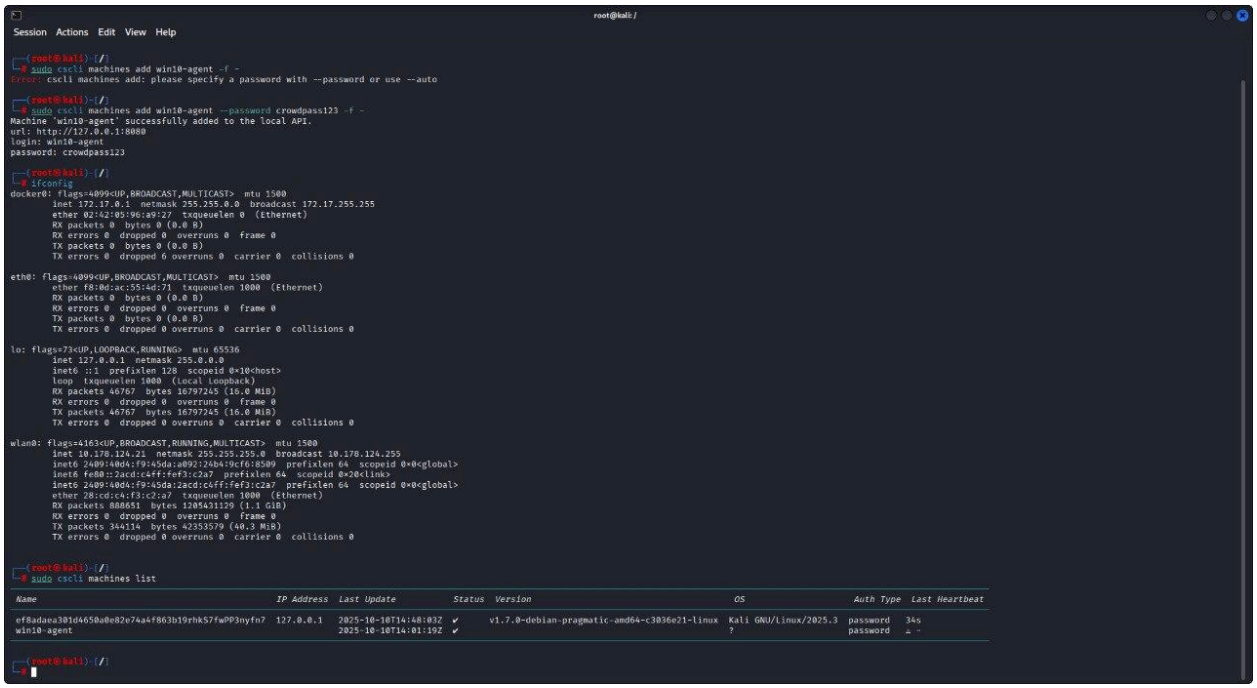
---

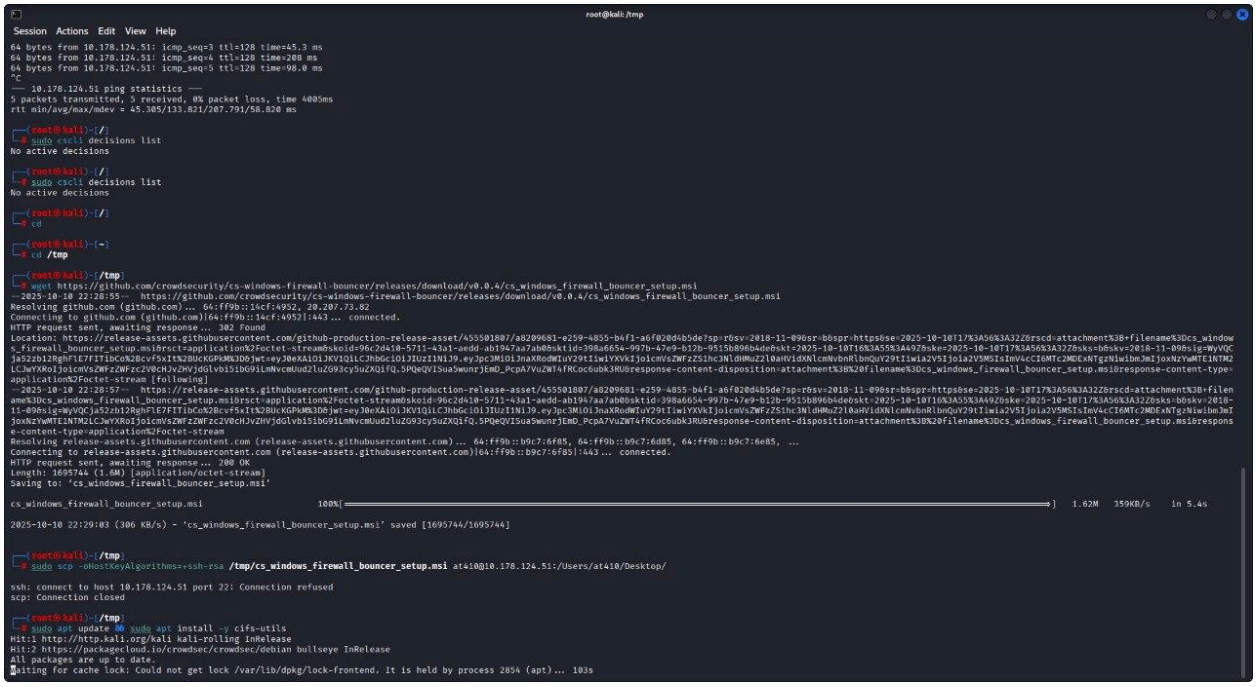
6. Supporting Evidence


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Kali linux
Windows 7
sumo
OPENVAS-FREE-2
Metasploitable2-
Windows 10 x64
Windows 10 x64
Kali linux
root@kali: /
Session Actions Edit View Help
< metasploit >
=[metasploit v6.4.90-dev]
+ -- --=[2,561 exploits - 1,310 auxiliary - 1,683 payloads]
+ -- --=[432 post - 49 encoders - 13 nops - 9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > use auxiliary/scanner/smb/smb_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf auxiliary(scanner/smb/smb_login) > set RHOSTS 10.178.124.51
RHOSTS => 10.178.124.51
msf auxiliary(scanner/smb/smb_login) > set USERNAME at410
USERNAME => at410
msf auxiliary(scanner/smb/smb_login) > set RHOSTS 10.178.124.51
RHOSTS => 10.178.124.51
msf auxiliary(scanner/smb/smb_login) > set USERNAME administrator
USERNAME => administrator
msf auxiliary(scanner/smb/smb_login) > msf > set PASSWORD Password1
[-] Unknown command: msf. Run the help command for more details.
msf auxiliary(scanner/smb/smb_login) > set PASSWORD Password1
PASSWORD => Password1
msf auxiliary(scanner/smb/smb_login) > run
[*] 10.178.124.51:445 - 10.178.124.51:445 - Starting SMB login bruteforce
[-] 10.178.124.51:445 - 10.178.124.51:445 - Failed: '.\administrator:Password1',
[*] 10.178.124.51:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.178.124.51:445 - Bruteforce completed, 0 credentials were successful.
[*] 10.178.124.51:445 - You can open an SMB session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_login) >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
23°C
Clear
Search
ENG
IN
21:58
10-10-2025


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Kali linux
Windows 7
sumo
OPENVAS-FREE-2
Metasploitable2-
Windows 10 x64
Windows 10 x64
Kali linux
root@kali: /
Session Actions Edit View Help
zsh: corrupt history file /home/username/.zsh_history
(username㉿kali)-[~]
$ sudo su
[sudo] password for username:
(root㉿kali)-[/home/username]
cd /
(root㉿kali)-[/]
echo -e "admin\npassword\n123456\nPassword1\nAdministrator" > /root/passwords.txt
(root㉿kali)-[/]
ping 10.178.124.51
PING 10.178.124.51 (10.178.124.51) 56(84) bytes of data.
