



Sniffing

Tramite tool Wireshark



Sniffing

Da Wikipedia, l'enciclopedia libera.

Con **sniffing** (dall'inglese, *odorare*), in **informatica** e nelle **telecomunicazioni**, si definisce l'attività di **intercettazione** passiva dei dati che transitano in una **rete telematica**: può essere svolta sia per scopi legittimi (ad esempio l'analisi e l'individuazione di problemi di comunicazione o di tentativi di intrusione) sia per scopi illeciti contro la **sicurezza informatica** (intercettazione fraudolenta di **password** o altre informazioni sensibili).

I prodotti **software** utilizzati per eseguire queste attività vengono detti **sniffer** ed oltre ad intercettare e memorizzare il **traffico** offrono funzionalità di analisi del traffico stesso: questi intercettano i singoli **pacchetti**, decodificando le varie **intestazioni** di **livello datalink**, **rete**, **trasporto**, **applicativo**, potendo offrire inoltre strumenti di analisi che analizzano ad es. tutti i pacchetti di una connessione TCP per valutare il comportamento del **protocollo di rete** o per ricostruire lo scambio di dati tra le applicazioni.

Wireshark

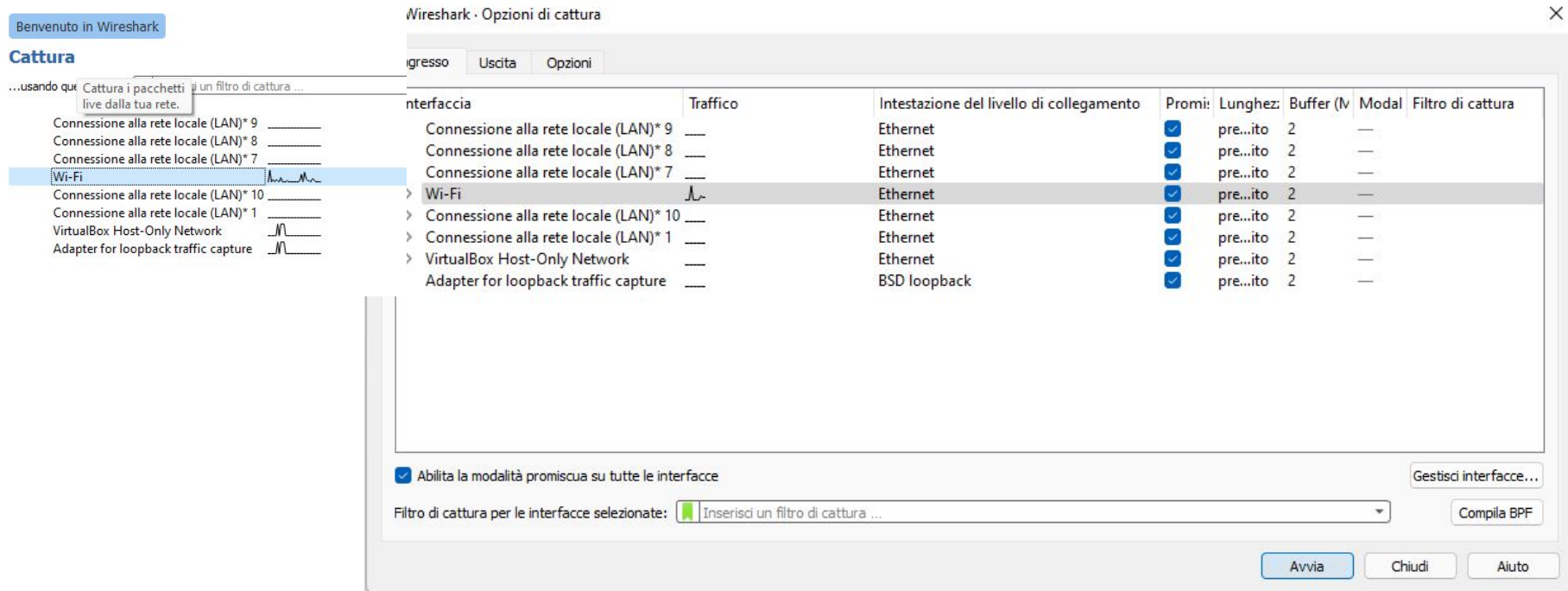
<https://www.wireshark.org/download.html>



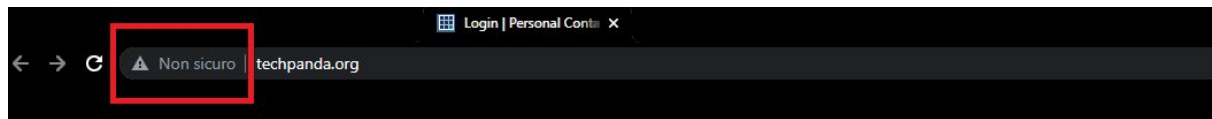
Sniffing di rete

1. Iniziare la registrazione dei pacchetti tramite Wireshark
2. Collegarsi al sito: <http://www.techpanda.org/>
3. Effettuare il login tramite protocollo non cifrato http (non sicuro)
4. Cercare nei pacchetti trasmessi un pacchetto http POST (invio di dati)
5. Leggere l'username e la password inseriti dall'utente

1 - Iniziare la registrazione



2,3 - Collegarsi al sito ed effettuare il login



Login | Personal Contacts Manager v1.0

Email*

Password*

☐ Remember me

Dashboard | Personal Contacts Manager v1.0

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	
34794	Dark	Maiden	8763544	darkmaiden@octopus.ps	Edit
34795	DarkDark	Maiden	87635444242	darkmaiden@octopus.ps	Edit
34796	bom bom	Hferhbr	8474937	min23@gmail.com	Edit
34797					Edit
34798					Edit
34799					Edit

Login | Personal Contacts Manager v1.0

Email*

Password*

☐ Remember me

4,5 - Cercare e leggere i dati trasmessi

No.	Time	Source	Destination	Protocol	Length	Info
362	17.989747	72.52.251.71	192.168.1.9	HTTP	693	HTTP/1.1 200 OK (application/javascript)
364	18.045385	192.168.1.9	72.52.251.71	HTTP	551	GET /css/check-radio-bg.png HTTP/1.1
413	18.170364	72.52.251.71	192.168.1.9	HTTP	739	HTTP/1.1 200 OK (PNG)
416	18.178445	192.168.1.9	72.52.251.71	HTTP	517	GET /favicon.ico HTTP/1.1
417	18.347682	72.52.251.71	192.168.1.9	HTTP	545	HTTP/1.1 200 OK (image/x-icon)
770	72.267370	192.168.1.9	72.52.251.71	HTTP	809	POST /index.php HTTP/1.1 (application/x-www-form-urlencoded)
777	72.392735	72.52.251.71	192.168.1.9	HTTP	1184	HTTP/1.1 302 Found (text/html)
779	72.398005	192.168.1.9	72.52.251.71	HTTP	646	GET /dashboard.php HTTP/1.1
792	72.523788	72.52.251.71	192.168.1.9	HTTP	74	HTTP/1.1 200 OK (text/html)
507	29.403656	192.168.1.7	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
521	32.477189	192.168.1.7	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
558	35.445668	192.168.1.7	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
36	5.947453	192.168.1.9	216.58.208.142	QUIC	1292	Initial, DCID=6ceddccc562fd8fb, PKN: 1, PING, PING, PADDING, PING
37	5.958157	216.58.208.142	192.168.1.9	QUIC	1292	Initial, SCID=6ceddccc562fd8fb, PKN: 1, ACK, CRYPTO, PADDING

