

Tesi Magistrale

Analisi dei Covert Channel applicati al protocollo ICMP

*Franceso Santini
Marco Mecarelli*

Università degli Studi di Perugia
25 aprile 2025

Indice

Parte 1 - Introduzione	4
1 Covert Channel	4
1.1 Cos'è un Covert Cahnnel?	4
1.2 Principali categorie di Covert Channel	4
1.2.1 Covert Channel Timing (temporizzazione)	5
1.2.2 Covert Channel Storage (Archiviazione)	5
1.2.3 Covert Channel Behavioral (Comportamentali)	5
1.3 Struttura/Caratteristiche dei Covert Channel	5
1.4 Vulnerabilità Utilizzate	8
1.5 Tipologie di attacchi Covert Channel	9
1.6 Strumenti di Mitigazione e Protezione	12
2 Protocollo ICMP	16
2.1 Possibili attacchi tramite ICMP	20
2.2 Buona practice di sicurezza	23
3 Riepilogo attacchi ICMP Covert Channel	25
3.1 Attacchi Covert Channel ICMP	26
3.2 Strategie di rilevamento	28
3.3 Strategie di mitigazione	29
4 Strumenti Utilizzati	31

Listings

shell	29
bash	30

Elenco delle figure

Parte 1 - Introduzione

1 Covert Channel

1.1 Cos'è un Covert Cahnnel?

Un **Covert Channel** è un attacco che permette (in ambienti ritenuti sicuri) la capacità di comunicare/trasferire dati, in maniera non autorizzata e non voluta, fra processi/entità comunicanti spesso senza essere rivelati e spesso evitando (se non violando) le normali politiche di sicurezza.

Solitamente operano al di fuori dei soliti meccanismi di comunicazioni sfruttando vulnerabilità o comportamenti non previsti nei sistemi. Quindi non usando i normali protocolli/canali di comunicazione (es network sockets, emails) non generano segnali di un uso improprio del sistema. Ciò li rende difficili da rilevare usando i tipici strumenti di monitoraggio.

In un Covert Channel, qualsiasi risorsa condivisa può essere utilizzata come canale nascosto e per questo possono esistere in qualunque sistema (che abbia delle risorse condivise). Lo sfruttamento di queste risorse porta alla fuita (o scambio) dei dati.

L'attacco è un problema siccome sono estremamente difficili da identificare e controllare. La loro esistenza spesso rimane non notata dagli amministratori (di sistema) siccome si nascondono all'interno dei normali processi del sistema. Sono inoltre un problema significativo in tutti quegli ambienti altamente sicuri (es ambienti militari, governativi,...) dove una fuita di informazioni può avere conseguenze gravi.

1.2 Principali categorie di Covert Channel

Le principali categorie di canali nascosti sono:

- Covert Channel Timing (Temporizzazione):
coinvolgono la scrittura di dati a un'area di memoria condivisa in cui entrambi i processi possono accedere

Esempio 1.1. *Modificare i permessi dei file o i metadati per codificare informazioni. Oppure modificare variabili condivise o buffer*

- Covert Channel Storage (Archiviazione):
manipolano la temporalizzazione o l'ordine di eventi per codificare informazioni.

Esempio 1.2. *Variare deliberatamente il tempo fra delle azioni (es trasmmissione di network packet, patter di uso della CPU) oppure codificando dati nella temporalizzazione dell'esecuzione dei processi o delay di risposta.*

1.2.1 Covert Channel Timing (temporizzazione)

I covert channel di temporizzazione sono metodi di comunicazione che permettono ad un osservatore (umano o processo) di acquisire informazioni attraverso il cambiamento nel tempo di risposta di una risorsa. Essenzialmente qualsiasi metodo che utilizza un orologio o una misurazione del tempo per segnalare il valore inviato sul canale. Video Esempio

1.2.2 Covert Channel Storage (Archiviazione)

Nei covert channel di archiviazione un processo scrive su una risorsa condivisa, mentre un altro processo legge da essa. I canali di archiviazione possono essere utilizzati tra processi all'interno di un singolo computer o tra più computer in una rete.

I veicoli dell'attacco sono tutte quelle risorse che consentono la scrittura, diretta o indiretta, di una risorsa da parte di un processo e la sua lettura, diretta o indiretta, da parte di un altro.

Esempio 1.3. *Un esempio di canale di archiviazione è la condivisione di un file. Supponiamo che l'utente A con privilegi di autorizzazione elevati voglia trasmettere in segreto, dati riservati all'utente B con un livello di sicurezza inferiore. Per farlo, utilizzerà un file word apparentemente contenente informazioni non classificate, dove invece occulterà l'informazione riservata.*

1.2.3 Covert Channel Behavioral (Comportamentali)

I canali nascosti comportamentali operano trasmettendo dati in base all'assegnazione di diversi eventi di processi, sistemi e applicazioni, generalmente suddividendo e trasmettendo i dati in pacchetti più piccoli.

1.3 Struttura/Caratteristiche dei Covert Channel

Tipicamente è costituito da due principali componenti:

- **Mittente** (Covert Transmitter): è l'entità che codifica e trasmette le informazioni nascoste usando una risorsa di sistema condivisa.

- **Destinatario** (Covert Listener): è l'entità che rileva e decifra l'informazione segreta dalla risorsa condivisa.

Come funzionano i Covert Channel?

Si opera cifrando dati nascosti nei comportamenti del sistema che i controlli di sicurezza tipicamente non monitorano così da permettere la comunicazione segreta fra due entità.

Le informazioni vengono inserite sfruttano gli effetti collaterali delle normali operazione del sistema senza un esplicito intento di comunicare.

