Network Security: Vulnerability and Network Attacks

Luca Veltri

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

Corso di Sicurezza nelle reti, Reti di telecomunicazioni C, a.a. 2009/2010

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

Vulnerabilities and Network Attacks

- Esistono differenti tipologie di vulnerabilità e di attacchi che possono essere eseguiti in una rete
- In genere gli obiettivi di un attacco includono:
  - **acquisizione indebita di informazioni e dati di vario tipo**
    - violazione della confidenzialità, autenticità delle parti
  - **danneggiamento o impedimento di un servizio**
    - violazione della disponibilità
  - **impersonificazione di una entità (per ottenere alcuni vantaggi)**
    - violazione della autenticità delle parti e/o dei dati

Vulnerabilities and Nettwork Attacks (cont.)

- Tecniche di attacco includono:
  - **violazione dei sistemi di autenticazione (e criptggio)**
    - password cracking, guessing
  - **attacco ai sistemi di istradamento e/o intercettazione di dati**
    - network eavesdropping (sniffing)
    - spoofing
    - redirection and routing attacks
  - **attacchi distribuiti a servizi o risorse di rete**
    - network flooding, Distributed Denial of service (DDoD)
  - **scansione delle risorse di rete e possibili vulnerabilità (network scanning)**
  - **sfruttamento di vulnerabilità**
    - di protocolli
    - di programmi (bachi)
  - **utilizzo di software malevoli (malware)**
  - **social engineering**

Password cracking

- Per password cracking si intende il processo che porta alla scoperta di password a partire da dati ottenuti indebitamente da archivi o catturadi durante una comunicazione
- Principali metodi di attacco alle password:
  - **Weak password encryption**
  - **Password guessing**
  - **Password capture**
  - **Social engineering**

Password cracking: weak pwd 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**

Password cracking: pwd guessing

- 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)**
  - **exhaustively searching all possible passwords**
    - Brute force attack
- Check by login attempt or against stolen password file (online/offline)
  - **success often depends on password chosen by user**
    - surveys show many users choose poorly

Password cracking: pwd capture

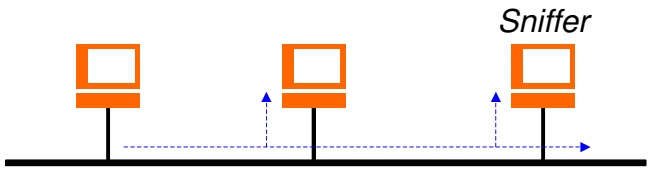
- Password is obtained by capturing during its usage or transmition
  - **watching over shoulder as password is entered**
  - **using a trojan horse program to collect**
  - **monitoring an insecure network login (e.g. FTP, web, email, etc.)**
  - **extracting recorded info after successful login (web history/cache, last number dialed, etc)**
- Users need to be educated to use suitable precautions and countermeasures

Network eavesdropping

- Network eavesdropping or network sniffing is an attack consisting of capturing packets from the network transmitted by others' nodes and reading the data content in search of sensitive information like passwords, session tokens, or any kind of confidential information.
- The attack could be done by using tools called network sniffers (or protocol analyzers)
  - these tools collect packets on the network and, depending on the quality of the tool, analyze the collected data like protocol decoders or stream reassembling
- Work in passive mode
  - packets are simply captured, copied, and passed at user level for further analysis
  - requires to be along the path or a broadcasting domain

Network eavesdropping (cont.)

- Per catturare pacchetti diretti ad altri nodi l'attaccante deve trovarsi lungo il percorso, oppure collegato ad un dominio di rete di tipo broadcast, e.g.
  - **non-switched LAN (LAN with HUBs)**
  - **wireless LAN**
- L'attaccante mette la sua interfaccia di rete in promiscuous mode e cattura tutti i pacchetti che transitano su di essa



Network eavesdropping (cont.)

