Sicurezza in Internet

Attacchi e Contromisure

Sommario

- Tipi di attacco
- Difese
  - Firewall
  - Proxy
  - Intrusion Detection System

Attacchi e Contromisure

- Sniffing
- Connection hijacking
- Denial of service (DoS)
- Spoofing
- Buffer overflow
- Malicious code
- Hyper malware
- Defacement
- “Social engineering”

Sniffing

- Intercettazione passiva delle comunicazioni dati
- Attore: un soggetto (Attacker) che ha accesso diretto a determinati segmenti di rete o sistema, che ha strumenti tecnologici idonei
- Intercettazione di password, messaggi di posta elettronica e contenuti vari
- Gli strumenti informatici si chiamano sniffer

Sniffing

- I “programmi” devono essere installati su un calcolatore presente sulla rete da attaccare ⇒ il calcolatore deve essere precedentemente violato, compromesso
- Per difendersi e’ necessario effettuare una “detection”
- Tale operazione non è semplice, un indizio è la presenza di schede di rete poste in modalità promiscua (lettura di tutti i pacchetti che transitano sul segmento di rete)
- Interessa segmenti wired e wireless

Attacchi al contenuto - Esempio di sniffing

```
 1 0.000000 abete.reti.dist.unige wpop10.libero.it      TCP     32811 > http [SYN] Seq=2175924618 Ack=0 Win=5840 Len=0
 2 0.047915 wpop10.libero.it      abete.reti.dist.unige TCP     http > 32811 [SYN, ACK] Seq=395931055 Ack=2175924619 Win=24616 Len=0
 3 0.047968 abete.reti.dist.unige wpop10.libero.it      TCP     32811 > http [ACK] Seq=2175924619 Ack=395931056 Win=5840 Len=0
 4 0.048136 abete.reti.dist.unige wpop10.libero.it      HTTP    POST /email.php HTTP/1.1
 5 0.080256 wpop10.libero.it      abete.reti.dist.unige TCP     http > 32811 [ACK] Seq=395931056 Ack=2175925157 Win=24616 Len=0
 6 0.080281 abete.reti.dist.unige wpop10.libero.it      HTTP    Continuation
 7 0.223209 wpop10.libero.it      abete.reti.dist.unige TCP     http > 32811 [ACK] Seq=395931056 Ack=2175925329 Win=24616 Len=0
 8 5.503723 wpop10.libero.it      abete.reti.dist.unige HTTP    HTTP/1.1 200 OK
 9 5.503763 abete.reti.dist.unige wpop10.libero.it      TCP     32811 > http [ACK] Seq=2175925329 Ack=395931407 Win=6432 Len=0
10 5.575033 abete.reti.dist.unige wpop10.libero.it      HTTP    GET /error.html HTTP/1.1
11 5.595797 wpop10.libero.it      abete.reti.dist.unige HTTP    HTTP/1.1 200 OK
12 5.595843 abete.reti.dist.unige wpop10.libero.it      TCP     32811 > http [ACK] Seq=2175925881 Ack=395932855 Win=8688 Len=0
13 5.598326 wpop10.libero.it      abete.reti.dist.unige HTTP    Continuation
14 5.598367 abete.reti.dist.unige wpop10.libero.it      TCP     32811 > http [ACK] Seq=2175925881 Ack=395934303 Win=11584 Len=0
15 5.598693 wpop10.libero.it      abete.reti.dist.unige HTTP    Continuation
16 5.598705 abete.reti.dist.unige wpop10.libero.it      TCP     32811 > http [ACK] Seq=2175925881 Ack=395934857 Win=14480 Len=0
17 5.638893 abete.reti.dist.unige wpop10.libero.it      HTTP    GET /old/xam_rc/template_xam/images/spacer.gif HTTP/1.1
18 5.643669 abete.reti.dist.unige wpop10.libero.it      TCP     32812 > http [SYN] Seq=2171723094 Ack=0 Win=5840 Len=0
19 5.667858 wpop10.libero.it      abete.reti.dist.unige HTTP    HTTP/1.1 200 OK
20 5.667898 abete.reti.dist.unige wpop10.libero.it      TCP     32811 > http [ACK] Seq=2175926465 Ack=395935211 Win=17376 Len=0
21 5.668389 abete.reti.dist.unige wpop10.libero.it      HTTP    GET /old/xam_rc/template_xam/images/button_err_back.gif HTTP/1.1
22 5.677580 wpop10.libero.it      abete.reti.dist.unige TCP     http > 32812 [SYN, ACK] Seq=1219537146 Ack=2171723095 Win=24616 Len=0
23 5.677615 abete.reti.dist.unige wpop10.libero.it      TCP     32812 > http [ACK] Seq=2171723095 Ack=1219537147 Win=5840 Len=0
24 5.677745 abete.reti.dist.unige wpop10.libero.it      HTTP    GET /old/xam_rc/template_xam/images/header_err.gif HTTP/1.1
25 5.699033 wpop10.libero.it      abete.reti.dist.unige HTTP    HTTP/1.1 200 OK
26 5.707494 wpop10.libero.it      abete.reti.dist.unige TCP     http > 32812 [ACK] Seq=1219537147 Ack=2171723683 Win=24028 Len=0
27 5.741745 abete.reti.dist.unige wpop10.libero.it      TCP     32811 > http [ACK] Seq=2175927058 Ack=395935708 Win=17376 Len=0
28 9.096682 wpop10.libero.it      abete.reti.dist.unige HTTP    HTTP/1.1 200 OK
29 9.096723 abete.reti.dist.unige wpop10.libero.it      TCP     32812 > http [ACK] Seq=2171723683 Ack=1219538216 Win=7483 Len=0
```


