



Network Security: Vulnerability and Network Attacks

Luca Veltri

(mail.to: luca.veltri@unipr.it)

Corso di Sicurezza nelle reti di telecomunicazioni, a.a. 2008/2009

<http://www.tlc.unipr.it/veltri>



Università degli Studi di Parma
Dipartimento di Ingegneria dell'Informazione

Vulnerability and Network Attacks

Alcune tipologie di attacco

- Password cracking
- Sniffing
- Spoofing
- Flooding
- Routing attacks
- Network scanning
- Application protocol attacks
- Malicious Code
- Bugs
- Social engineering

2



Università degli Studi di Parma
Dipartimento di Ingegneria dell'Informazione

Vulnerability and Network Attacks

Password cracking



- Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system
- Principali metodi di attacco alle password:
 - Weak password encryption
 - Password guessing
 - Password capture
 - Social engineering

3



Università degli Studi di Parma
Dipartimento di Ingegneria dell'Informazione

Vulnerability and Network Attacks

Weak password encryption

- If a system uses a poorly designed password hashing scheme to protect stored passwords, an attacker can exploit any weaknesses to recover even 'well-chosen' passwords
- Password encryption schemes that use stronger hash functions like MD5, SHA-512, SHA-1, can still be vulnerable to brute-force and precomputation attacks
 - Salting prevents precomputation attacks

4

Password guessing

- One of the most common attacks
- Attacker knows a login (from email/web page etc), then attempts to guess password for it
 - try default passwords shipped with systems
 - try all short passwords
 - then try by searching dictionaries of common words
 - Dictionary attack
 - intelligent searches try passwords associated with the user (variations on names, birthday, phone, common words/interests)
 - before exhaustively searching all possible passwords
 - Brute force attack
- Check by login attempt or against stolen password file (online/offline)
 - success depends on password chosen by user
 - surveys show many users choose poorly

5

Password capture

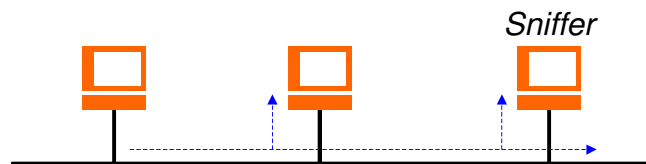
- Another password attack
 - watching over shoulder as password is entered
 - using a trojan horse program to collect
 - monitoring an insecure network login (eg. telnet, FTP, web, email)
 - extracting recorded info after successful login (web history/cache, last number dialed, etc)
- Users need to be educated to use suitable precautions/countermeasures

6

Network Sniffing



- Anche riferito come snooping
- E' alla base di diversi attacchi, soprattutto in ambito LAN e WLAN
- L'attaccante mette la sua interfaccia di rete in promiscuous mode



7

Network Sniffing (cont.)

- Comuni sniffer di rete sono: WireShark (ex Ethereal), tcpdump (unix), Windump (win), netcat, etc.
- I prodotti per Windows in genere si appoggiano alla libreria DLL packet.dll o winpcap
- mentre i prodotti per Unix si appoggiano alla libreria di funzioni libpcap
- Il più usato in ambiente Unix è tcpdump; per usarlo bisogna avere i privilegi di root
- Si definiscono Protocol Analyzer
 - quando hanno funzionalità di analisi del contenuto dei pacchetti intercettati e permettono di riconoscere il dettaglio dei protocolli trasportati

8

Rilevazione di network sniffer

- La loro presenza attiva su di un host può essere rilevata tramite specifici comandi quali:

- **ifconfig**

```
eth0 Link encap:Ethernet HWaddr 00:10:4B:E2:F6:4C
      inet addr:192.168.1.8 Bcast:192.168.1.255 Mask:255.255.255.0
      UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
      RX packets:1016 errors:0 dropped:0 overruns:0 frame:0
      TX packets:209 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
```

- **cpm (Check Promiscuous Mode)**

- **ifstatus**

9

Rilevazione di network sniffer (cont.)