- Sniffer usage with LANs
  - **LAN with HUBs**
    - the ideal case because the hub duplicates every frame to all interfaces (ports)
  - **LAN with switches**
    - a switch by default only transmits a frame to the destination port
    - sometimes by flooding a switch with a lare amount of frames (MAC flooding) makes the device to switch from partitioning to broadcasting mode (fail-open mode)
    - arp spoof attack can be used to redirect the traffic from one port to another; then the evil system may acts like a router between the source and destination (Man-In-The-Middle attack)
  - **Wireless LAN**
    - sniffing is possible if no encryption is used or if a crack attack is performed against the WEP key (scenario becomes equivalent to LAN wtih HUBs)
    - otherwise, the WLAN is similar to a switched LAN

Sniffer

- I più comuni sniffer di rete (o protocol analyzer) sono
  - **WireShark (ex Ethereal)**
    - con interfaccia grafica e
  - **tcpdump (unix)**
    - funziona a riga di comando
- I prodotti per Windows in genere si appoggiano alla libreria DLL packet.dll o winpcap
- I prodotti per Unix in genere si appoggiano alla libreria di funzioni libpcap
  - **il tool più usato è tcpdump**
- Di entrambe le librerie esiste anche un porting in Java (jpcap)
- In genere per usarli bisogna avere i privilegi di root/admin