64 bytes from 10.178.124.51: icmp_seq=1 ttl=128 time=1.09 ms
64 bytes from 10.178.124.51: icmp_seq=2 ttl=128 time=1.57 ms
64 bytes from 10.178.124.51: icmp_seq=3 ttl=128 time=2.14 ms
64 bytes from 10.178.124.51: icmp_seq=4 ttl=128 time=1.27 ms
64 bytes from 10.178.124.51: icmp_seq=5 ttl=128 time=2.17 ms
^C
— 10.178.124.51 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 1.094/1.648/2.166/0.440 ms
(root㉿kali)-[/]
ping 10.178.124.51
ping: connect: Network is unreachable
(root㉿kali)-[/]
#
Volume 42%
ES1371/ES1373 / Creative Labs CT2518 (Audio PCI 64V/128/5200 / Creative CT4810/CT5803/CT5806 [Sound Blaster PCI]) Analog Stereo
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
23°C
Clear
Search
ENG
IN
23:00
10-10-2025


root@kali: /
Session Actions Edit View Help
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
sudo ufw allow 8889/tcp
Rules updated
Rules updated (v6)
sudo ufw allow 8000/tcp
Rules updated
Rules updated (v6)
sudo ufw enable
Firewall is active and enabled on system startup
sudo ufw enable
Firewall is active and enabled on system startup
sudo ufw enable
Firewall is active and enabled on system startup
sudo ufw status
Status: active
To Action From
-- ------ ----
8889/tcp ALLOW Anywhere
8000/tcp ALLOW Anywhere
8889/tcp (v6) ALLOW Anywhere (v6)
8000/tcp (v6) ALLOW Anywhere (v6)
sudo /usr/local/bin/velociraptor --config /etc/velociraptor/server.config.yaml frontend
^C[ERROR] 2025-10-07T13:10:50Z ClientInfo Manager: SaveSnapshot: <nil>
sudo /usr/local/bin/velociraptor --config /etc/velociraptor/server.config.yaml config client > /tmp/client.config.yaml
sudo scp /usr/local/bin/velociraptor msfadmin@<10.178.124.21>:/home/msfadmin/
zsh: no such file or directory: 10.178.124.21
sudo scp /usr/local/bin/velociraptor msfadmin@10.178.124.114:/home/msfadmin/
Unable to negotiate with 10.178.124.114 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
scp: Connection closed
sudo scp -oHostKeyAlgorithms=+ssh-rsa /usr/local/bin/velociraptor msfadmin@10.178.124.114:/home/msfadmin/
The authenticity of host '10.178.124.114 (10.178.124.114)' can't be established.
RSA key fingerprint is SHA256:RQHm5ExHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB8Ark.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.178.124.114' (RSA) to the list of known hosts.
msfadmin@10.178.124.114's password:
velociraptor
1% 5376KB 448.4KB/s 10:22 ETA


root@kali: /
Session Actions Edit View Help
sudo cscli machines add win10-agent -f -
Error: cscli machines add: please specify a password with --password or use --auto
sudo cscli machines add win10-agent --password crowdpass123 -f -
Machine 'win10-agent' successfully added to the local API.
url: http://127.0.0.1:8080
login: win10-agent
password: crowdpass123
ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
ether 02:42:05:96:a9:27 txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 6 overruns 0 carrier 0 collisions 0
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether f8:0d:ac:55:4d:71 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 46767 bytes 16797245 (16.0 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 46767 bytes 16797245 (16.0 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.178.124.21 netmask 255.255.255.0 broadcast 10.178.124.255
inet6 2409:40d4:f9:45da:a092:24b4:9cf6:8509 prefixlen 64 scopeid 0×0<global>
inet6 fe80::2acd:c4ff:fef3:c2a7 prefixlen 64 scopeid 0×20<link>
inet6 2409:40d4:f9:45da:2acd:c4ff:fef3:c2a7 prefixlen 64 scopeid 0×0<global>
ether 28:cd:c4:f3:c2:a7 txqueuelen 1000 (Ethernet)
RX packets 888651 bytes 1205431129 (1.1 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 344114 bytes 42353579 (40.3 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
sudo cscli machines list
Name IP Address Last Update Status Version OS Auth Type Last Heartbeat
ef8adaea301d465a0e82e74a4f863b19rhkS7fwPP3nyfn7 127.0.0.1 2025-10-10T14:48:03Z ✔ v1.7.0-debian-pragmatic-amd64-c3036e21-linux Kali GNU/Linux/2025.3 password 34s
win10-agent 2025-10-10T14:01:19Z ✔ ? password -


root@kali: /tmp
Session Actions Edit View Help
64 bytes from 10.178.124.51: icmp_seq=3 ttl=128 time=45.3 ms
64 bytes from 10.178.124.51: icmp_seq=4 ttl=128 time=208 ms
64 bytes from 10.178.124.51: icmp_seq=5 ttl=128 time=98.0 ms
^C
--- 10.178.124.51 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 45.305/133.821/207.791/58.820 ms
┌──(root㉿kali)-[/]
└─# sudo cscli decisions list
No active decisions
┌──(root㉿kali)-[/]
└─# sudo cscli decisions list
No active decisions
┌──(root㉿kali)-[/]
└─# cd
┌──(root㉿kali)-[~]
└─# cd /tmp
┌──(root㉿kali)-[/tmp]
└─# wget https://github.com/crowdsecurity/cs-windows-firewall-bouncer/releases/download/v0.0.4/cs_windows_firewall_bouncer_setup.msi
--2025-10-10 22:28:55-- https://github.com/crowdsecurity/cs-windows-firewall-bouncer/releases/download/v0.0.4/cs_windows_firewall_bouncer_setup.msi
Resolving github.com (github.com) ... 64:ff9b::14cf:4952, 20.207.73.82
Connecting to github.com (github.com)|64:ff9b::14cf:4952|:443 ... connected.