- **Meccanismi di Codifica:**

Il mittente manipola una risorsa di sistema condivisa (osservabile dal destinatario) per codificare i dati segreti.

Tecniche comuni:

- Codifica basata sul Tempo: usa degli intervalli di tempo (e.g. ritardi fra i pacchetti di rete)
- Codifica basata sulla Memoria: modifica degli attributi del file, i bit di memoria oppure gli stati della cache
- Abuso del Protocollo: alterazione dei flag TCP, dei numeri di sequenza oppure dei bit inutilizzati nelle intestazione dei pacchetti

- **Meccanismo di comunicazione:**

il mittente modifica continuamente i comportamenti del sistema per trasmettere bit di informazione. Questo può essere fatto introducendo ritardi, cambiando il carico di lavoro della CPU, o modificando gli stati della memoria in maniera controllata.

- **Meccanismi di Decodifica:**

il destinatario monitora la risorsa condivisa per rilevare, ricostruire e decifrare i dati trasmessi.

Esempio 1.4.

Misurazione delle variazioni del tempo di esecuzione per dedurre i dati segreti.

- **Sincronizzazione e Correzione degli Errori:**

il mittente e il destinatario devono sincronizzarsi (e.g. utilizzando segnali di temporizzazione pre-concordati). I meccanismi di rilevamento degli errori (come bit di parità o checksum) garantiscono un recupero accurato dei dati.

Esempio 1.5. Esempio di un Covert channel in una rete

Mittente: modifica il campo TTL (time-to-live) nei pacchetti IP per rappresentare dati binari (e.g. TTL=65→bit 1, TTL=128→bit 0)

Destinatario: osserva i valori TTL dei pacchetti in arrivo per ricostruire il messaggio nascosto

Caratteristiche Chiave dei covert Channel

Le principali caratteristiche di un Covert Channel sono:

- **Stealthiness** (furtività):

si devono poter aggirare i controlli in maniera nascosta

- **Bandwidth** (capacità di trasmissione):

la capacità di trasmissione dei dati che è generalmente bassa in termini di dati/tempo (throughput). Un eccessivo carico di informazioni, potrebbe rendere anomalo il funzionamento di quelle risorse o delle normali strutture dati. Nei canali nascosti generalmente il throughput è inversamente correlato alla segretezza di un canale.

Più dati un canale trasmette in un determinato periodo di tempo, maggiore è il rischio che il canale venga scoperto

- **Indistinguishability** (Indistinguibilità):

di solito si sfruttano servizi e/o risorse già presenti e quindi non sospette.

Uno dei maggiori problemi nell'implementazione di un canale nascosto è il “rumore” (es. sfruttando eccessivamente le risorse alterando e/o danneggiando il corretto funzionamento delle stesse) che potrebbe attirare l'attenzione da parte degli amministratori di sistema. La necessità è quella di riuscire a trasmettere attraverso un canale nascosto mantenendo conforme e inalterato il funzionamento della risorsa utilizzata così da rendersi “indistinguibili” dalla risorsa autorizzata e quindi invisibili ai sistemi di monitoraggio.

Ulteriori caratteristiche sono:

- **Uso involontario delle risorse:**

i Covert channels sfruttano le risorse del sistema (e.g memoria condivisa, uso della CPU, attributi dei file) in maniere che non fossero previste per la comunicazione.

- **Comunicazione nascosta:**

sono progettati per evitare la rilevazione; il canale è incorporato operazioni di sistema legittime per poter mascherare la trasmissione dei dati. (e.g

carico della CPU, accesso alla memoria, traffico della rete, metadati del file systema).

- **Violazione delle politiche di sicurezza:**

permettono lo scambio non autorizzato di informazioni, potenzialmente violando i requisiti di confidenzialità, di integrità o quelli di disponibilità.

1.4 Vulnerabilità Utilizzate

I Covert Channel sfruttano le vulnerabilità nel design del sistema, nelle politiche di sicurezza e nei protocolli di comunicazione per trasferire informazioni segretamente. Sfruttando queste vulnerabilità, gli attaccanti possono stabilire Covert Channel che evitano il controllo degli standard sicurezza, permettendo esfiltrazione non autorizzata di dati o comunicazione fra processi interni (inter-process communication).

La loro mitigazione richiede controllo degli accessi, randomizzazione dei tempi, iniezione di rumore e una sicurezza hardware migliore.

Principali Vulnerabilità usate dai Covert Channel

Sfruttamento delle risorse condivise

- **Scheduling della CPU:** l'attaccante può modulare l'uso della CPU per diffondere informazioni.
- **Memoria Cache:** gli attacchi side-channel alla cache sfruttano le differenze nei tempi di accesso per dedurre i dati.
- **Accesso al File System:** i processi possono dedurre informazioni in base ai lock dei file, timestamp o sull'attività del disco

Vulnerabilità basate sulla temporizzazione

- **Variabilità del tempo di risposta:**
l'attaccante misura i tempi di risposta del sistema per estrarre segreti.
- **Ritardi nell'esecuzione delle istruzioni:**
le differenze del tempo di esecuzione tra le operazioni privilegiate e non possono causare la fuoriuscita di dati.
- **Tempistica dei pacchetti:**
le informazioni possono essere codificate negli intervalli durante la trasmissione dei pacchetti

- **Manipolazione delle intestazioni:**
campi come TTL, sequenza dei numeri o bit non utilizzati possono essere utilizzati per codificare i dati
- **Pattern del traffico:**
le variazioni nel flusso del traffico (es burst size) si possono comportare come un Covert Channel.