Rilevazione di network sniffer

- La loro presenza attiva può essere rilevata
  - **tramite specifici comandi direttamente sul nodo che li ospita e.g.:**
    - 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
```

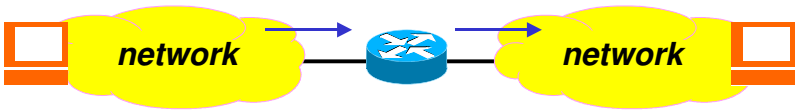
    - cpm (Check Promiscuous Mode)
    - ifstatus
  - **utilizzando appositi tool (AntiSniff) che sfruttano comportamenti particolari a livello di OS**

Rilevazione di network sniffer (cont.)

- Esempi di alcuni comportamenti che possono essere utilizzati per rilevare la presenza di sniffer:
  - **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 veniva attivata la modalità promiscua (promiscuous mode), soltanto il primo ottetto di un frame viene verificato per verificare se si tratta di un Ethernet broadcast addresses (ff:00:00:00:00:00 will be accepted)

Packets interception (MITM)

- L'utilizzo di network sniffer su interfacce di rete lungo il percorso non è l'unico modo con cui si possono intercettare dei pacchetti
- Altre tecniche possono utilizzare
  - **il controllo di un nodo lungo il percorso tramite il quale si intercettano i pacchetti o ridirigono verso un altro nodo**
  - **sfruttando funzionalità offerte dai meccanismi o protocolli di risoluzione di indirizzi o di routing**
    - e.g. ARP spoofing, ICMP redirect, DNS record poisoning, etc.
- In questo modo l'attaccante oltre a catturare i pacchetti può anche modificarli
  - **Man-In-The-Middle attack (MITM)**

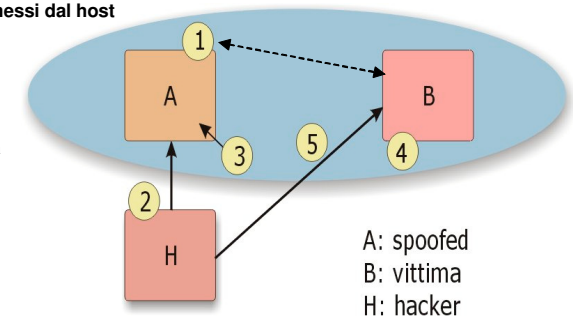


Spoofing

- Attacco dove viene impiegata in qualche maniera la falsificazione di una identità informatica (spoof)
- Può avvenire a diversi livelli 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
- Se l'identità falsificata è quella reale allora si parla più propriamente di social engineering

Esempio di attacco di tipo spoofing

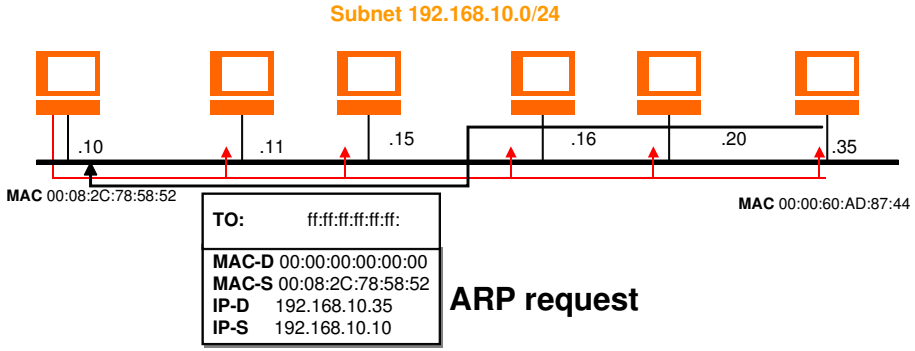
- In generale un attacco di spoofing prevede di inviare dati con mittente falsificato
- In molti casi è necessario catturare (quando possibile) o prevedere eventuali messaggi di risposta
- Per avere effetto si deve:
  1) **Selezione del host vittima ed individuazione di una relazione di fiducia rispetto ad un host (trusted host)**
  2) **Individuazione del host da impersonare (trusted host)**
  3) **Disabilitazione del host che si intende impersonare (DoS)**
  4) **Analisi dei pacchetti trasmessi dal host vittima (e.g. analisi dei sequence number), se possibile**
  5) **Impersonamento del host per il quale l'host vittima ha una relazione di fiducia (trusted host)**



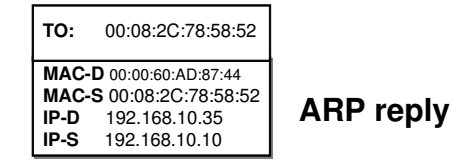
ARP Spoofing

- ARP spoofing è un tipo di attacco che consente in una switched-LAN di realizzare un MITM verso qualsiasi stazione della LAN
  - **è la principale tecnica di attacco nelle switched-LAN (quasi tutte oggigiorno), in cui non è possibile effettuare sniffing diretto**
  - **utile anche in LAN con hub poiché permette oltre che di catturare i paccheti di realizzare un MITM**
- Consiste nell'inviare intenzionalmente e in modo forzato risposte ARP con una falsa corrispondenza IP address → MAC address
  - **la tabella ARP (ARP cache) di un host conterrà dati alterati**
  - **tale tecnica è anche riferita come ARP poisoning**
  - **lo scopo di questo tipo di attacco è quello di redirigere i pacchetti verso un altra stazione**