> Frame 770: 809 bytes on wire (6472 bits), 809 bytes captured (6472 bits) on interface \Device\NPF_{AC4C5B25-4286-4F24-8A68-F11D65}

> Ethernet II, Src: IntelCor_b4:4c:6d (40:a3:cc:b4:4c:6d), Dst: zte_24:72:82 (c0:b1:01:24:72:82)

> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 72.52.251.71

> Transmission Control Protocol, Src Port: 59747, Dst Port: 80, Seq: 1, Ack: 1, Len: 755

> Hypertext Transfer Protocol

> HTML Form URL Encoded: application/x-www-form-urlencoded

> Form item: "email" = "prova@sistoprovando.it"

> Form item: "password" = "password_difficilissima"

0260	63 65 70 74 2d 45 6e 63	6f 64 69 6e 67 3a 20 67	cept-Enc oding: g
0270	7a 69 70 74 2c 20 64 65 66	6c 61 74 65 0d 0a 41 63	zip, def late .Ac
0280	63 65 70 74 2d 4c 61 6e	67 75 61 67 65 3a 20 69	cept-Lan guage: i
0290	74 2d 49 54 2c 69 74 3b	71 3d 30 2e 39 2c 65 6e	t-IT,it; q=0.9,en
02a0	2d 55 53 3b 71 3d 30 2e	38 2c 65 6e 3b 71 3d 30	-US;q=0. 8,en;q=0
02b0	2e 37 0d 0a 43 6f 6f 6b	69 65 3a 20 50 48 50 53	.7..Cook ie: PHPS
02c0	45 53 53 49 44 3d 61 35	30 37 33 37 63 34 38 39	ESSID=a5 0737c489
02d0	33 64 63 37 65 39 38 65	34 62 30 33 32 36 39 36	3dc7e98e 4b032696
02e0	34 33 35 64 38 34 0d 0a	0d 0a 65 6d 61 69 6c 3d	435d84...email=
02f0	70 72 6f 76 61 25 34 30	73 69 73 74 6f 70 72 6f	prova%40 sistopro
0300	76 61 6e 64 6f 2e 69 74	26 70 61 73 73 77 6f 72	vando.it &passwor
0310	64 3d 70 61 73 73 77 6f	72 64 5f 64 69 66 66 69	d=passwo rd diffi
0320	63 69 6c 69 73 73 69 6d	61	cilissima a



DDoS

Distributed Denial of Service



Denial of service

Da Wikipedia, l'enciclopedia libera.

Denial of Service (in [italiano](#) letteralmente *negazione del servizio* abbreviato in **DoS**), nel campo della [sicurezza informatica](#), indica un malfunzionamento dovuto ad un [attacco informatico](#) in cui si fanno esaurire deliberatamente le [risorse](#) di un [sistema informatico](#) che fornisce un servizio ai [client](#), ad esempio un [sito web](#) su un [web server](#), fino a renderlo non più in grado di erogare il servizio ai client richiedenti.^{[1][2]}

In un *denial of service distribuito* (*Distributed Denial of Service*), il traffico dei dati in entrata che inonda la vittima proviene da molte fonti diverse. L'esempio in analogia è quello di un gruppo di persone che affollano la porta d'ingresso o il cancello di un negozio o di un'azienda, e non consentendo alle parti legittime di entrare nel negozio o nel business, interrompono le normali operazioni. Ciò rende effettivamente impossibile fermare l'attacco semplicemente bloccando una singola fonte.

Oltre al senso primario di *denial of service* come azione deliberata ci si può riferire ad esso come azione accidentale, in seguito per esempio ad una errata configurazione,^{[3][4]} o come nel caso dell'effetto Slashdot.^[5]

Denial of Service

1. Trovare il proprio indirizzo IP (tramite prompt dei comandi)
2. Aprire il Task Manager e visualizzare l'attuale consumo di risorse
3. Eseguire un attacco DoS al proprio terminale
4. Aprire il Task Manager e visualizzare l'attuale consumo di risorse
5. Terminare l'attacco
6. Aprire il Task Manager e visualizzare l'attuale consumo di risorse

1 - Trovare il proprio indirizzo IP

ipconfig

```
C:\Users\level: ipconfig

Configurazione IP di Windows

Scheda Ethernet VirtualBox Host-Only Network:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::c06c:168f:2f41:685c%19
    Indirizzo IPv4. . . . . : 192.168.56.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda LAN wireless Connessione alla rete locale (LAN)* 1:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

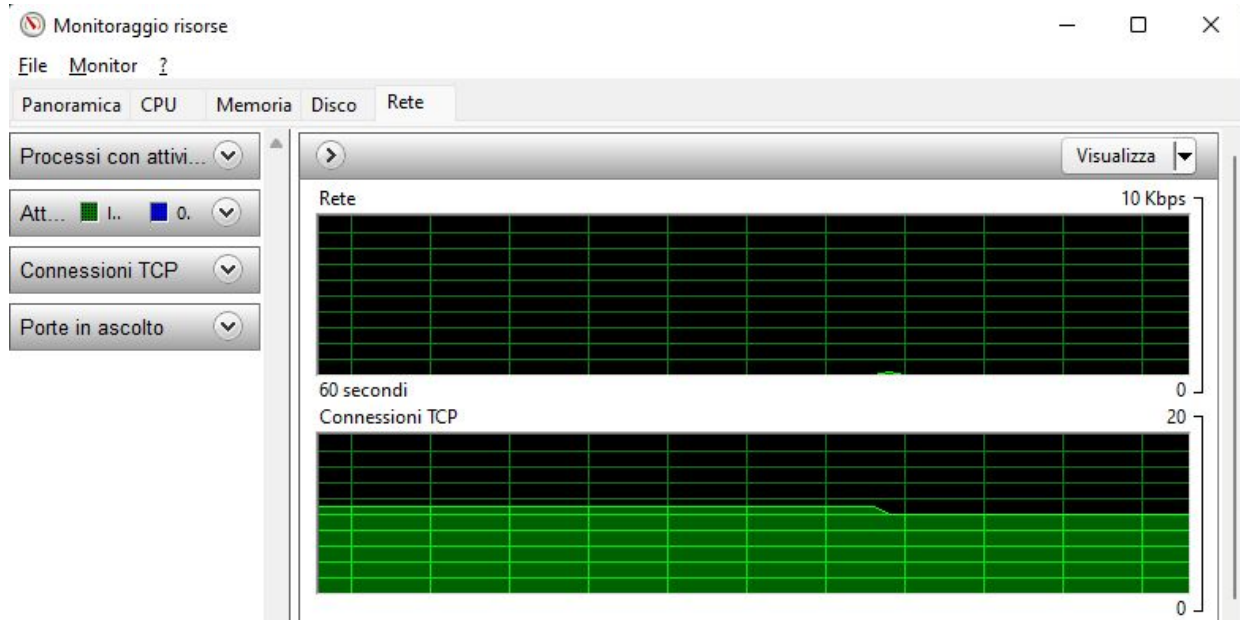
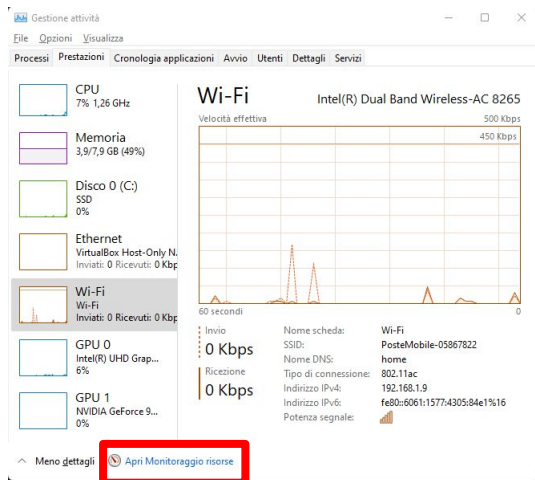
Scheda LAN wireless Connessione alla rete locale (LAN)* 10:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda LAN wireless Wi-Fi:

    Suffisso DNS specifico per connessione: home
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::6061:1577:4305:84e1%16
    Indirizzo IPv4. . . . . : 192.168.1.9
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1
```