- In alcuni casi la loro presenza in rete può essere rilevata tramite comportamento del Kernel, esempio

- **in alcuni OS**

- quando viene attivata la modalità promiscua (promiscuous mode), vengono accettati pacchetti che hanno un indirizzo Ethernet errato, ovvero differente da quello dell'interfaccia di rete della stazione sotto esame, sebbene l'indirizzo IP di destinazione sia quello corretto

- **in Windows 95, 98, NT**

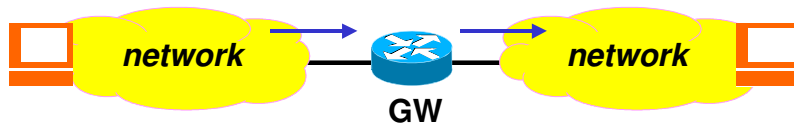
- quando viene attivata la modalità promiscua (promiscuous mode), soltanto il primo otetto di un frame viene verificato per verificare se si tratta di un Ethernet broadcast addresses (ff:00:00:00:00:00 will be accepted)

- AntiSniff tool

10

Man-in-the-middle (MITM)

- L'attaccante ha il controllo di un nodo (e.g. router) o link lungo il percorso tra 2 hosts



- Oltre ad intercettare/sniffare il traffico, l'attaccante può:
 - **bloccare il traffico (DoS)**
 - **ridirigerlo**
 - **modificare il contenuto dei dati**

11

Spoofing



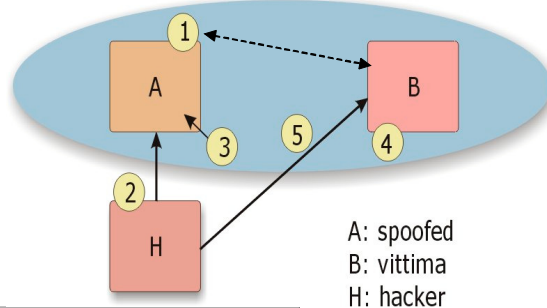
- Attacco dove viene impiegata in qualche maniera la falsificazione dell'identità (spoof)
- Può avvenire a diversi di una architettura protocollare
 - **livello 2 - MAC spoofing**
 - **livello 3 - IP spoofing**
 - **livello 4 - UDP o TCP spoofing**
 - **livello applicativo**
 - webpage spoofing, also known as phishing
 - VoIP Caller ID spoofing
 - E-mail address spoofing

12

Esempio di attacco di tipo spoofing

Ipotesi:

- B ha relazione di fiducia con A, ad esempio basata su IP address



- Selezione del host vittima ed individuazione di una relazione di fiducia rispetto ad un host (trusted host)
- Individuazione del host da impersonare (trusted host)
- Disabilitazione del host che si intende impersonare (DoS)
- Analisi dei pacchetti trasmessi dal host vittima (e.g. analisi dei sequence number), se possibile
- Impersonamento del host per il quale l'host vittima ha una relazione di fiducia (trusted host)

13

Esempio di TCP Spoofing

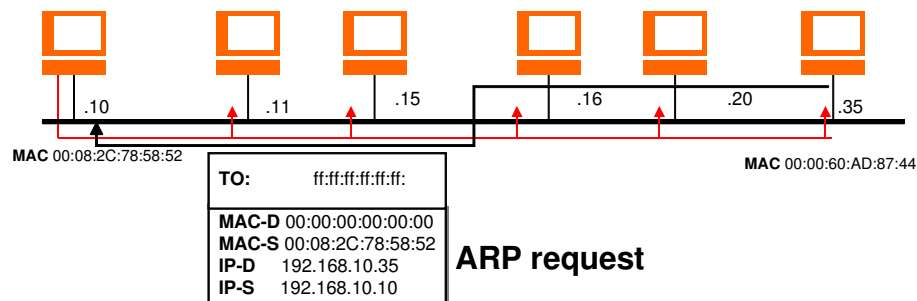
3 way handshake

H	>	SYN	>	B	Inizio connessione
A	<	SYN/ACK	<	B	Risposta vittima verso host trusted/spoofed
H	>	ACK	>	B	Handshake completo
H	>	PSH	>	B	Trasferimento dati