    - i pacchetti posso essere quindi letti in modo illegittimo; opzionalmente rilanciati inalterati o modificati verso la destinazione
- ARP spoofing è utilizzato in modo legittimo da sistemi come Capitve Portal

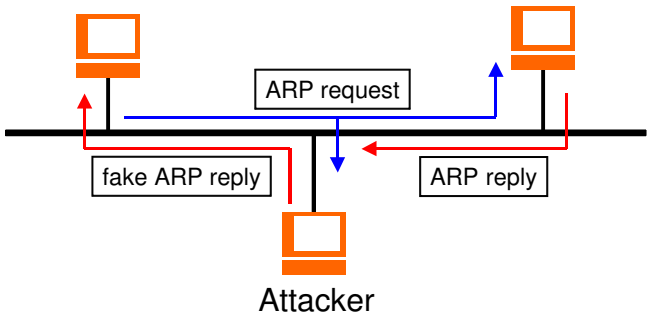
ARP Spoofing: ARP standard



La postazione aggiunge la coppia MAC/IP alla propria cache



ARP Spoofing (cont.)



IP Spoofing

- Consiste nel falsificare l'identità di un host inviando pacchetti IP con indirizzo di sorgente falsificato pacchetto IP nel quale viene falsificato
  - **in genere si utilizza l'indirizzo di una vittima di cui si vuole assumere l'identità ed eventuali diritti**
  - **può consentire l'esecuzione non autorizzata di servizi quali rlogin, rsh, etc.**
  - **In alcuni casi si riesce ad aggirare dei firewall**
- Utilizzabile con efficacia in attacchi
  - **MITM**
  - **DoS/DDoS**
- Può essere utilizzato in combinazione con l'opzione source routing
  - **può consentire di aggirare eventuali firewall mal configurati**

TCP spoofing

- Consiste nel cercare di istaurare una connessione TCP falsificando il proprio indirizzo TCP (IP address + port)
- Decisamente più complesso rispetto al semplice IP spoofing poiché richiede che venga conclusa con successo la procedura di instaurazione della connessione TCP (three way handshake)
  - **viene forgiato un pacchetto TCP SYN con l'indirizzo IP falsificato e questo viene inviato ad un server**
  - **il server risponde con un TCP SYN/ACK inviato all'indirizzo IP falsificato**
  - **il client invia un TCP ACK che deve confermare il sequence number del messaggio TCP precedete**
- Per inviare questo messaggio l'attaccante deve:
  - **trovarsi in configurazione MITM o comunque poter intercettare i pacchetti inviati dal server, oppure**
  - **riuscire ad predire tale sequence number (blind spoofing), sfruttando info di precedenti connessioni e del OS**

TCP Spoofing (cont.)

- TCP 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**

Denial of Service (DoS)

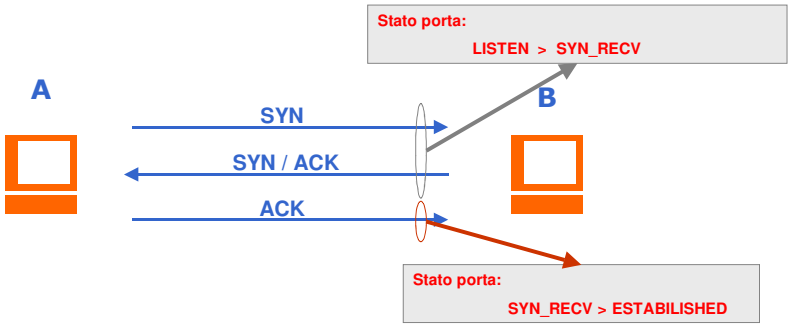
- Si cerca di impedire un servizio
- In questo tipo di attacco in genre si cerca di portare il funzionamento di un sistema, ad esempio un sito web, al limite delle prestazioni, fino a renderlo non più in grado di erogare il servizio
  - **Flooding attack**
- Possono essere eseguiti
  - **da un singolo host**
    - e.g. Syn-Flood
  - **oppure sfruttando la collaborazione (volontaria o involontaria) di numero anche elevato di host**
    - e.g. Smurf
- Nel secondo caso si parla di Distributed DoS (DDoS)

DoS: SYN flood

- Attacco di tipo DoS nel quale un utente malevolo invia una serie di richieste TCP SYN verso il sistema obiettivo dell'attacco
  - **attacco molto famoso ma per fortuna poco efficace nei sistemi più moderni**
  - **funziona se un server alloca delle risorse dopo aver ricevuto un SYN, ma prima di aver ricevuto un messaggio ACK**

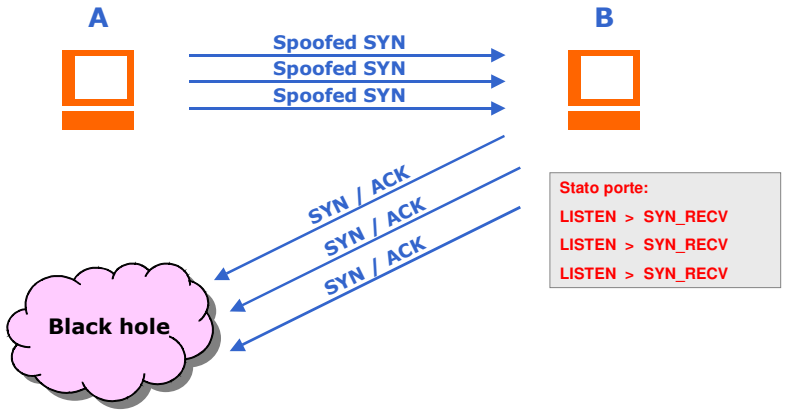
DoS: SYN flood (cont.)

- TCP three-way handshake e comportamento del server TCP



DoS: SYN flood (cont.)

- TCP SYN flooding attack:

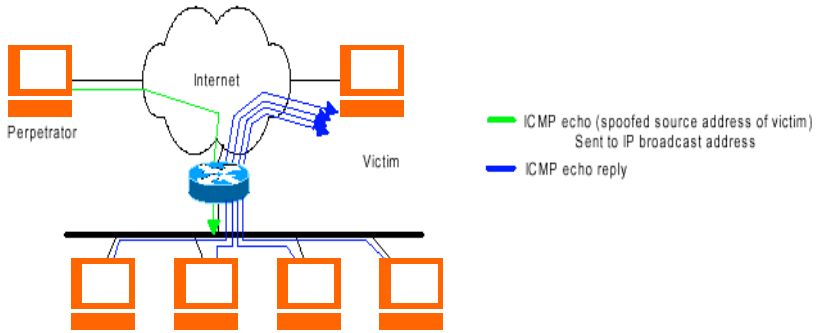


DDoS: ICMP Flooding (Smurf)

- 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
  - **smurf amplifier**
  - **traffico moltiplicato di un fattore da 50 a 200**