Manipolazione della Memoria e dello Stato della CPU

- **Previsione delle ramificazioni ed esecuzione speculativa:**
sfruttato in attacchi come Spectre e Meltdown
- **Analisi del consumo energetico:**
i canali secondari possono rilevare chiavi crittografiche

Falle nel sistema operativo e nella Virtualizzazione

- **Abuso della comunicazione fra processi (Inter-Process Communication IPC):**
i processi possono ricavare i dati tramite la memoria condivisa o il passaggio di messaggi
- **Debolezze dell'hypervisor:**
le macchine virtuali possono far trapelare informazioni tra le guest instances

Vulnerabilità Hardware

- **Emissioni elettromagnetiche:**
dati sensibili possono essere divulgati tramite dei segnali EM (attacco TEMPEST) Sensitive data can be leaked via EM signals (TEMPEST attacks).
- **Canali laterali acustici:**
è possibile analizzare i suoni/rumori della tastiera, le variazioni della velocità della ventola o il rumore dell'alimentatore.

1.5 Tipologie di attacchi Covert Channel

I Covert Channel sono spesso applicati in:

- **Malware and Spionaggio:** usati per esfiltrare dati sensibili.

- **Test di sicurezza:** identificare e mitigare i Covert Channel è una parte fondamentale nel stabilire la sicurezza del sistema.
- **Ricerca:** esplorare i Covert Channel aiuta a capire potenziali vulnerabilità in sistemi complessi.

Gli attacchi tramite Covert Channel sfruttano le debolezze, del timing del sistema, delle risorse condivise e dei protocolli di rete, per trasmettere dati nascosti. Pongono una seria minaccia nella comunicazione fra malware, esfiltrazione dei dati e il cyber-spionaggio.

Gli attacchi tramite Covert Channel sfruttano vulnerabilità nel design del sistema, nelle risorse condivise e nelle politiche di sicurezza per trasmettere segretamente dati fra processi o sistemi aggirando i tradizionali controlli di sicurezza. Questi attacchi sono spesso usati per l'esfiltrazione dei dati, privilege escalation o comunicazioni silenziose tra delle componenti malware.

Attacchi basati sulla memoria

Questi attacchi manipolano le risorse di sistema condivise per memorizzare e recuperare informazioni nascoste.

Esempio 1.6.

Manipolazione degli attributi dei file:

il malware altera i metadati dei file (e.g. timestamp, permessi) per codificare i messaggi.

Sfruttamento della memoria condivisa:

i processi comunicano modificando le regioni di memoria condivise.

Segnali tramite l'utilizzo del disco:

un processo scrive o elimina i dati mentre un altro processo rileva le modifiche. Disk Usage Signaling: One process writes or deletes data, and another process detects changes.

Campi nell'intestazione TCP/IP:

gli attaccanti codificano i dati in campi inutilizzati o facoltativi dei pacchetti di rete (e.g. ID IP, numeri di sequenza o valori TTL).

Attacchi basati sulla temporizzazione

Questi attacchi manipolano la tempistica o le prestazioni del sistema per trasmettere informazioni nascoste.

Esempio 1.7.

Fluttuazione del carico della CPU: il malware altera gli schemi di utilizzo della CPU, che un altro processo misura per decodificare le informazioni.

Temporizzazione dei pacchetti di rete: il mittente trasmette i pacchetti a intervalli di tempo specifici per codificare i dati binari.

Attacchi basati sulla cache: gli aggressori utilizzano i tempi di accesso alla cache (e.g. Flush+Reload, Prime+Probe) per far trapelare segreti

Analisi del consumo energetico: i dati sensibili vengono estratti analizzando le variazioni del consumo energetico (utilizzate negli attacchi crittografici side-channel).

Esempi reali di attacchi Covert Channel

- Attacchi basati sui Malware:
Duqu 2.0 (2015) utilizzava canali TCP/IP occulti per esfiltrare i dati evitando il rilevamento
- Attacchi di tunneling DNS:
il malware nasconde i dati all'interno delle query DNS (ad esempio, comunicazione C2 per le botnet).
- Covert Channels basati sul Cloud e sulla Virtualization:
Hypervisor Covert Channels: Le macchine virtuali (VM) sullo stesso host fisico perdono dati attraverso la cache o la memoria della CPU condivisa.
Cloud Timing Attacks: Cloud tenants use execution timing differences to infer co-resident VM activities.

Nome Attacco	Tipo	Descrizione
Spectre and Meltdown	Timing (Cache)	Exploit speculative execution to leak memory contents
Flush+Reload	Timing (Cache)	Attacker flushes shared memory and reloads it to observe access patterns.
Prime+Probe	Timing (Cache)	Attacker fills cache and monitors eviction patterns to infer secret data.
Packet Timing Attack	Timing (Network)	Varies packet transmission timing to send hidden messages.
Keystroke Timing Attack	Timing (Human Interaction)	Infers typed keys based on timing variations between keystrokes.
TCP Covert Channel	Storage (Network)	Encodes data in TCP packet fields (e.g., sequence numbers, flags).
File Lock Covert Channel	Storage (Filesystem)	Uses file locking/unlocking as a signaling mechanism.

Tabella 1: Menzione a degli attacchi Covert Channel

1.6 Strumenti di Mitigazione e Protezione

Il loro rilevamento e la loro mitigazione richiede un rigoroso monitoraggio, l’isolamento delle risorse e tecniche per introdurre rumore. Difendersi da loro, richiede una combinazione di rinforzo delle politiche, gestione delle risorse e tecniche di monitoraggio. Mitigarli, richiede una sicurezza multi livello fra hardware, OS, applicazioni e reti.