14

Messaggi ARP

Subnet 192.168.10.0/24



ARP request

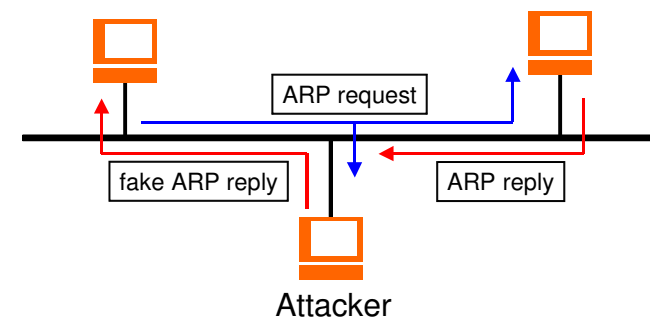
La postazione aggiunge la coppia
MAC/IP alla propria cache

TO:	00:08:2C:78:58:52
MAC-D	00:00:60:AD:87:44
MAC-S	00:08:2C:78:58:52
IP-D	192.168.10.35
IP-S	192.168.10.10

ARP reply

15

ARP Spoofing



Tipi di attacchi possibili:

- Denial-of Service
- Ridirezione del traffico (MITM)

16

Hub Ethernet vs. Switched Ethernet

- Le reti Ethernet di tipo switched non permettono sniffing diretto
- ARP spoofing può essere usato per superare la protezione (MITM)
- Un altro modo è tramite MAC flooding
 - Lo switch viene inondato di indirizzi MAC sino a riempire le tabelle di risoluzione e commutare da "switch" a "hub"

17

IP Spoofing

- Gli attacchi più diffusi che si basano sul protocollo IP utilizzano tecniche di IP spoofing
- Consistono nell'assumere l'indirizzo IP di un'altra entità (Host, server, dispositivo di rete) al fine di acquisirne i diritti
 - l'inserimento di indirizzi IP sorgenti falsificati può consentire l'esecuzione non autorizzata di servizi quali rlogin, rsh, etc.
 - In alcuni casi tramite spoofing si riesce ad aggirare dei firewall
- L'attacco è a volte effettuato sfruttando l'opzione source routing per l'instradamento forzato dei pacchetti:
 - l'instradamento forzato dei pacchetti può consentire di aggirare eventuali firewall mal configurati e penetrare in porzioni di rete protette

18

Flooding



- Flooding attack is an attack that attempts to cause a failure in a computer system or other data processing entity by providing more input than the entity can process properly

19

ICMP Flooding (Smurf) DDoS

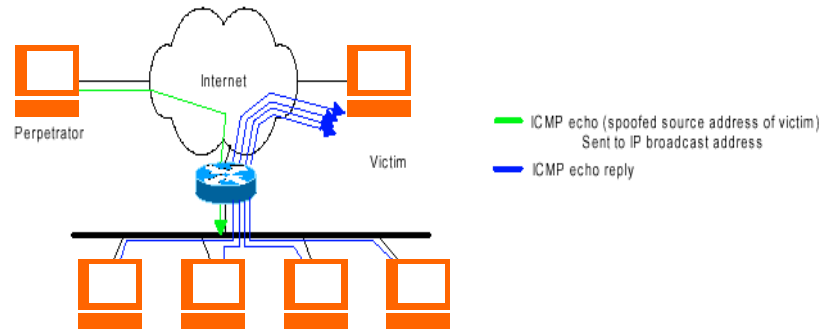
- Network-based, esaurisce le risorse dei collegamenti
- Usa le richieste ICMP echo/reply con reti broadcast per moltiplicare il traffico
- Richiede l'abilità di inviare "spoofed packets"
- Abuso di "bounce-sites" per attaccare vittime
 - Traffico moltiplicato di un fattore da 50 a 200



- L'aggressore invia un grosso flusso di traffico ICMP echo verso una serie di indirizzi di broadcast attribuendosi come indirizzo sorgente quello della vittima. Il traffico viene moltiplicato per il numero di host presenti

20

ICMP Flooding (Smurf)



21

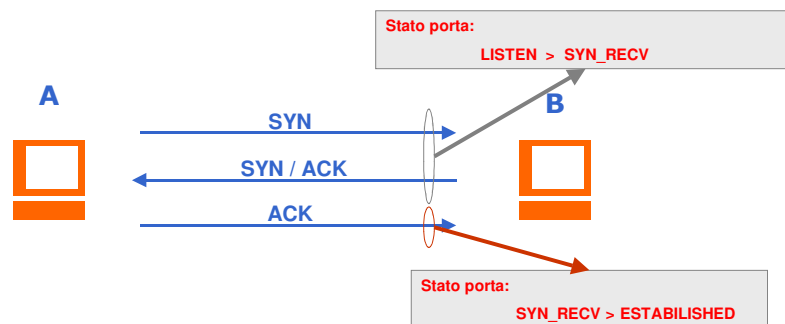
UDP Flooding (Fraggle)