2 - Consultare il Task Manager (monitoraggio risorse)

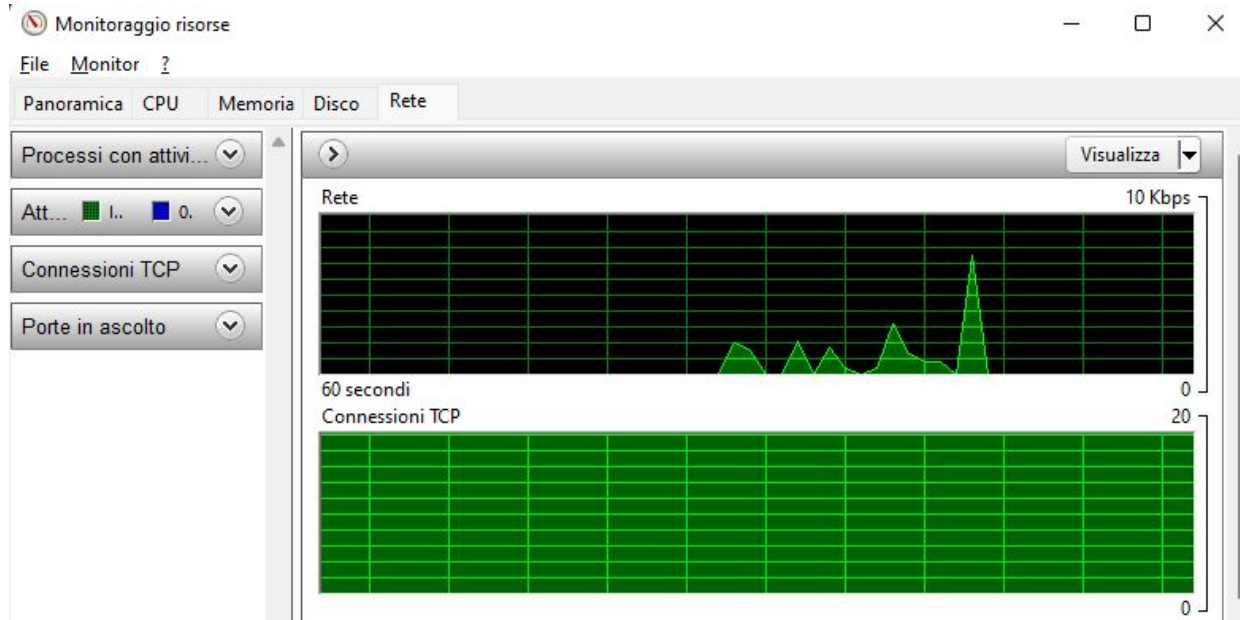
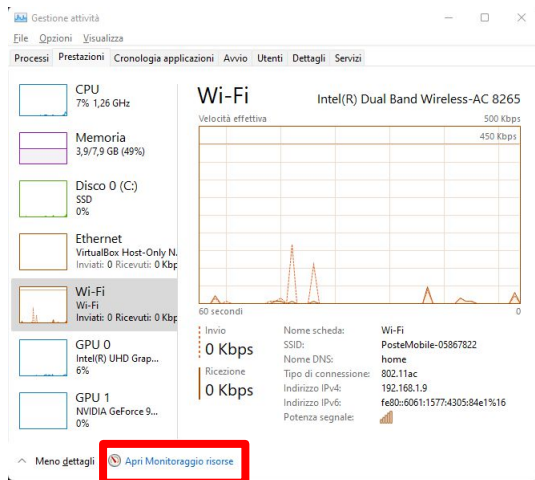