- L'aggressore invia un grosso flusso di messaggi ICMP echo request verso una serie di indirizzi di broadcast attribuendosi come indirizzo sorgente quello della vittima
  - **gli host risponderanno con dei messaggi di ICMP echo reply inviati all'indirizzo IP sorgente indicato nella ICMP echo request**
  - **il traffico viene moltiplicato per il numero di host che rivono la request**

DDoS: Smurf (cont.)



DDoS: UDP Flooding (Fraggle)

- Il "Fraggle" opera esattamente nella stessa maniera, usando però l'UDP echo invece di ICMP echo
  - **UDP port 7 (echo)**
  - **UDP port 19 (chargen)**
- Entrambi gli attacchi (basati su ICMP o UDP) 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 di broadcast su tutte le interfacce in cui è possibile broadcast a livello 2 (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

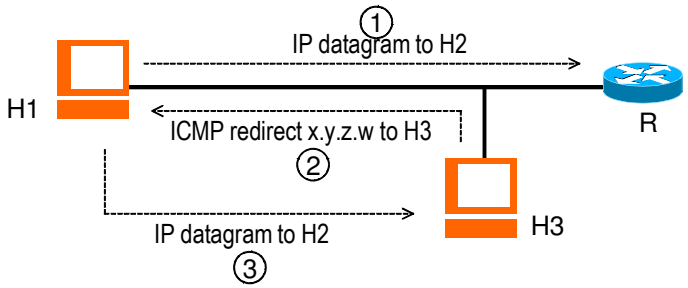
```
interface Ethernet0
    no ip directed-broadast
```


Routing attacks

- Attacchi che sfruttano debolezze deii meccanismi e protocolli di routing per ridirigere o bloccare il traffico di rete
- Possono attaccare meccanismi di risoluzione di indirizzi (e.g. ARP o DNS) configurazione (BOOTP/DHCP) o di routing in senso stretto
- 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

Routing attacks: ICMP Redirect

- ICMP Redirect può essere usato per costruire un attacco di tipo MITM
  - **alternativa rispetto a soluzioni tipo ARP spoofing**



Routing attacks: 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)

Routing attacks: BOOTP/DHCP attack

- 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

Network scanning

- Also refereed as Network enumerating
- Activity through specific software for scanning a network for discovering active hosts and open ports (Port scanning)
  - **e.g. ping, traceroute, nmap**
- This is often used by administrators to check the security of their networks
- Can be used by hackers to identify running services on a host with the view to compromising it
- Related to network scanning are:
  - **Vulnerability scanning**
  - **Penetration test**

Network scanning (cont.)

- What a network scanner can do
  - **Host Discovery**
    - identifying hosts on a network, for example listing the hosts which respond to pings, or which have a particular port open
  - **Port Scanning**
    - enumerating the open ports on one or more target hosts
  - **Version Detection**
    - interrogating listening network services listening on remote devices to determine the application name and version number
  - **OS Detection**
    - remotely determining the operating system and some hardware characteristics of network devices

Host Discovery

- Host discovery may be performed by using different techniques
  - **ICMP scan**
    - determines if a host responds to ICMP requests, such as echo (ping), netmask, etc
  - **TCP SYN/ACK/RST**
    - tries to open a TCP connection using port numbers
      - associtated to most common application services (e.g. HTTPd), or
      - by a given set
    - two modes (see later):
      - user space (TCP connect())
      - root space (TCP SYN/ACK/RST)

Port scanning

- A port scanner may scan
  - **the most common port numbers, or**
  - **ports most commonly associated with vulnerable services, on a given host, or**
  - **a given list of TCP and UDP port numbers**