- Il "fraggle" opera esattamente nella stessa maniera, usando però l'UDP echo invece di ICMP echo
- Entrambi gli attacchi danneggiano fortemente sia la vittima che l'intermediario, o amplificatore
- Per evitare di fare da amplificatore si dovrebbe disabilitare su tutti i router presenti sulla rete la propagazione dei broadcast a livello 2 su tutte le interfacce "broadcast enabled" (quali Ethernet, FDDI, FR/ATM in multipoint mode etc.)
 - in alcuni router commerciali il blocco dei broadcast è di default
 - esempio router Cisco a partire dalla IOS 12.0

```
interface Ethernet0
no ip directed-broadcast
```

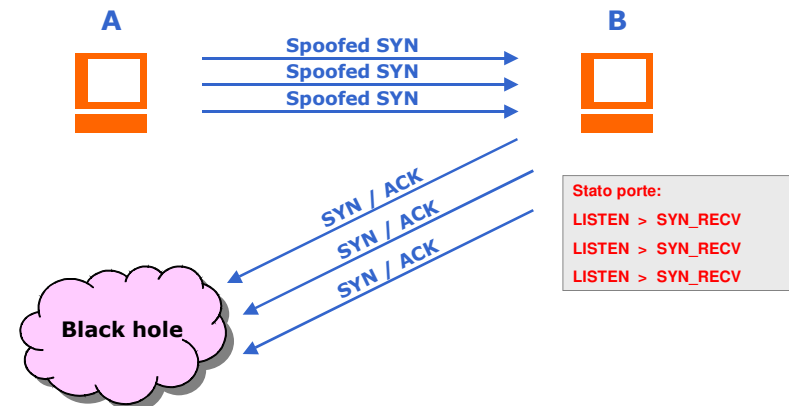
22

Apertura di una connessione TCP



23

(TCP) SYN flood attack



24

Routing attacks

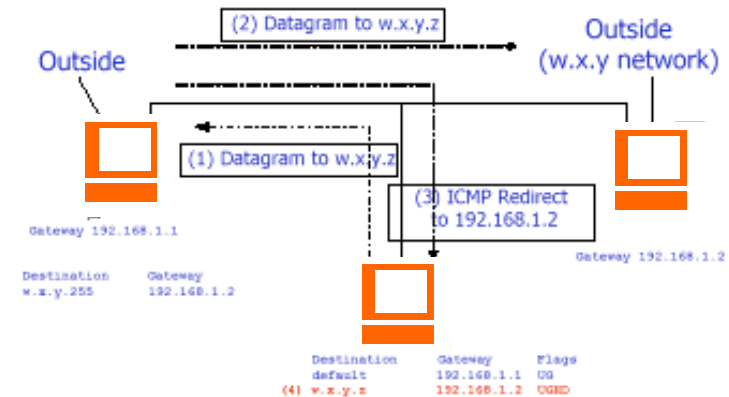


- Attacchi che sfruttano i meccanismi e protocolli di routing per ridirigere o bloccare il traffico di rete
- Possono operare a vari livelli protocollari:
 - livello 2 - e.g. tramite ARP spoofing
 - livello 3 - attaccando i protocolli di controllo ICMP e IGMP, o i protocolli di routing RIP e OSPF
 - livello applicativo - e.g. attacchi basati su DNS poisoning

25

ICMP Redirect

- ICMP Redirect può essere usato per costruire un attacco di tipo "Man in the Middle" e/o per ovviare alla presenza di switch a livello 2



26

ICMP Destination unreachable

- Messaggi ICMP inviati da router per indicare che un datagramma non può essere rinviato
- Diversi sottotipi:
 - Network unreachable
 - Host unreachable
 - Protocol unreachable
 - Port unreachable
 - Fragmentation needed but don't fragment bit set
 - Destination host unknown
 - Destination network unknown
- ICMP Destination unreachable può essere usato per costruire un attacco di tipo DoS, o come ausilio per altri tipi di attacchi (e.g. spoofing di una terza macchina)