Siccome la completa eliminazione è difficile, strategie di rilevazione e minimizzazione sono essenziali (es randomizzazione, rigoroso controllo degli accessi delle risorse, rilevamento delle anomalie).

Esempio 1.8. *Un file può essere aperto e chiuso da un programma in modo specifico pattern temporale così che possa essere rilevato da un altro programma.*

ma; lo schema potrà essere poi interpretato come una stringa di bit formando così un Covert Channel. Di conseguenza, siccome è improbabile che l'utente legittimo controlli i pattern relativi alla chiusura/apertura dei file; questo tipo di Covert Channel può rimanere non identificato per un lungo periodo.

Principali strategie di difesa per la mitigazione

Difese basate sul Sistema e sulle Politiche(Policy)

1. Politiche di controllo degli accessi:

Applicare un forte controllo degli accessi (MAC, RBAC) per evitare interazioni non autorizzate con i processi. Implementare il minimo privilegio e il controllo obbligatorio dell'accesso (MAC) per limitare la comunicazione non autorizzata tra i processi. Utilizzare sandbox e compartimentazione per isolare i processi.

2. Controllo del flusso di informazioni:

Utilizzare obbligatoriamente modelli di controllo del flusso di dati (Bell-LaPadula, Biba) per evitare fughe di informazioni e impedire così che i processi ad alta sicurezza perdano dati ai processi a bassa sicurezza.

3. Separazione e isolamento dei processi:

Disattivare le risorse condivise non necessarie (ad esempio, comunicazione tra processi, memoria condivisa). Utilizzare la virtualizzazione e la containerizzazione per separare i processi. Applicare l'air-gapping per i sistemi altamente sensibili.

Protezioni basate sulla gestione delle risorse e dei tempi

- **Tecniche di Randomizzazione**

Introdurre rumore nelle risposte del sistema (ad esempio, randomizzando i tempi di esecuzione, aggiungendo ritardi) per interrompere i Covert Channel basati sul tempo. Utilizzare tecniche di randomizzazione o svuotamento della cache per prevenire attacchi side-channel basati sulla cache.

- **Limitazione della velocità e controllo della larghezza di banda**

Limitare la CPU, la memoria o la larghezza di banda della rete per limitare la capacità di un canale nascosto. Implementare meccanismi di throttling (limitazione) per le risorse condivise.

Protezioni basate sulla sicurezza della rete

- **Ispezione e filtraggio dei pacchetti:**

Utilizzare la Deep Packet Inspection (DPI) per rilevare schemi anomali nel traffico di rete. Bloccare o sanificare i campi inutilizzati dei protocolli (ad esempio, le intestazioni TCP/IP).

- **Analisi del traffico e rilevamento delle anomalie:**

Applicare la segmentazione della rete per limitare i flussi di dati non autorizzati. Utilizza il monitoraggio basato sull'intelligenza artificiale per rilevare modelli di comunicazione insoliti. Utilizza sistemi di rilevamento delle intrusioni (IDS) e analisi dei log per identificare attività sospette.

Miglioramenti della sicurezza hardware e software

Difese hardware e OS

- Randomizzare i tempi di esecuzione e iniettare rumore nelle risposte del sistema (per interrompere gli attacchi basati sulla temporizzazione).

- Implementare operazioni crittografiche a tempo costante per prevenire i canali laterali di temporizzazione.

- Svuotare e partizionare le cache della CPU per prevenire gli attacchi alla cache cross-process.

- Progettazione hardware sicura

Implementare operazioni crittografiche a tempo costante per prevenire attacchi basati sulla temporizzazione. Utilizzare enclave sicuri (ad esempio, Intel SGX, ARM TrustZone) per proteggere i calcoli sensibili.

- Protezioni a livello di sistema operativo

Applicare l'isolamento della memoria e disabilitare la memoria condivisa quando non è necessaria. Implementare algoritmi di pianificazione sicuri per prevenire fuoriuscite di dati tramite la temporizzazione basata sui processi.

Verifica e test dei Covert Channel

- Eseguire regolarmente analisi dei canali nascosti nei test di penetrazione.
- Utilizzare strumenti di rilevamento dei Covert Channel (ad esempio, analisi del flusso di rete, monitoraggio del comportamento del sistema).

Strategie di Mitigazione

Controllo sugli Accessi:

limitare i permessi per prevenire scambio di informazioni non autorizzato
Monitoraggio del Traffico:

analizzare i comportamenti del sistema per rilevare anomalie Aggiunta di Rumore (Noise Injection):

introdurre casualità nei pattern temporali o di accesso alla memoria per rendere il prelevamento dei dati difficile. Strategie di mitigazione:

- System Design: Minimize shared resources and unnecessary communication paths.
- Monitoring: Detect unusual patterns in resource usage or timing.
- Access Controls: Restrict access to critical resources.
- Noise Introduction: Add random delays or variations to disrupt timing-based channels.

2 Protocollo ICMP

ICMP (Internet Control Message Protocol) è un protocollo a livello rete utilizzato per la diagnostica, per la segnalazione di errori, per ottenere informazioni di controllo e per la risoluzione dei problemi nelle reti. Aiuta i dispositivi (come i router e gli host) a comunicare, gestire e risolvere i problemi della rete ma non è utilizzato per la trasmissione di dati (come TCP o UDP).

Sebbene sia essenziale per la diagnostica di rete e la segnalazione di errori; può essere utilizzato in modo improprio per degli attacchi o per la ricognizione della rete (network reconnaissance). Gli aggressori possono utilizzare ICMP per attacchi DDoS, di ricognizione, di esfiltrazione di dati o di covert channel.