- The result of a scan on a target {host,proto,port} can be:
  - **Open or Accepted**
    - the host sent a reply indicating that a service is listening on the port
    - open ports may revel vulnerabilities associated with
      - the program responsible for delivering the service
      - the operating system that is running on the host
  - **Closed or Denied or Not Listening**
    - the host sent a reply indicating that connections will be denied to the port
  - **Filtered, Dropped or Blocked**
    - there was no reply from the host

Port scanning (cont.)

- Port scanning types:
  - **TCP scanning**
    - the simplest port scanners
    - use the operating system's network functions (e.g. connect() call)
    - if a port is open, the operating system completes the TCP three-way handshake, and the port scanner immediately closes the connection; otherwise an error code is returned
    - has the advantage that the user does not require special privileges
    - however, it prevents low-level control
  - **SYN scanning**
    - the port scanner generates raw IP packets itself (TCP SYN packet), and monitors for responses (TCP SYN-ACK packet), rather than use the operating system's network functions
    - the scanner responds with a TCP RST packet, closing the connection before the handshake is completed
    - also known as "half-open scanning", because it never actually opens a full TCP connection

Port scanning (cont.)

- Port scanning types: (cont.)
  - **UDP scanning**
    - if a UDP packet is sent to a port that is not open, some systems respond with an ICMP port unreachable message
    - an alternative approach is to send application-specific UDP packets, hoping to generate an application layer response
  - **ACK scanning**
    - it does not exactly determine whether the port is open or closed, but whether the port is filtered or unfiltered
- There is debate over which scan is less intrusive on the target host between TCP connect or TCP SYN scans
  - **SYN scan has the advantage that the individual services never actually receive a connection while some services can be crashed with a connect scan**
  - **however, the RST during the handshake can cause problems for some network stacks, in particular simple devices like printers**

Port scanning (cont.)

- There is debate over which scan is less intrusive on the target host between TCP connect or TCP SYN scans
  - **SYN scan has the advantage that the individual services never actually receive a connection while some services can be crashed with a connect scan**
  - **however, the RST during the handshake can cause problems for some network stacks, in particular simple devices like printers**

Port scanning: 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

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

Malicious software (Malware)

- Malware (malicious software) è genericamente un software progettato per infiltrarsi in un sistema (e.g. PC o smartphone) in modo inconsapevole rispetto al proprietario del sistema
  - **e.g. virus, worm, trojan horse, spyware, dishonest adware, rootkit, etc.**
  - **il termine "virus" è spesso utilizzato come sinonimo per indicare un generico malware, oltre che un particolare tipologia di malware (virus)**

Malware: Virus, Worm, etc.

- Virus
  - **sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene eseguito**