27

Network scanning



- Activity through specific software for scanning a network for discovering active hosts and open ports (Port scanning)
- This is often used by administrators to check the security of their networks and by hackers to identify running services on a host with the view to compromising it
- Related to network scanning are:
 - Vulnerability scanning
 - Penetration test
- Esempio di applicativo di network scanning:
 - nmap
- Esempio di applicativo di vulnerability scanning:
 - nessus

28

Network scanning tramite ICMP Echo Request

- Messaggi ICMP Echo Request possono essere usati per effettuare una scansione di rete (pingscan)
 - **ICMP echo datagrams are sent to all the hosts in a subnetwork**
 - **The attacker collects the replies and determines which hosts are actually alive**

Starting nmap V. 2.12 by Fyodor (www.insecure.org/nmap/)

Host cisco-sales.ns.com (195.121.31.11) appears to be up.

Host sales1.ns.com (195.121.31.19) appears to be up.

Host sales4.ns.com (195.121.31.22) appears to be up.

Host sales2.ns.com (195.121.31.43) appears to be up.

Host sales3.ns.com (195.121.31.181) appears to be up.

Nmap run completed -- 256 IP addresses (5 hosts up) scanned in 1 second

29

Host scanning tramite TCP SYN/ACK/RST

- Tramite la richiesta di apertura di connessioni TCP su un intervallo di porte di un host è possibile monitorare i servizi eventualmente attivi
 - **user space: tramite TCP connect() (SYN/SYN-ACK/ACK/FIN)**
 - **root space: tramite invio di TCP SYN/ACK/RST**

30

Application protocol attacks



- Attacco a specifiche applicazioni e protocolli (DNS, Mail, FTP, etc.)
- Alcuni esempi:
 - **Posta elettronica**
 - mail spamming
 - mail spoofing
 - mail phishing
 - **DNS**
 - Pharming is a hacker's attack aiming to redirect a website's traffic to another, bogus website
 - can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software
 - DNS cache poisoning
 - the attacker exploits a flaw in the DNS software that can make it accept incorrect information

31

Host misconfiguration attacks

- Attacchi a protocolli di configurazione quali BOOTP/DHCP
- Questi protocolli (basati su UDP) sono vulnerabili ad attacchi di spoofing
- Possono essere usati per configurare un diverso default gateway e ridirigere il traffico
 - **Man in the middle, Hijacking**
- Possono essere usati per configurare un diverso default DNS server

32

Malicious Code: Viruses, Worms, etc. ✓

- Computer “**Viruses**” and related programs have the ability to replicate themselves on an ever increasing number of computers
 - **They originally spread by people sharing floppy disks**
 - **Now they spread primarily over the Internet (a “Worm”)**
- Other “**Malicious Programs**” may be installed by hand on a single machine
 - **They may also be built into widely distributed commercial software packages**
 - **These are very hard to detect before the payload activates (Trojan Horses, Trap Doors, and Logic Bombs)**

33

Definitions (1/2)

- **Virus** - code that copies itself into other programs
- **Worm** - a program that replicates itself across the network (usually riding on email messages or attached documents (e.g., macro viruses)
- **Trojan Horse** - instructions in an otherwise good program that have a different and hidden purpose (sending your data or password to an attacker over the net)
- **Trap Door (or Back Door)** - undocumented entry point written into code for debugging that can allow unwanted users