Attacchi al contenuto - Esempio di sniffing

```
⊟ Frame 6 (238 on wire, 238 captured)
    Arrival Time: Dec 10, 2002 13:39:46.422800000
    Time delta from previous packet: 0.000025000 seconds
    Time relative to first packet: 0.080281000 seconds
    Frame Number: 6
    Packet Length: 238 bytes
    Capture Length: 238 bytes
⊟ Ethernet II
    Destination: 00:00:0c:03:de:0a (Cisco_03:de:0a)
    Source: 00:e0:18:a0:36:cc (Asustek_a0:36:cc)
    Type: IP (0x0800)
⊟ Internet Protocol, Src Addr: abete.reti.dist.unige.it (130.251.8.11), Dst Addr: wpop10.libero.it (193.70.192.46)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 224
    Identification: 0x2efe
  ⊞ Flags: 0x04
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0xfe9e (correct)
    Source: abete.reti.dist.unige.it (130.251.8.11)
    Destination: wpop10.libero.it (193.70.192.46)
⊟ Transmission Control Protocol, Src Port: 32811 (32811), Dst Port: http (80), Seq: 2175925157, Ack: 395931056
    Source port: 32811 (32811)
    Destination port: http (80)
    Sequence number: 2175925157
    Next sequence number: 2175925329
    Acknowledgement number: 395931056
    Header length: 32 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 5840
    Checksum: 0x24ab (correct)
  ⊞ Options: (12 bytes)
⊟ Hypertext Transfer Protocol
    Content-Type: application/x-www-form-urlencoded\r\n
    Content-Length: 100\r\n
    \r\n
    Data (100 bytes)
```