  - **si trasmettono tramite lo spostamento di file infetti ad opera degli utenti**
- Worm
  - **malware che non hanno bisogno di infettare altri file perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet**
  - **per indurre gli utenti ad eseguirli utilizzano tecniche di social engineering, oppure sfruttano dei difetti (bug) di alcuni programmi per diffondersi automaticamente**

Malware: Virus, Worm, etc. (cont.)

- Trojan horse
  - **software che contiene istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore**
  - **in genere non possiede funzioni di auto-replicazione, quindi per diffondersi deve essere scambiato insieme al programma che lo ospita**
- Backdoor
  - **sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione**
  - **tipicamente si diffondono in abbinamento ad un trojan o un worm**
- Spyware
  - **software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato**
    - e.g. doc e programmi usati, siti navigati, password, chiavi crittografiche, etc.

- Dialer
  - **si occupano di gestire di nascosto e in modo fraudolento la connessione ad Internet tramite linea telefonica (PSTN o UMTS)**
- Rootkit
  - **i rootkit solitamente sono composti da un driver e, a volte, da delle copie modificate di programmi normalmente presenti nel sistema. I rootkit non sono dannosi in se ma hanno la funzione di nascondere, sia all'utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare spyware e trojan.**
- Adware
  - **programmi software che presentano all'utente messaggi pubblicitari durante l'uso**
  - **possono causare danni quali rallentamenti del pc e rischi per la privacy in quanto possono comunicare le abitudini di navigazione ad un server remoto**

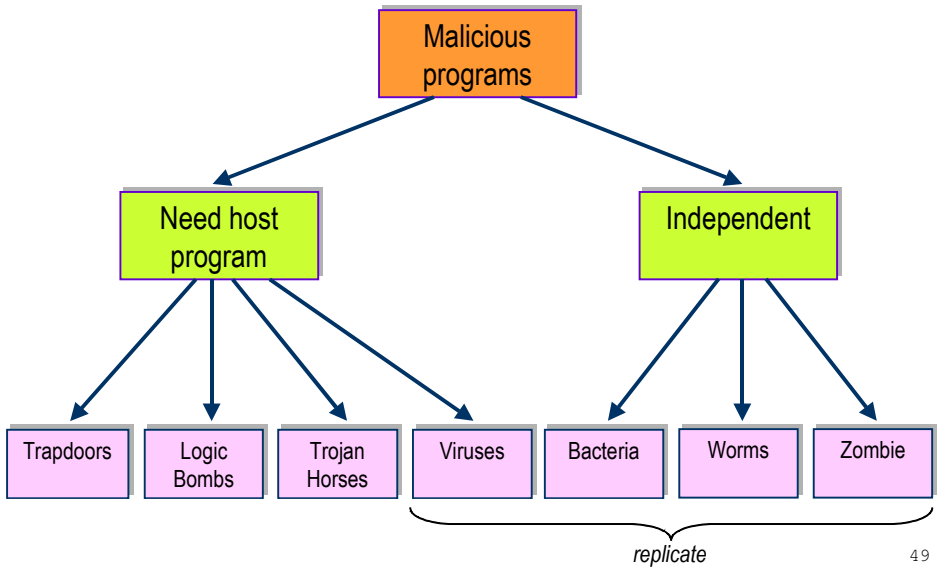
Definitions (1/2)

- 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

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

Taxonomy



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

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**

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`

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

Social Engineering

- Metodo utilizzto per convincere qualcuno a rilevare dati sensibili
  - **attraverso l'interazione con altri esseri umani (conversazione telefonica, email, dal vivo, etc)**
  - **basato su trucchi psicologici**
- Si basa principalmente sulla tendenza delle persone a avere fiducia nel prossimo, e sulla particolare capacità dell'attaccante nello sfruttare questo a suo vantaggio
- 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

Social Engineering (cont.)

- Strumenti utilizzati
  - **ottime conoscenze tecnologiche**
  - **telefono privato o pubblico**
  - **fax**
  - **mail**
  - **fotoritocco**
  - **etc.**
  - **..ma soprattutto, ottima capacità di persuasione e fantasia**

Possibili contromisure a vari tipi di attachi

- Strumenti crtittografici
  - **cifratura**
  - **autenticazione delle parti**
  - **MAC**
  - **firma digitale**
- Protocolli
  - **IPSec, TLS, AAA, etc.**
  - **X.509, S/MIME, etc.**
- Meccanismi di protezione di rete e dei sistemi
  - **Firewalll**
  - **Intrusion detection Systems (IDSs)**
  - **Virus scanner e disinfector**
- Altre procedure
  - **Backup**
  - **Aggiornamento del software**

Gestione della sicurezza