IKEv1 Certificate Authentication Bypass Hunting Guide

Purpose

This guide provides recommended log-hunting steps to help identify potential IKEv1 certificate authentication bypass activity in Check Point environments.

Review **Check Point SmartConsole** logs for VPN and IKEv1-related events associated with known attacker infrastructure, suspicious certificate subject names, and possible post-exploitation activity.

SmartConsole supports custom log searches from **Logs & Monitor** / **Logs & Events**.

The guide also includes recommendations for identifying post-exploitation activity that may occur after a successful certificate authentication bypass, including internal reconnaissance, service probing, and lateral-movement preparation.

Recommended Search Period

Search at least in the following period: 2026-05-07 through 2026-06-08

Detection Steps

1. Hunt for Known Attacker IP Addresses

In **SmartConsole**, go to **Logs & Monitor** / **Logs & Events**, and search for events where either the source IP or destination IP matches one of the known attacker IP addresses.

These IP addresses may appear during the exploitation stage and may also appear in post-exploitation activity, including communication with malware-hosting infrastructure.

Attacker IP Addresses

45.77.149[.]152

209.182.225[.]136

38.60.157[.]139

162.33.177[.]101

45.76.26[.]42

144.208.127[.]155

38.54.88[.]201

38.54.107[.]167

66.42.99[.]200

45.63.104.106

45.61.136.173

SmartConsole Query

Use this query to search for any log where one of the attacker IP addresses appears as either the source or destination:

(src:45.77.149.152 OR dst:45.77.149.152 OR src:209.182.225.136 OR dst:209.182.225.136 OR src:38.60.157.139 OR dst:38.60.157.139 OR src:162.33.177.101 OR dst:162.33.177.101 OR src:45.76.26.42 OR dst:45.76.26.42 OR src:144.208.127.155 OR dst:144.208.127.155 OR src:38.54.88.201 OR dst:38.54.88.201 OR src:38.54.107.167 OR dst:38.54.107.167 OR src:66.42.99.200 OR dst:66.42.99.200 OR dst:45.63.104.106 OR dst:45.61.136.173)

2. Hunt for VPN / IKEv1 Activity

After identifying logs that match the attacker IP address list, focus the investigation on VPN and IKEv1-related events.

Pay special attention to events with the **action:"Key Install"**

A successful exploit requires a ‘Quick Mode completion’ key install event.

Focused Key Install Query

Use this query to identify ‘Key Install’ events involving one of the known attacker IP addresses:

action:"Key Install" AND (src:45.77.149.152 OR dst:45.77.149.152 OR src:209.182.225.136 OR dst:209.182.225.136 OR src:38.60.157.139 OR dst:38.60.157.139 OR src:162.33.177.101 OR dst:162.33.177.101 OR src:45.76.26.42 OR dst:45.76.26.42 OR src:144.208.127.155 OR dst:144.208.127.155 OR src:38.54.88.201 OR dst:38.54.88.201 OR dst:38.54.107.167 OR dst:66.42.99.200 OR dst:45.63.104.106 OR dst:45.61.136.173)

3. Hunt for Quick Mode Completion Events

Use this query to identify IKEv1 ‘Key Install’ events where the log record contains **‘Quick Mode completion’** and one of the known attacker IP addresses appears as either the source or destination.

Quick Mode Completion / IKEv1 Query

action:"Key Install" AND "Quick Mode completion" AND (src:45.77.149.152 OR dst:45.77.149.152 OR src:209.182.225.136 OR dst:209.182.225.136 OR src:38.60.157.139 OR dst:38.60.157.139 OR src:162.33.177.101 OR dst:162.33.177.101 OR src:45.76.26.42 OR dst:45.76.26.42 OR src:144.208.127.155 OR dst:144.208.127.155 OR src:38.54.88.201 OR dst:38.54.88.201 OR dst:38.54.107.167 OR dst:66.42.99.200 OR dst:45.63.104.106 OR dst:45.61.136.173)

Events matching this query should be prioritized for investigation.

4. Monitor for Suspicious User Certificate Authentication

In addition to monitoring the attacker IP addresses, you should also monitor for **“Key Install”** events with **“Quick Mode completion”** where the user certificate contains suspicious certificate subject strings.