Attacchi al contenuto - Esempio di sniffing

```
0000  00 00 0c 03 de 0a 00 e0  18 a0 36 cc 08 00 45 00   ....P..à . 6Ì..E.
0010  00 e0 2e fe 40 00 40 06  fe 9e 82 fb 08 0b c1 46   .à.þ@.@. þ..û..ÁF
0020  c0 2e 80 2b 00 50 81 b1  fb a5 17 99 6d b0 80 18   À..+.P.± û¥..m°..
0030  16 d0 24 ab 00 00 01 01  08 0a 00 0e d7 79 22 87   .Ð$«.... ....×y".
0040  96 9d 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ..Conten t-Type:
0050  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 2d 77 77   applicat ion/x-ww
0060  77 2d 66 6f 72 6d 2d 75  72 6c 65 6e 63 6f 64 65   w-form-u rlencode
0070  64 0d 0a 43 6f 6e 74 65  6e 74 2d 4c 65 6e 67 74   d..Conte nt-Lengt
0080  68 3a 20 31 30 30 0d 0a  0d 0a 64 6f 6d 69 6e 69   h: 100.. ..domini
0090  6f 3d 6c 69 62 65 72 6f  2e 69 74 26 4c 4f 47 49   o=libero .it&LOGI
00a0  4e 3d 75 74 65 6e 74 65  26 50 41 53 53 57 44 3d   N=utente &PASSWD=
00b0  70 61 73 73 26 63 68 6f  69 63 65 3d 6c 69 62 65   pass&cho ice=libe
00c0  72 6f 26 41 63 74 5f 4c  6f 67 69 6e 2e 78 3d 35   ro&Act_L ogin.x=5
00d0  26 41 63 74 5f 4c 6f 67  69 6e 2e 79 3d 39 26 41   &Act_Log in.y=9&A
00e0  63 74 5f 4c 6f 67 69 6e  3d 45 6e 74 72 61         ct_Login =Entra
```

Login: **utente**

Password: **pass**

Connection Hijacking

- Riguarda le transazioni o comunque i flussi di dati point-to-point
- Non è una tecnica semplice da attuare è necessaria una certa rapidità nell'azione per impossessarsi dei dati che interessano per continuare la transazione
- L'attacker simula di essere una macchina che in realtà non è in modo da ottenere l'accesso

Contromisure a Connection Hijacking

- Adozione della Crittografia.
  - sia per gestire la cifratura dei dati scambiati;
  - sia l'autenticazione dei due poli della transazione.

Denial of Service

- Ha come scopo rendere l'obiettivo difficile o addirittura impossibile da raggiungere
- La tecnica di tale attacco prevede l'invio di un flusso consistente e continuo (flood) di dati verso l'obiettivo con il fine di rallentarlo e/o mandarlo in "crash"
- Può essere singolo o distribuito ovvero indirizzato ad un singolo calcolatore o verso una rete

Denial of Service

- DoS local based
  - Sovraccarico o arresto del servizio attaccato
  - scopo rendere inutilizzabile il servizio per un certo periodo di tempo
- DoS network based
  - Realizzati in maniera distribuita: utilizzo client ignari
  - Organizzata di solito contro obiettivi di un certo rilievo
- Bandwidth consumption
  - Inibizione della risposta del target (in gergo: riempendo il tubo)

Contromisure al Denial of Service

- Complessa: alcuni effetti si possono solo mitigare
- E' utile l'impiego di
  - firewall (filtri in ingresso e in uscita)
  - "Intrusion detection systems" per individuare la presenza di agenti (zombies) e di malicious code

Spoofing

- Non è un'intrusione in senso stretto, ma una serie di operazioni funzionali alla penetrazione di altri attacchi.
- "Spoofare" un indirizzo significa falsificarlo.
- Principalmente, o meglio inizialmente, si agisce sugli indirizzi IP, ma tale tecnica è attuata anche su altre categorie di credenziali (indirizzi di partenza della posta elettronica, numeri di telefono di partenza degli sms).
- È utilizzato per attuare tecniche DoS con il fine di mascherare le macchine attacker (anche le teste di ponte).

Contromisure Spoofing

- Crittografia rivolta ad autenticare i due poli.
- A livello IP:
  - Protocollo Ipsec;
  - Protocollo ssh (telnet sicuro).
- Per la posta elettronica:
  - Dispositivi di firma;
  - Crittografia a chiave pubblica con l'ausilio di certificati digitali.