Differenze tra ICMP, TCP e UDP

Funzionalità	ICMP	TCP	UDP
Scopo	Segnalazione di errori e diagnostica	Trasferimento di dati affidabile	Trasferimento di dati veloce e senza connessione
Orientato alla connessione?	No	Sì	No
Numeri di porta?	No	Sì	Sì
Affidabilità	No	Sì (Acknowledgments)	No
Utilizzato da	Ping, Traceroute, PMTUD	HTTP, FTP, Email	DNS, VoIP, Streaming

Caratteristiche di ICMP

- Opera al Livello 3 (Livello di rete) nel modello OSI.
- Funziona con IP per fornire feedback sui problemi di rete.
- Non stabilisce una sessione (Stateless e Connectionless).
- Nessun numero di porta (a differenza di TCP e UDP).
- Utilizzato per la risoluzione dei problemi di rete (e.g. esempio, ping, traceroute).

- Supporta IPv4 (ICMPv4) e IPv6 (ICMPv6) con funzionalità avanzate in ICMPv6.

ICMP è utilizzato principalmente per:

- Segnalazione errori: informa il mittente sui problemi di rete (ad esempio, destinazione non raggiungibile, perdita di pacchetti).
- Diagnostica di rete: aiuta nella risoluzione dei problemi di rete utilizzando strumenti come ping e traceroute.
- Messaggistica di controllo: gestisce la congestione della rete e gli aggiornamenti di routing in alcuni casi.

Struttura di un messaggio ICMP

Ogni messaggio ICMP è composto da:

- Tipo - Identifica il tipo di messaggio (ad esempio, Echo Request, Destinazione irraggiungibile).
- Codice - Fornisce dettagli aggiuntivi sul tipo di messaggio.
- Checksum - Garantisce l'integrità dei dati.
- Dati - Opzionale, può contenere parte del pacchetto IP originale che ha causato l'errore.

Formato dell'intestazione ICMP

```

+-----+
|      — Type — Code — Checksum —
+-----+
|      — Additional Data (if required) —
+-----+

```

I messaggi ICMP sono classificati o come messaggi di errore o come messaggi informativi

- **Messaggi di errore** - Segnalano problemi nella comunicazione di rete.
- **Messaggi informativi** - Utilizzati per scopi diagnostici e di controllo.

Error Messages

Type	Code	Meaning
3	0-15	Destination Unreachable (e.g., no route to host, port unreachable)
4	0	Source Quench (deprecated, used to indicate congestion)
5	0-3	Redirect Message (suggesting a better route)
11	0-1	Time Exceeded (TTL expired, used in traceroute)
12	0-1	Parameter Problem (invalid IP header)

Error Messages

Type	Code	Message Name	Description
3	0	Network Unreachable	No route to destination network.
3	1	Host Unreachable	No route to specific host.
3	3	Port Unreachable	Destination port is closed.
3	4	Fragmentation Needed	Packet needs fragmentation, but DF bit is set.
4	0	Source Quench (Deprecated)	Indicates network congestion.
5	0-3	Redirect Message	Suggests a better route for packets.
11	0	Time Exceeded	TTL expired before reaching the destination (used in traceroute).
12	0-1	Parameter Problem	Invalid IP header field.

Informational Messages

Type	Code	Message Name	Description
0	0	Echo Reply	Response to a ping request.
8	0	Echo Request	Used by ping to test connectivity.
9	0	Router Advertisement	Routers announce themselves to hosts.
10	0	Router Solicitation	Hosts request router advertisements.

Utilizzi di ICMP nelle reti

1. Ping (Richiesta Echo ICMP e Risposta Echo)

Il comando **ping**, invia pacchetti ICMP Echo Request per testare la connettività.

- Invia delle richieste Echo ICMP a una destinazione per verificare la connettività.
- Se l'host è raggiungibile, risponde con un ICMP Echo Reply.

2. Traceroute (tracert su Windows, traceroute su Linux/macOS)

Il comando **traceroute**, utilizza messaggi ICMP Time Exceeded per mappare il percorso dei pacchetti.

- Tramite i messaggi ICMP Time Exceeded traccia il percorso che i pacchetti seguono attraverso una rete
- Il valore TTL (Time-To-Live) viene incrementato per determinare ciascun router lungo il percorso.

3. Scoperta del percorso MTU (PMTUD)

La **PMTUD**, utilizza messaggi ICMP Fragmentation Needed per ottimizzare le dimensioni dei pacchetti. Ovvero per trovare la dimensione ottimale del pacchetto per un percorso di rete.

2.1 Possibili attacchi tramite ICMP

Attacchi Denial-of-Service (DoS/DDoS)

ICMP Flood (Ping Flood)

Sopraffare un bersaglio con richieste Echo

- Attacco:

L'attaccante invia un gran numero di richieste di ICMP Echo (richieste di ping) a un sistema bersaglio. Se il sistema risponde con risposte ICMP Echo, consuma potenza di elaborazione e larghezza di banda. Se più macchine attaccano contemporaneamente, si parla di un attacco DDoS (Distributed DoS) ICMP Flood.

- Mitigazione:

Limitare la velocità del traffico ICMP su firewall e router. Disattivare le richieste di eco ICMP dalle reti esterne se non necessarie. Utilizzare sistemi di rilevamento delle intrusioni (IDS) per monitorare le richieste di ping eccessive.

Attacco Smurf

Richieste ICMP contraffatte amplificano il traffico verso una vittima.