3 - Eseguire l'attacco DoS al proprio IP

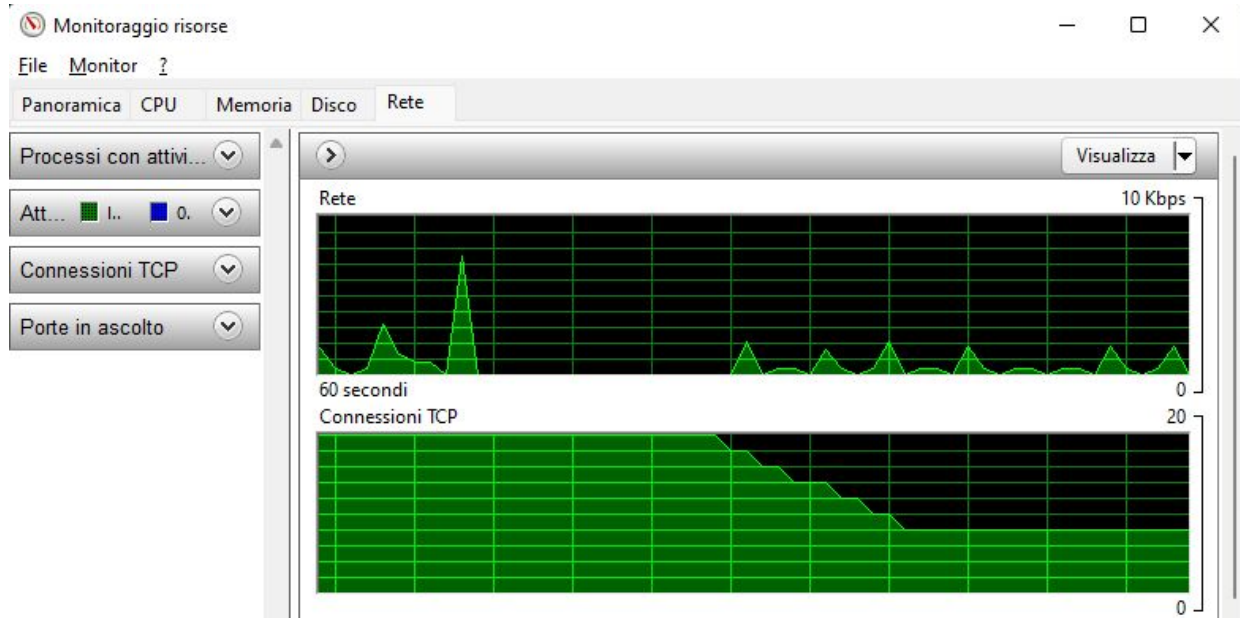
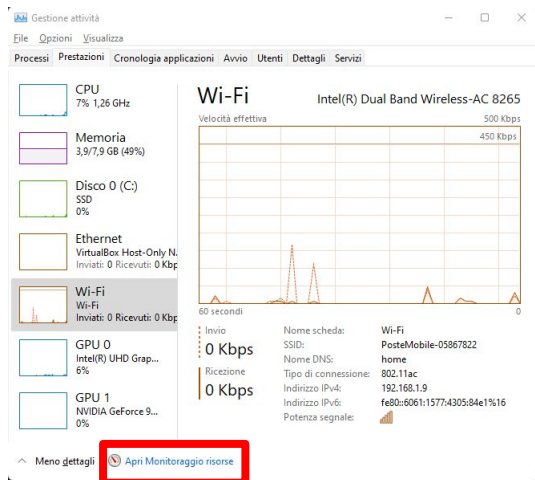
ping IP -t -l 65500

[illegible]

4 - Consultare il Task Manager (monitoraggio risorse)



6 - Consultare il Task Manager (monitoraggio risorse)



Distributed Denial of Service

1. Aprire il prompt dei comandi come amministratore
 - 1.1. **cmd (esegui come amministratore)**
2. Resettare la tabella ARP (mapping di rete IP - MAC)
 - 2.1. **arp -d**
3. Cercare un buon numero di indirizzi IP collegati alla rete locale
 - 3.1. **for /L %a in (1,1,254) do start ping 192.168.0.%a**
 - 3.2. **for /L %a in (1,1,254) do start ping 192.168.1.%a**
4. Visualizzare gli IP identificati
 - 4.1. **arp -a**
5. Utilizzare tutti gli IP per eseguire un attacco **SMURF** o **BOTNET**

Smurf

Da Wikipedia, l'enciclopedia libera.

Lo **Smurf** è un tipo di attacco su rete [Internet](#) volto a causare un [denial of service](#), sovraccaricando il computer vittima con numerosi messaggi provenienti da molti altri nodi della rete, in risposta a false richieste che vengono spacciate per richieste della vittima stessa.

Il nome deriva dal nome inglese dei [Puffi](#) e si riferisce al fatto che molti piccoli agenti insieme possono ottenere un grosso risultato.

Botnet

Da Wikipedia, l'enciclopedia libera.

Una **botnet** è una [rete](#) di [computer](#), solitamente [PC](#), controllata da un botmaster e composta da dispositivi infettati da [malware](#) specializzato, detti [bot](#) o [zombie](#).^[1]

I dispositivi connessi ad [Internet](#), al cui interno sussistono [vulnerabilità](#) nella loro infrastruttura di [sicurezza informatica](#), possono talvolta diventare parte della botnet e, se l'agente infettante è un [trojan](#), il botmaster può controllare il sistema tramite [accesso remoto](#). I [computer](#) così infettati possono scagliare attacchi, denominati, [Distributed Denial of Service](#) contro altri sistemi e/o compiere altre operazioni illecite, in alcuni casi persino su commissione di organizzazioni criminali.^[1]



DDOS

EXPLAINED

ANIMATED





Malware

Rabbit, Backdoor, Ransomware,
Trojan, Virus, Worm



Malware

Da Wikipedia, l'enciclopedia libera.

Malware (abbreviazione dell'inglese *malicious software*, lett. "software malevolo"), nella [sicurezza informatica](#), indica un qualsiasi [programma](#) informatico usato per disturbare le operazioni svolte da un [utente](#) di un [computer](#). Termine coniato nel 1990 da [Yisrael Radai](#),^[1] precedentemente veniva chiamato [virus per computer](#); in italiano viene anche comunemente chiamato [codice](#) maligno.

Indice

Classificazione

- 1 [Rabbit](#)
- 2 [Backdoor](#)
- 3 [Ransomware](#)
- 4 [Trojan](#)
- 5 [Virus](#)
- 6 [Worm](#)



Rabbit

Fork Bomb



Rabbit

Da Wikipedia, l'enciclopedia libera.

Un **rabbit** (anche **wabbit**), nella [sicurezza informatica](#), indica un tipo di [malware](#) che attacca le risorse del sistema duplicando in continuazione la propria immagine su disco, o attivando nuovi processi a partire dal proprio eseguibile, in modo da consumare tutte le risorse disponibili sul sistema in pochissimo tempo. Entrambi i nomi si riferiscono proprio alla prolificità di questo "infestante" (*rabbit* è l'[inglese](#) per [coniglio](#)). Si distinguono dai [virus](#) in quanto non "infettano" i file.

L'origine probabile del termine è la pronuncia da parte del personaggio dei [cartoni animati Elmer Fudd](#) (Taddeo), dell'universo di [Bugs Bunny](#), della parola "rabbit", in [inglese](#): coniglio. Tale personaggio è un cacciatore che viene ridicolizzato, tra l'altro, per la sua incapacità a pronunciare le "r": "rabbit" diventa "wabbit"; inoltre i conigli, come Bugs Bunny, possono riprodursi a gran velocità. Oltre ad autoriprodursi velocemente, i rabbit possono avere altri effetti malevoli. Un esempio di rabbit è la [fork bomb](#), dal nome del comando Unix sfruttato, ovvero [fork](#).

Fork Bomb (windows)

1. Creare un file di testo RABBIT.txt
2. Digitare nel file la Fork Bomb
 - 2.1. **start cmd /k echo PIPPO | %0**
3. Modificare l'estensione del file da .txt a .bat
4. Aprire un prompt dei comandi
 - 4.1. **cmd**
5. Digitare il seguente comando senza eseguirlo
 - 5.1. **TASKKILL /F /IM cmd.exe /T**
6. Fare doppio click sul file RABBIT.bat e successivamente eseguire il comando digitato sul prompt dei comandi per bloccare la Fork Bomb...

Fork bomb

Da Wikipedia, l'enciclopedia libera.