Buffer Overflow

- Si basa sul presupposto, comune ai sistemi *nix (Linux, Unix), che alcuni programmi hanno privilegi particolari ("girano" anche come root)
- Se è presente un bug architetturale un attacker potrebbe sconvolgere le funzionalità del programma stesso prendendo possesso del calcolatore dove è installato il programma

Contromisure al Buffer Overflow

- Attenzione in fase di programmazione
- Problema costo in termini di lavoro aggiuntivo che richiede l'analisi e la verifica accurata
- Una soluzione consiste nel limitare i processi con diritti elevati assegnando ai programmi solo i diritti di cui hanno bisogno (least privilege)
- Utilizzo di strumenti di terze parti che agiscano da controllore (watchdog) intercettando possibili stringhe anomale (sintomo di prove generative di Buffer Overflow)

Malicious Code (sezione precedente)

- Macro categoria di codici che alterano e/o danneggiano (parzialmente o totalmente) il funzionamento di un sistema informatico o telematico.
- Sinonimi sono Malware e Mmc (Malicious mobile code).
- virus e worm

Mass Mailing

- è sempre Malicious Code ma:
  - non punta, in modo prioritario, a danni logici
  - cerca l'alterazione sistemi mailer e sistemi collegati
- ha come effetto DoS
  - Esempi:
    - » BadTrans:
    - » Nimda
  - cercano di sfruttare una particolare vulnerabilità di una piattaforma software (possibilmente molto diffusa)

Hyper-Malware - Mixed Mmc

- Insieme di più categorie malware
  - Il più in voga: worm/trojan
  - Rischio duplice
- Esempi:
  - Badtrans:
    - » Possibiltà rubare password su target (possibiltà di crearsi una conoscenza da riutilizzare per altri attacchi)
  - Goner:
    - » Disabilita personal firewall
    - » Correlazione tra Mmc e servizio di chat come Icq

Remote Access Trojan

- Ieri agiva sulle modalità di accesso remoto modificando il numero chiamato
  - Spese telefoniche stratosferiche
- Oggi sempre più apre backdoor al fine di permettere il controllo remoto del PC per rubare chiavi di accesso (es: conti bancari)

Defacement

- I "graffitari" del Web
  - Modificare o sostituire una o più pagine di un sito
  - Danni all'immagine
- Contromisure
  - Hardening
    - » Azione mista di aggiornamento dei sistemi e rafforzamento della loro configurazione
    - » Associata a controllo di accesso e l'uso di Intrusion Detection System

Social Engineering

- Tecnica psicologica
  - Sfrutta l'inesperienza degli utenti per mettere in essere attacchi o recare danni
    - » Furto di password
    - » Sulfnbk.exe (burla; fake alert per cancellarlo)
      - In realtà esistono copie di questo file contaminate dal virus magister che sono inviate via e-mail
  - Difesa principale: educazione utenti

Riassumendo: Difese da attuare

- Reattività: esempio aggiornando frequentemente il pattern degli antivirus (efficiente per fermare goner, non con badtrans che sfrutta una debolezza della piattaforma)
- Aggiornamento Software piattaforme di base (sistemi operativi e applicativi)
- Software antivirus a livello client e a livello gateway

Reti Wireless

- Hanno un livello aggiuntivo per la sicurezza
- 802.11 wireless lan standard
  - Wired Equivalent Privacy
    - » Vuole rendere equivalente dal punto di vista fisico la trasmissione wireless con quella via cavo
  - Advanced Encryption Standard: algoritmo simmetrico che sostituisce il DES (il rilascio in concomitanza con Wep 2)

Reti Wireless

  - Wireless application protocol utilizzando il livello Wtls (Wireless transport layer security) che ha il compito di
    - » Garantire autenticazione
    - » Integrità dei dati
    - » Privacy
  - Il tutto compatibilmente con le capacità di calcolo dei terminali wireless

Sicurezza nel wireless

- I problemi sono due
  - Comunicazione tra dispositivi wireless
  - Comunicazioni con siti di commercio elettronico e remote banking
    - » Questi ultimi usano Ssl (Secure Socket Layer) quindi deve esserci un gateway che effettua la conversione … qui potrebbe esserci l'intercettazione anche se attualmente si tratta di un operazione non semplicissima da effettuare, ma è molto pericolosa e quindi deve essere considerata.