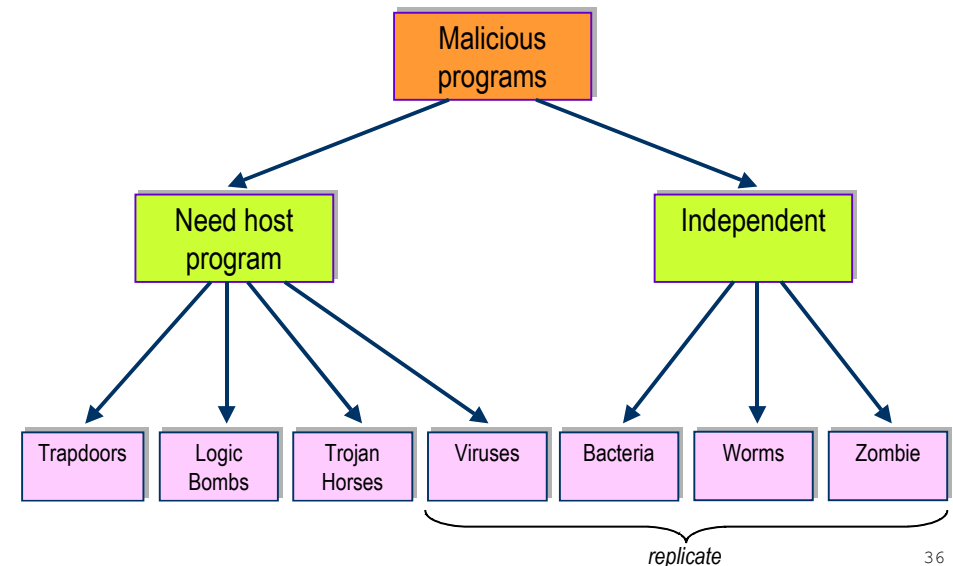
34

Definitions (2/2)

- “**Bacteria**” - malicious code that replicates until it fills all disk space, or exhausts some resource
- **Logic Bomb** - malicious code that activates on an event (e.g., date)
- **Easter Egg** - extraneous code that does something “cool.” A way for programmers to show that they control the product
- **Zombie** - program which secretly takes over another networked computer; then uses it to indirectly launch attacks

35

Taxonomy



36

Worms

- replicating but not infecting program
- typically spreads over a network
 - e.g. **Morris Internet Worm in 1988**
 - **led to creation of CERTs**
- using users distributed privileges or by exploiting system vulnerabilities
- widely used by hackers to create zombie PC's, subsequently used for further attacks, e.g. DoS
- major issue is lack of security of permanently connected systems, esp PC's

37

Worm Operation

- worm phases like those of viruses:
 - **dormant**
 - **propagation**
 - search for other systems to infect
 - establish connection to target remote system
 - replicate self onto remote system
 - **triggering**
 - **execution**

38

Bugs: Buffer Overflow



```
char sample[10]
```

- The C compiler sets aside 10 bytes to store this buffer, `sample[0]` through `sample[9]`
- Now execute the statement:

```
sample[i] = 'A'; // i = 10
```
- The 'A' may overwrite user code or data or spill into a memory area being used by the operating system
- By carefully choosing what is written, you can overwrite part of the OS or application with your own code
- You can overwrite both data and/or executable code
- Especially vulnerable: OS routines that use `strcpy` instead of `strncpy`

39

Stack Overflow

- Subroutine calls are executed with the help of a runtime stack
- The activation record (or frame, containing the parameters, local variables and return address) for the most recently called procedure is pushed on the stack
- By entering long unchecked parameters, the attacker can manipulate the return address
- If the procedure was a system routine running with root privileges, the attacker can get those privileges

40

Social Engineering



- Metodo utilizzato per convincere qualcuno a rivelare dati sensibili
 - attraverso l'interazione con altri esseri umani (conversazione telefonica, email, dal vivo, etc)
 - basato su trucchi psicologici
- Il Social Engineering si basa su due assiomi fondamentali:
 - 1. **gli esseri umani sono esseri molto fiduciosi nel prossimo e tendono a credere a ciò che si dice loro**
 - 2. **Sebbene un computer memorizza molto bene le informazioni, un essere umano è il soggetto migliore per fornirle ad altri**
- L'arte del Social Engineering è ancor più antica di quella dell'hacking
 - **I primi che la utilizzarono estesamente furono i phreaker per riuscire a carpire informazioni sensibili dalle compagnie telefoniche**
- Molti hacker conosciuti per i loro skill tecnici erano primariamente degli ottimi social engineering (e.g. Kevin Mitnick)

41

Social Engineering

- "Tools" utilizzati
 - telefono cellulare/fisso, e/o telefono pubblico
 - fax
 - connessione a internet
 - server di posta elettronica
 - stampante, scanner, un buon programma di fotoritocco
 - etc.
 - ..ma soprattutto, ottima capacità di persuasione e fantasia

42

Possibili contromisure a vari tipi di attacchi

- Cifratura
- Autenticazione
- Controllo accessi
- Auditing e intrusion detection (IDS)
- Virus scanner e disinfectors
- Backup
- Aggiornamento del software
- Architetture di rete sicure (VPN, Firewall)
- etc.



Gestione della sicurezza

43