- Attacco:

L'aggressore invia richieste ICMP Echo con un IP sorgente falsificato (l'IP della vittima). Le richieste vengono inviate a un indirizzo broadcast, provocando la risposta di tutti gli host della rete. La vittima viene sommersa da risposte ICMP Echo, che portano a una condizione DoS.

- Mitigazione:

Disabilitare le richieste di broadcast ICMP sui router (nessuna trasmissione diretta IP) Implementare filtri in ingresso per bloccare i pacchetti con indirizzi di origine falsificati. Utilizzare le regole del firewall per bloccare il traffico ICMP non necessario.

Ping della morte (attacco storico)

invio di pacchetti ICMP di grandi dimensioni per mandare in crash i sistemi

- Attacco: L'attaccante invia un pacchetto ICMP sovradimensionato (> 65.535 byte) causano crash da buffer overflow nei sistemi vulnerabili. I

sistemi operativi più vecchi potrebbero crashare, bloccarsi o riavviarsi quando gestiscono tali pacchetti.

- Mitigazione: I sistemi moderni rifiutano i pacchetti di dimensioni eccessive. Applicare aggiornamenti e patch di sistema per prevenire questa vulnerabilità.

ICMP Unreachable Flood

- Attacco:
L'attaccante invia un numero massiccio di messaggi ICMP Destination Unreachable. Può sovraccaricare i dispositivi di rete e causare un denial of service.
- Mitigazione:
Configurare limiti di velocità per i messaggi di errore ICMP. Implementare regole firewall per eliminare il traffico ICMP eccessivo

Attacchi di riconoscimento

ICMP Ping Sweep

- Attacco:
L'aggressore invia richieste ICMP Echo a più host su una rete. Sulla base delle risposte, l'attaccante identifica gli host attivi per ulteriori attacchi.
- Mitigazione:
Blocca le richieste ICMP Echo da fonti esterne. Utilizzare sistemi di prevenzione delle intrusioni (IPS) per rilevare e bloccare attività di scansione sospette.

Attacco Timestamp ICMP

- Attacco:
Le richieste ICMP Timestamp (tipo 13) consentono agli aggressori di determinare il tempo di attività del sistema. Queste informazioni aiutano gli aggressori a individuare i sistemi vulnerabili o riavviati di recente.
- Mitigazione:
Disattivare le richieste di timestamp ICMP su firewall e router. Utilizzare protocolli di sincronizzazione temporale (NTP) con autenticazione anziché query orarie basate su ICMP.

Attacco ICMP che maschera l'indirizzo

- Attacco:

L'aggressore invia una richiesta di mascheramento dell'indirizzo ICMP (tipo 17) a un bersaglio. Se l'obiettivo risponde con la sua maschera di sottorete (subnet mask), rivela i dettagli della rete all'attaccante.

- Mitigazione:

Disattivare le risposte ICMP Address Mask a meno che non siano necessarie per le operazioni di rete. Utilizzare i firewall per filtrare il traffico ICMP proveniente da fonti non attendibili.

Attacchi ICMP Tunneling e Covert Channel

ICMP Tunneling

Covert Channel che utilizzano pacchetti ICMP per aggirare i firewall.

- Attacco:

Gli attaccanti encapsulano dati dannosi all'interno delle richieste e delle risposte ICMP Echo. I dati sono incorporati nei pacchetti ICMP per poter aggirare i firewall che consentono il traffico ICMP (ma bloccano le connessioni TCP/UDP) ed esfiltrare così le informazioni. Spesso utilizzato per comunicazioni segrete in malware e canali C2 (comando e controllo).

- Esempi di strumenti:

- Icmpsh - Crea una reverse shell utilizzando ICMP.
- PingTunnel - Incanala il traffico TCP attraverso pacchetti ICMP.

- Mitigazione:

Ispezione approfondita dei pacchetti (DPI) per rilevare ICMP Tunneling. Blocca le richieste/risposte di ICMP Echo da reti non attendibili. Monitorare il traffico di rete per individuare modelli ICMP insoliti.

Esfiltroazione ICMP (furto di dati tramite ICMP)

- Attacco:

Gli attaccanti inseriscono dati sensibili (password, file, comandi) all'interno dei pacchetti ICMP. I dati vengono inviati a un server esterno controllato dall'attaccante.

- Mitigazione:

Monitorare e registrare il traffico ICMP per rilevare attività anomale. Utilizzare i firewall per limitare il traffico ICMP solo ai dispositivi necessari. Utilizzare soluzioni DLP (Data Loss Prevention) per rilevare i tentativi di esfiltrazione.

ICMP Covert Channels

- Attacco:

Malware e attaccanti utilizzano pacchetti ICMP per stabilire un canale di comunicazione nascosto. Spesso utilizzato nella comunicazione C2 per botnet o operazioni di malware furtive.

- Mitigazione:

Monitorare il traffico ICMP per individuare modelli di utilizzo insoliti. Utilizzare i sistemi di rilevamento delle intrusioni di rete (NIDS) per rilevare Covert Channel. Limitare la comunicazione ICMP tra reti interne ed esterne.

Attacco di reindirizzamento ICMP

- Messaggi di reindirizzamento ICMP non autorizzati reindirizzano il traffico verso un gateway dannoso.
- Mitigazione: disabilitare il reindirizzamento ICMP.

2.2 Buona practice di sicurezza

Per prevenire gli attacchi basati su ICMP; buone misure di sicurezza sono:

- limitare e filtrare l'utilizzo di ICMP tramite i firewall
- la limitazione della velocità
- il monitoraggio del traffico (tramite strumenti di sicurezza) per rilevare le anomalie

Regole del firewall

Limitare o bloccare il traffico ICMP non necessario.