La **bomba fork** è un attacco di tipo **denial of service** contro un **computer** che utilizza la funzione **fork**. L'azione si basa sull'assunto che il numero di **programmi** e **processi** che possono essere eseguiti contemporaneamente su un computer abbia un limite.

Introduzione [[modifica](#) | [modifica wikitesto](#)]

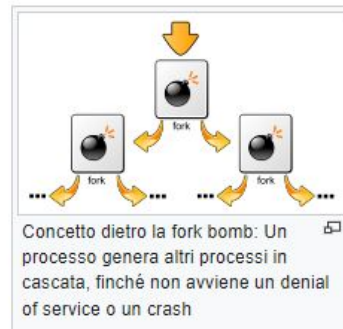
Una bomba fork agisce creando un gran numero di processi in un tempo molto rapido, così da saturare lo spazio disponibile nella lista dei processi che viene mantenuta dal **sistema operativo**. Se la tabella dei processi è piena, non possono essere avviati ulteriori programmi finché un altro non termina. Anche se ciò avvenisse, non è probabile che un programma utile all'utente venga avviato, dal momento che le istanze del programma bomba sono a loro volta in attesa di utilizzare per sé gli slot che si liberano nella tabella stessa.

Le bombe fork non si limitano ad utilizzare in maniera invasiva la tabella dei processi, ma impiegano anche del tempo di processore e della memoria. Pertanto il sistema rallenta e può diventare più difficile, se non impossibile da utilizzare.

Le bombe fork possono essere considerate un particolare tipo di **wabbit** (un programma che si auto-riproduce senza utilizzare funzionalità offerte da servizi o dalla rete).

Su un sistema con **Microsoft Windows**, utilizzando un **comando batch** (questa versione, al contrario di altre, funziona con tutti i sistemi **Windows 9x** e con tutti i sistemi della famiglia **Windows NT**):

```
%0|%0
```





Backdoor

Edward Snowden



Backdoor

Da Wikipedia, l'enciclopedia libera.

Una **backdoor** (dal termine inglese per *porta di servizio* o *porta sul retro*) è un metodo, spesso segreto, per passare oltre (aggirare, bypassare) la normale [autenticazione](#) in un prodotto, un [sistema informatico](#), un [crittosistema](#) o un [algoritmo](#).

Le backdoor sono spesso scritte in diversi [linguaggi di programmazione](#) e hanno la funzione principale di superare le difese imposte da un sistema, come può essere un [firewall](#), al fine di [accedere in remoto](#) a un [personal computer](#), ottenendo per mezzo di un sistema di [crittografia](#) un'autenticazione che permetta di prendere il completo o parziale possesso del computer vittima.

Una backdoor può celarsi segretamente all'interno di un ignaro [programma](#) di sistema, di un [software](#) separato, o può anche essere un componente [hardware](#) malevolo come apparati di rete, sistemi di sorveglianza e alcuni dispositivi di infrastruttura di comunicazione che possono avere celate al loro interno backdoor maligne permettendo l'intrusione di un eventuale criminale informatico ([cracker](#)).

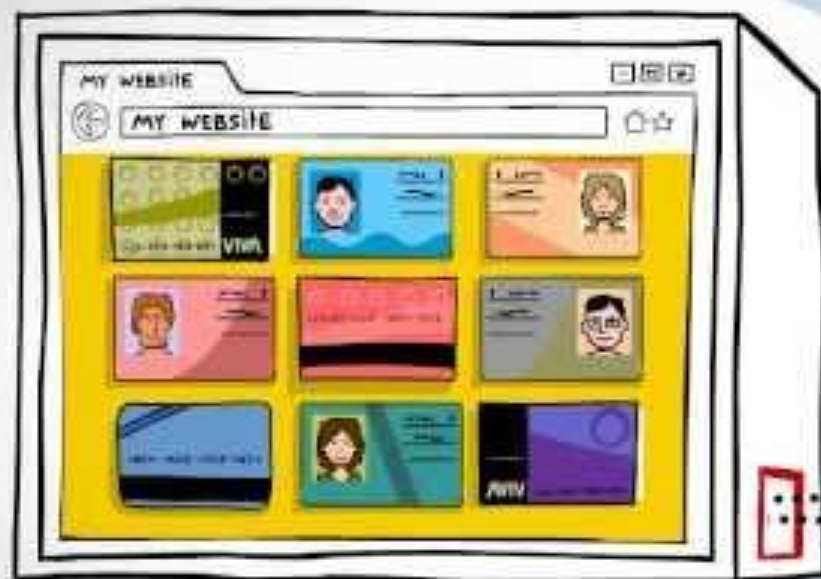
Furto di informazioni



- Il 17 marzo 2011, RSA pubblica una lettera aperta in cui annuncia, pur rimanendo vaga, che alcune informazioni relative all'uso delle chiavi SecurID sono state sottratte dai propri server.
- A seguito delle rivelazioni di Edward Snowden pubblicate su 5 settembre 2013, il *Guardian*, il *New York Times* e *ProPublica* rivelano che la NSA e il GCHQ sono in grado di decodificare la maggior parte dei sistemi di crittografia delle comunicazioni su Internet, sulla base dei documenti forniti da Edward Snowden. Attraverso il programma Bullrun della National Security Agency, i tre media spiegano che i metodi utilizzati dalle agenzie di intelligence anglosassoni includono misure per garantire il controllo sulla creazione di standard di crittografia americani e internazionali (NIST). Tre giorni dopo queste rivelazioni, il NIST ha fortemente raccomandato di non utilizzare il suo standard sul generatore di bit casuale deterministico a doppia curva ellittica (en). Portando il nome di "Pubblicazione speciale 800-90A", il NIST ha così riportato questo standard allo stato di "progetto", sei anni dopo averlo ufficialmente pubblicato come standard. Il 20 settembre 2013, RSA Security raccomanda ufficialmente di non utilizzare i suoi prodotti B-SAFE dopo l'installazione di una backdoor nello standard Dual_EC_DRBG da parte della NSA.
- Il 20 dicembre 2013, l'agenzia Reuters rivela l'esistenza di un contratto segreto tra la NSA e RSA Security per un importo di 10 milioni di dollari al fine di implementare una backdoor per bypassare l'algoritmo di crittografia RSA.
- Il 23 dicembre 2013, Mikko Hyppönen, Chief Research Officer di F-Secure, annulla la sua conferenza a RSA-2014

<https://www.ibs.it/errore-di-sistema-libro-edward-snowden/e/9788830454392>







Ransomware

Crittografia



Ransomware

Da Wikipedia, l'enciclopedia libera.

Un **ransomware** è un tipo di **malware** che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (*ransom* in inglese) da pagare per rimuovere la limitazione. Ad esempio alcune forme di ransomware bloccano il sistema e [intimano all'utente di pagare](#) per sbloccare il sistema, altri invece [cifrano](#) i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro.