HTTP request sent, awaiting response ... 302 Found
Location: https://release-assets.githubusercontent.com/github-production-release-asset/455501807/a8209681-e259-4855-b4f1-a6f020d4b5de?sp=r&sv=2018-11-09&sr=b&spr=https&se=2025-10-10T17%3A56%3A32Z&rscd=attachment%3B+filename%3Dcs_windows_firewall_bouncer_setup.msi&rsct=application%2Foctet-stream&skoid=96c2d410-5711-43a1-aedd-ab1947aa7ab0&sktid=398a6654-997b-47e9-b12b-9515b896b4de&skt=2025-10-10T16%3A55%3A49Z&ske=2025-10-10T17%3A56%3A32Z&sks=b&skv=2018-11-09&sig=WyVQCja52zb12RghFlE7fITibCoX%2Bcvf5xIt%2BUcKGPkM%3D&jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmVsZWFzZS1hc3NldHMuZ2l0aHVidXNlcmNvbnRlbnQuY29tIiwia2V5IjoiaZV5MSIsInV4cCI6MTc2MDExNTgzNiwibmJmIjoxNzYwMTE1NTM2LCJwYXRoIjoicmVsZWFzZWFzc2V0cHJvZHVjdGlvbi1ib1bG91LmNvcmUud2luZG93cy5uZXQifQ.5PQeQVI5ua5wunrjEmD_PcpA7VuZWT4fRCoc6ubk3RU&response-content-disposition=attachment%3B%20filename%3Dcs_windows_firewall_bouncer_setup.msi&response-content-type=application%2Foctet-stream [following]
--2025-10-10 22:28:57-- https://release-assets.githubusercontent.com/github-production-release-asset/455501807/a8209681-e259-4855-b4f1-a6f020d4b5de?sp=r&sv=2018-11-09&sr=b&spr=https&se=2025-10-10T17%3A56%3A32Z&rscd=attachment%3B+filename%3Dcs_windows_firewall_bouncer_setup.msi&rsct=application%2Foctet-stream&skoid=96c2d410-5711-43a1-aedd-ab1947aa7ab0&sktid=398a6654-997b-47e9-b12b-9515b896b4de&skt=2025-10-10T16%3A55%3A49Z&ske=2025-10-10T17%3A56%3A32Z&sks=b&skv=2018-11-09&sig=WyVQCja52zb12RghFlE7fITibCoX%2Bcvf5xIt%2BUcKGPkM%3D&jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmVsZWFzZS1hc3NldHMuZ2l0aHVidXNlcmNvbnRlbnQuY29tIiwia2V5IjoiaZV5MSIsInV4cCI6MTc2MDExNTgzNiwibmJmIjoxNzYwMTE1NTM2LCJwYXRoIjoicmVsZWFzZWFzc2V0cHJvZHVjdGlvbi1iOTFiMDU1LmNvcmUud2luZG93cy5uZXQifQ.5PQeQVI5ua5wunrjEmD_PcpA7VuZWT4fRCoc6ubk3RU&response-content-disposition=attachment%3B%20filename%3Dcs_windows_firewall_bouncer_setup.msi&response-content-type=application%2Foctet-stream
Resolving release-assets.githubusercontent.com (release-assets.githubusercontent.com) ... 64:ff9b::b9c7:6f85, 64:ff9b::b9c7:6d85, 64:ff9b::b9c7:6e85, ...
Connecting to release-assets.githubusercontent.com (release-assets.githubusercontent.com)|64:ff9b::b9c7:6f85|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 1695744 (1.6M) [application/octet-stream]
Saving to: 'cs_windows_firewall_bouncer_setup.msi'
cs_windows_firewall_bouncer_setup.msi 100%[==========>] 1.62M 359KB/s in 5.4s
2025-10-10 22:29:03 (306 KB/s) - 'cs_windows_firewall_bouncer_setup.msi' saved [1695744/1695744]
┌──(root㉿kali)-[/tmp]
└─# sudo scp -oHostKeyAlgorithms=+ssh-rsa /tmp/cs_windows_firewall_bouncer_setup.msi at410@10.178.124.51:/Users/at410/Desktop/
ssh: connect to host 10.178.124.51 port 22: Connection refused
scp: Connection closed
┌──(root㉿kali)-[/tmp]
└─# sudo apt update && sudo apt install -y cifs-utils
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Hit:2 https://packagecloud.io/crowdsec/crowdsec/debian bullseye InRelease
All packages are up to date.
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by process 2854 (apt)... 103s