- Bloccare le richieste Echo di ICMP da reti esterne, a meno che non siano necessarie.

- Disabilitare le risposte a ICMP Timestamp e Address Mask per impedire la ricognizione.
- Consentire solo i messaggi di errore ICMP necessari (ad esempio, Destinazione non raggiungibile).
- Eliminare i messaggi di reindirizzamento ICMP per impedire la manipolazione dell'instradamento (del routing).

Limitazione della velocità

Limitare la velocità delle richieste ICMP.

- Limita il numero di pacchetti ICMP al secondo per prevenire la sovrastazione.
- Configura i criteri di limitazione della velocità ICMP su router e firewall.

Monitoraggio della rete e Rilevamento

- Utilizzare i sistemi di rilevamento delle intrusioni (IDS/IPS) per rilevare abusi del protocollo ICMP.
- Analizza i registri di rete per attività ICMP insolite (ad esempio, pacchetti ICMP di grandi dimensioni, ping frequenti).
- Implementa l'ispezione approfondita dei pacchetti (DPI) per identificare il Tunneling ICMP.

Rafforzamento del sistema

- Mantieni aggiornati i sistemi e il firmware per correggere le vulnerabilità ICMP note
- Disattivare i servizi ICMP sui sistemi critici se non necessari.
- Utilizzare soluzioni di sicurezza degli endpoint per rilevare malware che utilizzano ICMP per la comunicazione

3 Riepilogo attacchi ICMP Covert Channel

Un **Covert channel** è un metodo di comunicazione nascosto che consente agli attaccanti di trasferire dati in un modo da aggirare le politiche di sicurezza. I canali nascosti ICMP pongono seri rischi per la sicurezza, consentendo l'esfiltrazione furtiva dei dati, il tunneling e la comunicazione di malware.

I Covert Channel ICMP utilizzano pacchetti ICMP (tipicamente richieste e risposte di eco) per nascondere i dati all'interno di campi che normalmente vengono ignorati o non monitorati.

ICMP (Internet Control Message Protocol) è un protocollo, utilizzato principalmente per la diagnostica della rete e la segnalazione di errori. Tuttavia può essere sfruttato per creare covert channel, percorsi di comunicazione nascosti utilizzati per l'esfiltrazione dei dati, operazioni di comando e controllo (C2) e aggiramento delle policy di sicurezza.

Gli aggressori utilizzano ICMP perché:

- Molti firewall e dispositivi di sicurezza consentono il traffico ICMP per la diagnostica della rete.
- I pacchetti ICMP possono trasportare dati (payload) nascosti senza destare sospetti.
- I sistemi di sicurezza tradizionali si concentrano sul traffico TCP/UDP, trascurando ICMP.

Implementando rigide restrizioni ICMP, l'ispezione approfondita dei pacchetti, le regole del firewall e il rilevamento delle anomalie, le organizzazioni possono rilevare e mitigare efficacemente queste minacce.

3.1 Attacchi Covert Channel ICMP

Tipo di attacco	Descrizione
Tunneling ICMP	Incapsulamento del traffico TCP/IP all'interno di pacchetti ICMP per eludere le restrizioni del firewall
Esfiltrazione dati ICMP	Invio di dati rubati nascosti all'interno di payload ICMP a un server esterno.
Comando e controllo (C2) basati su ICMP	Malware che riceve comandi da un aggressore tramite ICMP.
ICMP Reverse Shell	Una backdoor che consente a un aggressore di controllare una macchina da remoto tramite ICMP.

Tabella 2: Esempi di attacchi Covert Channel ICMP

ICMP Tunneling

Il tunneling ICMP consente agli aggressori di incapsulare i dati all'interno dei pacchetti ICMP, creando un canale di comunicazione nascosto.

1. L'attaccante inserisce istruzioni di comando e controllo (C2) nei pacchetti ICMP.
2. Questi pacchetti vengono inviati a un sistema compromesso dietro un firewall.
3. Il sistema estrae le istruzioni nascoste e le esegue.
4. Le risposte vengono inviate tramite ICMP Echo Replies

Esempio 3.1. Esempio di un caso d'uso

I malware (ad esempio le botnet) utilizzano il protocollo ICMP per aggirare i firewall e ricevere comandi da aggressori remoti. Gli attaccanti stabiliscono una reverse shell tramite ICMP, controllando una macchina compromessa.

Esempio 3.2. Esempi di Strumenti per il tunneling ICMP

Icmpsh - Crea una shell inversa tramite ICMP. PingTunnel – Incanala il traffico TCP attraverso richieste e risposte di eco ICMP. Ptunnel-NG – Versione avanzata di PingTunnel per aggirare i firewall

Esfiltrazione dei dati ICMP

Gli aggressori possono rubare dati (password, file, informazioni sensibili) incorporandoli nei pacchetti ICMP e inviandoli a un server esterno.

1. L'aggressore codifica dati sensibili (ad esempio numeri di carte di credito, chiavi di crittografia) in pacchetti ICMP.
2. I pacchetti vengono inviati a un server esterno controllato dall'aggressore.
3. L'aggressore estrae e decodifica i dati rubati dal traffico ICMP.

Esempio 3.3. Esempio di caso d'uso

Una minaccia interna estrae dati classificati tramite richieste ICMP Echo. Un'infezione da malware trasmette keylog o screenshot tramite pacchetti ICMP

Esempio 3.4. Esempio di strumenti per l'esfiltrazione di dati con ICMP
icmptx - Codifica e trasferisce dati tramite pacchetti ICMP. LOKI - Nasconde i dati nelle risposte ICMP Echo. Hans - Utilizza ICMP per il trasferimento di dati criptati.