The following subject strings have been observed and should be reviewed:

CN=Default

CN=DefautI

CN=usertest

Note: The value `CN=Defautl` is intentionally included as written.

Recommended SmartConsole Query

Use this query to search for ‘Key Install’ events with ‘Quick Mode completion’ where the user certificate contains one of the suspicious certificate subject strings:

action:"Key Install" AND "Quick Mode completion" AND ("CN=Default" OR "CN=Defautl" OR "CN=usertest")

5. Recommended Combined Query

Use this combined query to identify events that match all these conditions:

- The action is “Key Install”
- The log record contains “Quick Mode completion”
- The user certificate contains one of the suspicious certificate subject strings
- One of the known attacker IP addresses appears as either the source or destination

action:"Key Install" AND "Quick Mode completion" AND ("CN=Default" OR "CN=Defautl" OR "CN=usertest") AND (src:45.77.149.152 OR dst:45.77.149.152 OR src:209.182.225.136 OR dst:209.182.225.136 OR src:38.60.157.139 OR dst:38.60.157.139 OR src:162.33.177.101 OR dst:162.33.177.101 OR src:45.76.26.42 OR dst:45.76.26.42 OR src:144.208.127.155 OR dst:144.208.127.155 OR src:38.54.88.201 OR dst:38.54.88.201 OR src:38.54.107.167 OR dst:38.54.107.167 OR src:66.42.99.200 OR dst:66.42.99.200 OR dst:45.63.104.106 OR dst:45.61.136.173)

Investigation Guidance

Any event matching the following conditions should be prioritized for investigation:

- action:"Key Install"
- The log record contains "Quick Mode completion"
- The user certificate contains one of the suspicious certificate subject strings:
  - CN=Default
  - CN=Defautl
  - CN=usertest

These events should be reviewed even if the source or destination IP address does not match the known attacker IP IOC list.

Recommended Action

If matching events are identified, investigate the activity as potentially suspicious and review related VPN, IKEv1, and certificate authentication logs for the affected Security Gateway.

Also, validate whether the observed certificate subject names are expected in their environment. If they are not expected, the events should be treated as a higher priority for investigation.

Possible Post-Exploitation Activity to Review

Observed post-exploitation activity may include broad service probing and internal reconnaissance across multiple services and ports, including **SSH, LDAP, Kerberos, SMB, MS-RPC Endpoint Mapper, MS-SQL, and Telnet**.

This activity consists of discovery and lateral-movement preparation behavior, including network service discovery, Active Directory reconnaissance, file share discovery, and attempts to identify remotely accessible administrative services.

Recommended action

Review firewall, VPN, endpoint, Active Directory, and server logs for unusual connection attempts, authentication attempts, or successful sessions to the following services and ports:

22, 23, 88, 135, 389, 445, 1433

Review unusual user activity occurring around the same timeframe as the suspicious VPN / IKEv1 events or service-probing activity. This may include authentication outside normal working hours, access to atypical internal systems, repeated authentication attempts, or user activity that coincides with internal reconnaissance and lateral-movement indicators.

MITRE ATT&CK

Observed activity	Port(s)	MITRE ATT&CK mapping	Tactic
SSH brute-force or enumeration	22	T1046 - Network Service Discovery T1110 / T1110.001 - Brute Force / Password Guessing T1021.004 - Remote Services: SSH	Discovery / Credential Access / Lateral Movement
LDAP / Active Directory reconnaissance	389	T1087.002 - Account Discovery: Domain Account T1069.002 - Permission Groups Discovery: Domain Groups	Discovery
Kerberos service probing / abnormal ticket activity	88	T1558.003 - Steal or Forge Kerberos Tickets: Kerberoasting	Credential Access
SMB / file share probing	445	T1135 - Network Share Discovery T1021.002 - Remote Services: SMB/Windows Admin Shares	Discovery / Lateral Movement
MS-RPC Endpoint Mapper probing	135	T1046 - Network Service Discovery T1021.002 - Remote Services: SMB/Windows Admin Shares	Discovery / Lateral Movement
Telnet probing / possible credential guessing	23	T1046 - Network Service Discovery T1110 / T1110.001 - Brute Force / Password Guessing T1021 - Remote Services	Discovery / Credential Access / Lateral Movement