Inizialmente diffusi in [Russia](#), gli attacchi con ransomware sono ora perpetrati in tutto il mondo.^{[1][2][3]} Nel giugno 2013, la casa software [McAfee](#), specializzata in software di sicurezza, ha rilasciato dei dati che mostravano che nei primi tre mesi del 2013 erano stati registrati 250 000 diversi tipi di ransomware, più del doppio del numero ottenuto nei primi tre mesi dell'anno precedente.^[4] [CryptoLocker](#), un [worm](#) ransomware apparso alla fine del 2013, ha ottenuto circa 3 milioni di dollari prima di essere reso innocuo dalle autorità.^[5]

WannaCry
Ransomware Attack



WannaCry

Da Wikipedia, l'enciclopedia libera.

WannaCry, chiamato anche **WanaCrypt0r 2.0**, è un [worm](#), di tipologia [ransomware](#), responsabile di un'[epidemia](#) su larga scala avvenuta nel maggio 2017 su computer con [Microsoft Windows](#). In esecuzione cripta i file presenti sul computer e chiede un riscatto di alcune centinaia di [dollari](#) per decriptarli.^{[2][3]}

Il 12 maggio 2017 il [malware](#) ha infettato i sistemi informatici di numerose aziende e organizzazioni in tutto il mondo, tra cui [Portugal Telecom](#), [Deutsche Bahn](#), [FedEx](#), [Telefónica](#), [Tuenti](#), [Renault](#), il [National Health Service](#), il Ministero dell'interno russo, l'Università degli Studi di Milano-Bicocca.

Al 28 maggio sono stati colpiti oltre 230.000 computer in 150 paesi, rendendolo uno dei maggiori contagi informatici mai avvenuti.^{[4][5]}

767%

Kaspersky: aumentati del 767% tra il 2019 e il 2020 gli attacchi ransomware mirati rivolti a vittime di alto profilo, l'Italia è tra i 10 Paesi più colpiti

Ransomware mirati

https://www.kaspersky.it/about/press-releases/2021_kaspersky-aumentati-del-767-gli-attacchi-ransomware-mirati-rivolti-a-vittime-di-alto-profilo-litalia--tra-i-10-paesi-pi-colpiti

I ransomware mirati sono dei malware utilizzati per estorcere denaro a obiettivi di alto profilo, come aziende, agenzie governative ed enti comunali

Ricatto finanziario

https://www.kaspersky.it/about/press-releases/2021_nel-2021-i-ransomware-hanno-rappresentato-quasi-la-meta-degli-incidenti-di-sicurezza-rilevati-in-italia-questi-attacchi-sono-aumentati-dell81

Questa tecnica consiste nel minacciare di far trapelare informazioni sensibili sulle società vittime dell'attacco per far crollare i prezzi delle loro azioni, come ad esempio durante eventi finanziari critici. Ad esempio i criminali potrebbero sfruttare le fusioni o le acquisizioni delle aziende, o divulgare informazioni su eventuali piani delle imprese di diventare pubbliche. Quando le aziende si trovano in uno stato finanziario così vulnerabile è più probabile che paghino il riscatto.

RaaS: Ransomware as a Service

Il Ransomware come Servizio o RaaS è una strategia imprenditoriale che include un nuovo soggetto nel processo dell'attacco informatico.

Da una parte abbiamo infatti le classiche organizzazioni di sviluppatori di malware con le competenze tecniche per scrivere il codice di un ransomware. Questi dopo aver sviluppato e distribuito con successo il proprio prodotto (in questo caso il ransomware) continueranno a concentrare i loro sforzi nel perfezionare e rendere sempre più letale il proprio prodotto mettendolo a disposizione sotto forma di servizio in abbonamento.


Dall'altra parte troveremo quindi una platea di nuovi soggetti, senza competenze tecniche necessarie per creare un malware, che si affilieranno all'organizzazione criminale e si occuperanno di individuare gli obiettivi e gli strumenti per la distribuzione del Ransomware.

<https://cyberment.it/malware/raas-o-ransomware-as-a-service-un-nuovo-modello-di-busines/>

2017's TOP 10 RANSOMWARE ATTACKS

NOTPETYA

- Posed as Ukrainian tax software update
- Infected thousands of computers in over 100 countries

 **RANSOM:**
\$300

WANNACRY

- Strain used the Eternal Blue vulnerability found in Microsoft's Server Block Message Protocol
- Infected 300,000+ computers in over 150 countries



 **RANSOM:**
\$300 - \$600

LOCKY

- Locky's Diablo and Lukitus variants embedded malicious macros in Word docs and delivered them via phishing emails
- Hollywood Presbyterian Medical Center paid a ransom of \$17,000 after falling victim to Locky

 **RANSOM:**
\$400 - \$800

CRYSIS

- Enabled cybercriminals to use Microsoft's Remote Desktop Protocol to exploit administrators and machines
- Affected victims in over 22 countries



 **RANSOM:**
\$455 - \$1,022

NEMUCOD

- Delivered via phishing email with fake shipping invoice attachment that contained malicious Javascript
- Infected machines in over 26 countries

 **RANSOM:**
\$300

JAFF

- Delivered via phishing emails
- Infected machines in over 21 countries

 **RANSOM:**
\$3,700



SPORA

- Delivered via malicious Javascript on legitimate websites, leading to pop-up alert to update Chrome browser, clicking the alert downloaded the ransomware
- Tiered ransom - cybercriminals would restore 2 files for free and charge more for additional files, as well as for immunity from future Spora infections

 **RANSOM:**
\$20 - \$79

CERBER

- Delivered via spam emails and Microsoft's Remote Desktop Protocol
- Packaged as a ransomware-as-a-service and given to other cybercriminals to distribute as they see fit
- (Cerber author took a 30% cut)

 **RANSOM:**
\$300 - \$600

CRYPTOMIX

- Distributed through Remote Desktop Protocol and exploit kits, such as malvertising
- Doesn't have a payment portal, so victims have to wait for the cybercriminal to email them instructions

 **RANSOM:**
\$3,000

JIGSAW

- Delivered via spam email with embedded image of Jigsaw from Saw
- Deleted victims' files every hour and each time the infection process started (i.e., after reboot) until the ransom was paid

 **RANSOM:**
\$20 - \$2,000



No Network Box client has ever been attacked by any ransomware. Our multilayered approach to security has protected each and every single one of our clients.

Contact us to find out how we can do the same for you.

www.networkboxusa.com

© 2017 Network Box USA, Inc. All rights reserved. This document is for informational purposes only and does not constitute an offer or a contract. Network Box USA, Inc. is not responsible for any damages or losses resulting from the use of this information.



Trojan

Cavallo di Troia



Trojan

Da Wikipedia, l'enciclopedia libera.

Un **trojan** o **trojan horse** (in italiano "cavallo di Troia"), nell'ambito della [sicurezza informatica](#), indica un tipo di [malware](#). Il trojan nasconde il suo funzionamento all'interno di un altro [programma](#) apparentemente utile e innocuo: l'utente, eseguendo o installando quest'ultimo programma, in effetti attiva anche il codice del trojan nascosto^{[1][2]}.