Comando e controllo (C2) della botnet basato su ICMP

Alcune botnet e malware utilizzano ICMP per comunicare con i loro server di comando e controllo (C2)

1. L'attaccante inserisce i comandi C2 nei pacchetti ICMP.
2. Il bot infetto legge il comando e lo esegue.
3. Il bot invia i risultati dell'esecuzione tramite risposte ICMP

Esempio 3.5. Esempio di malware che utilizzano ICMP per la comunicazione C2

Duqu – Utilizza ICMP per inviare dati crittografati. Pingback - Un malware che riceve comandi tramite ICMP. Trojan.Medo - Utilizzava ICMP come canale backdoor.

3.2 Strategie di rilevamento

Tecnica	Rilevamento	Mitigazione
Analisi del traffico di rete	Identifica anomalie nel volume e nei pattern ICMP ed esfiltrazione di dati	Limita i tipi ICMP non necessari
Deep Packet Inspection (DPI)	Rileva l'esfiltrazione e il tunneling dei dati	Blocca i pacchetti ICMP con payload inattesi
IDS/IPS (Snort, Zeek)	Segnala comportamenti ICMP insoliti	blocca le richieste ICMP sospette

Tabella 3: Strumenti di rilevamento

Monitoraggio del traffico di rete

Analizzare il volume e le dimensioni dei pacchetti ICMP (ad esempio, payload insolitamente grandi) per eventuali anomalie. Rileva il traffico ICMP ad alta frequenza verso host esterni sconosciuti. Verificare la presenza di pacchetti ICMP con payload insolitamente grandi (e.g tentativi di esfiltrazione dei dati) o con schemi irregolari (e.g valori TTL variabili). Pacchetti ICMP con modifiche costanti del payload potrebbero indicare il trasferimento di dati nascosti.

Deep Packet Inspection (DPI)

Esaminare il contenuto del payload ICMP per rilevare eventuali dati incorporati insoliti (messaggi codificati, crittografia o anomalie). Contrassegna i pacchetti ICMP che contengono risposte non standard (e.g, una risposta Echo contenente dati inaspettati). Identificare schemi di comunicazione con indirizzi IP esterni tramite ICMP

Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)

Utilizzare Snort, Suricata o Zeek per rilevare e segnalare attività ICMP sospette

Esempio 3.6. *Regola Snort per il rilevamento del tunneling ICMP*

```

alert icmp any any -> any any (
    msg:"ICMP tunnel detected";
    content:"malicious-payload";
    sid:100001;
)

```

Rilevamento basato su anomalie

Rilevare il traffico ICMP che potrebbe indicare una comunicazione C2 implementando analisi comportamentali che possano rilevare un utilizzo anomalo di ICMP. Utilizzare strumenti di apprendimento automatico o SIEM (Security Information and Event Management) per segnalare deviazioni nell'utilizzo di ICMP.

3.3 Strategie di mitigazione

Metodo di mitigazione	Effetti
Disattiva ICMP se non necessario	Impedisce la maggior parte degli attacchi basati su ICMP
Limita ICMP ai tipi necessari	blocca i vettori di attacco non necessari
Limitazione della velocità	Impedisce il flooding e il tunneling ICMP
Regole del firewall	Blocca l'ICMP in uscita dai sistemi critici
Blocca ICMP in uscita dai firewall	Impedisce perdite di dati tramite ICMP
Endpoint Security (EDR)	Previene l'esecuzione dannosa di ICMP

Tabella 4: Metodologie di mitigazione

Restringere/ Limitare il traffico ICMP

Disattivare ICMP sui server e sugli endpoint a meno che non sia esplicitamente necessario e bloccare il traffico ICMP proveniente da fonti non attendibili. Configurare firewall e router in modo tale da consentire solo i messaggi ICMP necessari (e.g Destinazione non raggiungibile, Tempo Scaduto). Disattivare le richieste/risposte di eco ICMP sui sistemi critici.

Esempio 3.7. Regola del firewall per bloccare il traffico ICMP

```
iptables -A INPUT -p icmp  
--icmp-type echo-request -j DROP
```

Limitazione della velocità del traffico ICMP

Limitare la frequenza e la dimensione dei pacchetti ICMP per evitare il trasferimento nascosto di dati. Configurare i firewall in modo da consentire solo un numero specifico di pacchetti ICMP al secondo.

Esempio 3.8.

```
iptables -A INPUT -p icmp -m limit  
--limit 1/second -j ACCEPT
```

Utilizza la crittografia per prevenire la fuga di dati

Implementa la crittografia TLS/SSL per tutte le comunicazioni legittime così da impedire agli aggressori di utilizzare ICMP per l'esfiltrazione. Bloccare le trasmissioni non autorizzate di testo in chiaro su ICMP.

Blocca ICMP su interfacce esterne

Impedisci il traffico ICMP in uscita dalle reti interne per fermare l'esfiltrazione. Consenti ICMP solo per scopi diagnostici interni.

Sicurezza degli endpoint & Antivirus

Implementare strumenti antivirus e soluzioni EDR (Endpoint Detection & Response) per rilevare le minacce informatiche che utilizzano i covert channel ICMP per comunicare.

Implementa ICMP Proxy Filtering

Utilizza proxy ICMP per ispezionare, sanificare e bloccare payload ICMP inaspettati. Consenti solo il passaggio di traffico ICMP diagnostico legittimo

4 Strumenti Utilizzati

aaa