Reti Wireless e Malicious Code

- Attualmente sono un pericolo remoto, ma alcuni produttori hanno rilasciato soluzioni per i Personal Digital Assistant e i wap gateway
- Pki: per l'autenticazione ci si affida alle Public key infrastructure
  - Insieme di tecnologie e policy che si appoggiano alla crittografia e ai certificati digitali
    - » Algoritmi a chiave pubblica
    - » Problemi di complessità per il mondo wireless

Soluzioni e prospettive

- Portare il livello di sicurezza proprio delle reti cablate alle reti wireless
- La comunità tecnico-scientifica prevede una stabilizzazione della wireless security progressiva

I sistemi di protezione delle reti

- Firewall
- Reverse proxy
- Intrusion Detection System

Firewall

- Realizza uno strato di:
  - Controllo degli accessi
  - Monitoraggio della sicurezza
- Posto tra la rete interna e quella esterna
  - Protocollo base TCP-IP
- Usa le tecnologie
  - Proxy
  - Packet filtering
  - Stateful Inspection

Proxy

- Tra il programma client, residente sul computer di un utente, e un server residente su un qualsivoglia server in Internet
- Decide se i tentativi di accesso sono consentiti o meno in base ai parametri impostati

Packet Filtering

- Tecnica di analisi dei pacchetti in transito
- I pacchetti vengono filtrati in base a delle regole stabilite a priori

Stateful Inspection

- Tecnica avanzata di ispezione dei pacchetti in transito
- attualmente utilizzata da alcuni software commerciali
  - Se ben realizzata è ritenuta una delle più efficaci

Personal firewall

- Legge sulla privacy e sue integrazioni (dpr 318/99 introducono degli obblighi)
- Protezione della rete distribuita su più livelli
  - Perimetrale
  - Sulle singole postazioni
- Nasce come ultimo punto di difesa
- Gestisce i tentativi di accesso non bloccati a livello di rete e integra l'azione degli antivirus

Reverse Proxy

- Posizionato tra il firewall e la Dmz (zona demilitarizzata dove vengono posizionati i server web e simili)
- Effettua una sorta di inoltro, subordinato a un controllo di sicurezza, del traffico diretto verso una delle risorse da lui gestite
- Obiettivo: fungere da unico punto di controllo nei confronti delle transazioni provenienti dall'esterno verso determinati obiettivi a rischio

Reverse Proxy

- Si basa sul presupposto che gli attacchi avvengono a livello di applicazione
- Passano attraverso il firewall o per cattiva configurazione o perché non si effettua un controllo totale a basso livello del codice in transito
- Altro motivo il mancato hardening (rafforzamento)
- Molto costoso in termini hardware e software

Intrusion Detection System

- Funzione di auditing
  - Registrare i tentativi di attacco
  - Consente la segnalazione delle possibili violazioni in atto
- File di log
  - Bisogna proteggerli: chi effettua un accesso illegale cerca sempre di modificarli per divenire invisibile
- Processano i vari file di Log per segnalare violazioni in atto

Intrusion Detection System

- Modo di operare
  - Real-time durante l'attacco; con varie segnalazioni all'amministratore di sistema
  - Post-incidente
- Metodiche
  - Controllo delle firme degli attacchi
    - » Come per gli antivirus
  - Riconoscimento anomalie
    - » Comportamenti del sistema diversi da quelli standard su cui il software Ids è stato istruito