L'attribuzione del termine "[cavallo di Troia](#)" ad un programma (o file eseguibile) è dovuta al fatto che esso nasconde il suo vero fine. È proprio il celare le sue reali "intenzioni" che lo rende un trojan. In questo modo l'utente inconsapevolmente è indotto ad eseguire il programma.

In questo modo, come i troiani fecero entrare in città gli [achei](#) celati nel [mitico](#) cavallo di legno progettato da [Ulisse](#), così la vittima è indotta a far entrare il programma nel computer.

Oggi col termine "trojan" ci si riferisce ai malware ad accesso remoto (detti anche RAT dall'inglese *Remote Administration Tool*), composti generalmente da 2 file: il file server, che viene installato nella macchina vittima, ed un file client, usato dall'attaccante per inviare istruzioni che il server esegue.

Un *trojan* può contenere qualsiasi tipo di istruzione maligna. Spesso i trojan sono usati come veicolo alternativo ai [worm](#) e ai [virus](#) per installare delle [backdoor](#) o dei [keylogger](#) sui sistemi bersaglio.

I programmi di nuova generazione hanno molteplici funzionalità, quali connessioni tramite [bot IRC](#) che permettono di formare una [Botnet](#). Possiedono inoltre migliori funzioni e opzioni per nascondersi nel computer ospite, utilizzando tecniche di [Rootkit](#).



Virus

Infected files



Virus

Da Wikipedia, l'enciclopedia libera.

Un **virus**, in **informatica**, è un **software** appartenente alla categoria dei **malware** che, una volta eseguito, infetta dei **file** in modo da fare copie di se stesso, generalmente senza farsi rilevare dall'**utente**. Il termine viene usato per un programma che si integra in qualche codice eseguibile (incluso il sistema operativo) del sistema informatico vittima, in modo tale da diffondersi su altro codice eseguibile quando viene eseguito il codice che lo ospita, senza che l'utente ne sia a conoscenza.

I virus entrano nel computer sfruttando le vulnerabilità (**exploit**) dell'applicazione o del **sistema operativo** e arrecando danni al sistema, rallentando o rendendo inutilizzabile il dispositivo infetto. I virus comportano dunque un certo spreco di risorse in termini di **RAM**, **CPU** e spazio sul **disco fisso**. Come regola generale si assume che un virus possa danneggiare direttamente solo il software della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all'**hardware**, ad esempio causando il surriscaldamento della CPU mediante **overclocking**, oppure fermando la ventola di raffreddamento. La parola è spesso erroneamente utilizzata in **sineddoche** per parlare di **malware**. Ne è un esempio il diffuso termine *antivirus*.



Vorm

Creeper, Reaper, Morris Worm



Worm

Da Wikipedia, l'enciclopedia libera.

Un **worm** (termine della [lingua inglese](#) tradotto letteralmente in "verme"), nella [sicurezza informatica](#), è una particolare categoria di [malware](#) in grado di autoreplicarsi.

Uno dei primi worm di epoca moderna diffusi sulla rete fu il [Morris worm](#), creato da [Robert Morris](#), figlio di un alto dirigente della [NSA](#) il 2 novembre [1988](#), quando [internet](#) era ancora agli albori. Tale virus riuscì a colpire tra le 4000 e le 6000 macchine, si stima il 4-6% dei computer collegati a quel tempo in rete^[3].

È simile ad un [virus](#) ma, a differenza di questo, non necessita di legarsi ad altri [programmi eseguibili](#) per diffondersi, ma a tale scopo utilizza altri [computer](#), ad esempio tramite [e-mail](#) e una [rete di computer](#).^[4]

Il mezzo più comune impiegato dai worm per diffondersi è la posta elettronica: il Programma maligno ricerca indirizzi e-mail memorizzati nel computer ospite ed invia una copia di sé stesso come file allegato (*attachment*) a tutti o parte degli indirizzi che è riuscito a raccogliere. I messaggi contenenti il worm utilizzano spesso tecniche di social engineering per indurre il destinatario ad aprire l'allegato.



<https://www.kaspersky.it/blog/il-worm-morris-compie-25-anni/1986/>



Spoofing

Falsificazione dell'identità



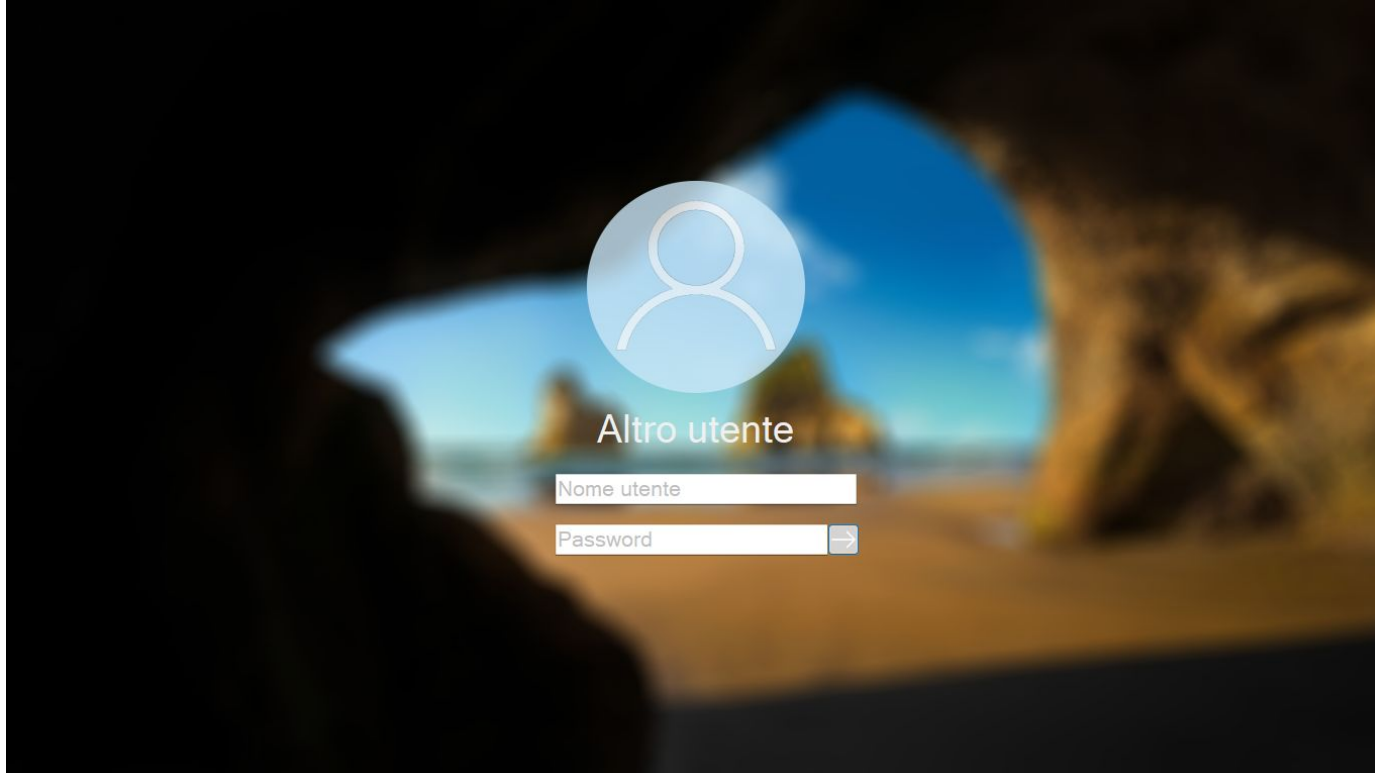
Spoofing

Da Wikipedia, l'enciclopedia libera.

Lo **spoofing** è un tipo di [attacco informatico](#) che impiega in varie maniere la falsificazione dell'identità (*spoof*). Lo spoofing può avvenire a qualunque livello della pila [ISO/OSI](#) e può riguardare anche la falsificazione delle informazioni applicative.

Questa tecnica di attacco può essere utilizzata per falsificare diverse informazioni, come ad esempio l'identità di un host all'interno di una rete o il mittente di un messaggio. Una volta che un attaccante riesce ad impersonare qualcun altro all'interno di una rete gli è possibile intercettare informazioni riservate, diffondere informazioni false e tendenziose o effettuare qualsiasi tipo di attacco. Risulta particolarmente efficace combinata a tecniche di [social engineering](#) per ottenere l'accesso ad informazioni "riservate" e credenziali degli utenti. Social media scammers o phishers possono usare questa tecnica ad esempio per convincere un utente a connettersi ad un server malevolo intercettando così le sue credenziali.

Login Spoofing (esempio)



Login Spoofing (esempio)

1. L'attaccante entra nel proprio account ed esegue il proprio programma di spoofing (login identica all'originale)
2. L'attaccante lascia la postazione in attesa della vittima
3. La vittima di fronte alla presunta schermata di login inserisce le proprie credenziali non accorgendosi dell'inganno (login identica all'originale)
4. Il programma acquisisce i dati inseriti e li salva nell'account dell'attaccante
5. Il programma informa l'utente di un errore di autenticazione
6. Il programma esegue la disconnessione dall'account dell'attaccante ri-presentando la schermata (questa volta originale) di login
7. La vittima re-inserisce le credenziali e accede al proprio account senza nessun sospetto



Phishing

Vero o falso?



Phishing

Da Wikipedia, l'enciclopedia libera.

Il **phishing** è un tipo di **truffa** effettuata su **Internet** attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire **informazioni** personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.^{[1][2]}

Il termine phishing è una variante di *fishing* (letteralmente "pescare" in **lingua inglese**),^[3] probabilmente influenzato da *phreaking*.

Si tratta di un'attività illegale che sfrutta una tecnica di **ingegneria sociale**: il malintenzionato effettua un invio massivo di messaggi che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio. Per la maggior parte è una truffa perpetrata usando messaggi di posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali i messaggi SMS.

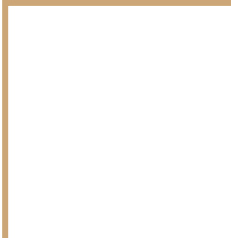
Phishing (esempio)

Sei in grado di
riconoscere i
tentativi di phishing?

Identificare il phishing può essere più difficile di quello che pensi. Il phishing è un tentativo di ingannarti per sottrarti informazioni personali in cui utenti malintenzionati fingono di essere qualcuno che conosci. Riesci a distinguere un messaggio ingannevole?

FAI IL QUIZ

<https://phishingquiz.withgoogle.com/>



Social Engineering

Tecniche psicologiche



Ingegneria sociale

Da Wikipedia, l'enciclopedia libera.

L'**ingegneria sociale** (dall'**inglese** *social engineering*), nel campo della **sicurezza informatica**, è lo studio del **comportamento** di una persona al fine di carpire informazioni utili. Essa è utilizzata soprattutto dagli **hacker** (più in particolare dai cracker) per scoprire **password**, violare **sistemi informatici** e ottenere dati personali importanti di un individuo.

Le fasi dell'attacco [[modifica](#) | [modifica wikitesto](#)]

L'ingegnere sociale comincia con il raccogliere informazioni sulla vittima per poi arrivare all'attacco vero e proprio.

- Durante la prima fase (che può richiedere anche alcune settimane di analisi), l'ingegnere cercherà di ricavare tutte le informazioni di cui necessita sul suo bersaglio: **e-mail**, recapiti telefonici, ecc.

Superata questa fase, detta *footprinting*, l'ingegnere passerà alla fase successiva,

- Seconda fase, l'ingegnere verifica se le informazioni che ha ricavato sono più o meno attendibili, anche telefonando all'azienda del bersaglio e chiedendo cortesemente di parlare con la vittima.
- Terza fase, la più importante, quella che determinerà il successo dell'attacco, è lo studio dello *stile vocale* della persona per la quale vuole spacciarsi (ad esempio cercando di evitare in tutti i modi l'utilizzo di **espressioni dialettali** e cercando di essere quanto più naturale possibile, sempre utilizzando un tono neutro e cortese). In questa fase l'attaccante avrà sempre vicino a sé i propri appunti con tutte le informazioni raccolte nella fase di *footprinting*, dimostrandosi pertanto sicuro nel caso gli venisse posta qualche domanda.

La ricerca si suddivide in due parti: 1. *di contesto*, si trovano tutte quelle informazioni che sono pubbliche e dunque facilmente reperibili, per capire che domande rivolgere e soprattutto a chi. 2. *cumulativa* si raccolgono tutti questi dati e si utilizzano per fare delle richieste maggiormente complesse alla vittima, includendo anche nomi del personale, competenze e tutto il necessario per acquisire più fiducia possibile.^[1]



Kevin Mitnick, autore dei libri *L'arte dell'inganno* e *L'arte dell'intrusione*

L'anello più debole della sicurezza


Un'azienda potrebbe anche essersi dotata delle migliori tecnologie di sorveglianza, avere addestrato i dipendenti a mettere sotto chiave tutti i segreti prima di smontare la sera e assunto guardie giurate della migliore agenzia del settore.

Ed essere ancora vulnerabile.

I singoli individui possono seguire le migliori tattiche consigliate dagli esperti, installare supinamente tutti i prodotti raccomandati, essere assolutamente rigorosi sull'adatta configurazione di sistema e tempestivi nell'apportare le correzioni del caso.

Ma queste persone sarebbero ancora totalmente vulnerabili.

[tratto da: L'arte dell'inganno, Kevin D. Mitnick]



“L’unico vero sistema sicuro è un sistema spento,
chiuso in una gettata di cemento,
sigillato in una stanza rivestita di piombo
protetta da guardie armate.

Ma anche in questo caso ho i miei dubbi.”



[prof. Eugene Howard Spafford (Spaf)]