Sicurezza nelle reti

Rischi

Spoofing

Indicazione di un differente mittente della comunicazione in modo da imbrogliare il destinatario

- IP
- ARP
- e-mail
- Web

IP spoofing

- Indirizzo mittente IP falso
  - Ovviamente indirizzo IP destinatario corretto
  - Serve a nascondere il mittente
  - Serve a travestirsi da mittente conosciuto e fidato
  - Serve a non essere riconosciuto

IP spoofing

- Routing avviene su destinatario
  - Il pacchetto viene inviato al corretto destinatario
  - La risposta non arriva al reale mittente

IP spoofing

- Blind o non-blind
  - Non blind se sulla stessa rete locale e quindi l'attacker può osservare i pacchetti anche se non diretti a lui
- Utilizzabile per attacchi di tipo 'man-in-the-middle' o 'session-hijacking'
  - Tecniche di predizione delle sequenze
  - Tipo di attacco non semplice

IP spoofing

- Utilizzato per attacchi di tipo Denial of Service
  - Sfruttando il fatto che le repliche non arrivano al reale mittente.

IP spoofing

- Cura non semplice
  - Si può limitare filtrando indirizzi IP con i firewall
    - Indirizzi della rete interna o di reti private o riservati
  - Importante l'opera di filtro di ISP
    - Evitare di far uscire su internet pacchetti che non provengono dalla rete interna in modo di evitare il più possibile il diffondersi di attacchi basati su questa tecnica

ARP spoofing

- Utilizzabile solo con reti IP su ethernet
- Il protocollo ARP è semplice
  - Stateless / usa una cache
  - Avvelenabile con pacchetti ARP di richiesta e di risposta fasulli (tecnica di ARP poisoning)

ARP spoofing

- Rischio di sniffing anche con gli switch
  - L'ARP spoofing permette di inserire il proprio MAC address associandolo all'IP della macchina da sniffare in modo da riuscire ad ingannare gli switch
- Possibile 'man-in-the-middle-attack'
  - Si unisce il proprio MAC address all' IP delle due macchine nel cui dialogo introdursi

ARP spoofing

- Possibile Denial of Service
  - Si può creare un flusso di pacchetti ARP con differenti indirizzi MAC in modo da riempire le tabelle degli switch che generalmente sono limitate
- Cura non semplice
  - Ove necessario si può ricorrere a tabelle ARP statiche

e-mail spoofing

- Falsificazione del campo 'mail from' negli headers del messaggio
  - Molto semplice da fare per i limiti del protocollo SMTP
    - Generalmente unico dato credibile è l'indirizzo IP di ultima provenienza delle mail
  - Utilizzato normalmente dagli spammers per nascondere le proprie tracce
  - Per ora non è risolubile: comunque si stanno studiando nuovi protocolli.

e-mail spoofing

- Falsificazione del tipo MIME negli headers dell'allegato
  - Utile con client che gestiscono diversamente gli allegati
    - Presentazione del tipo isando il tipo MIME
    - Gestione utilizzando le estensioni del nome
    - Relativo alle piattaforme Windows
  - Utilizzato per far eseguire programmi con virus oppure trojan
  - Combattibile con una corretta gestione dei tipi MIME

Web spoofing

- Attacco del tipo 'man-in-the-middle'
  - Fatto tramite plugin che rimanda ad un server
  - Il server logga le attività e serve le pagine richieste agendo come un application-proxy trasparente
  - Spoofing in quanto falsifica l'indirizzo che viene chiesto
  - Non risolubile

Web spoofing

- Altre tecniche
  - Inserimento di un @ in un indirizzo in modo da farlo apparire differente da quello che è
    - (a@b vuol dire che il server è b e si usa un utente a)

Denial of Service

- Attacco che crea una inutilizzabilità del servizio
- Creato saturando le risorse necessarie all'erogazione del servizio
- Fattibile se l'attaccante ha maggiori risorse dell' attaccato
  - Oppure distribuendo l'attacco con DDoS

Denial of Service

- L'unica cura è il possesso di risorse maggiori di quelle degli attaccanti e l'intervento tempestivo di blocco degli IP intrusi non solo sul firewall ma anche da parte dei rispettivi ISP

Denial of Service

- Sovente effettuato sfruttando deficenze dell'attaccato
  - Ping-of-death: pacchetto scorretto perchè più lungo di 64k, può portare al blocco di un sistema che non sa come frammentarlo correttamente.
    - Ora normalmente inoffensivo

Denial of Service

- Sovente effettuato sfruttando deficenze dell'attaccato
  - Jolt: pacchetto ICMP lungo frammentato in modo che il ricevente non riesce a riassemblarlo correttamente.
    - Può colpire W95 o WNT senza le opportune patches installate
- Si risolve tenendo aggiornati i prodotti

Distributed DoS

- Attacco di tipo denial of service fatto distribuendo l'attacco tra più attaccanti in modo da disporre di più risorse dell'attaccato

Distributed DoS

- Attacchi IP spoofing fatti su reti IP
  - Ping indirizzati ad un'intera rete con l'indirizzo dell'attaccato come mittente: l'intera rete risponde inviando la risposta al mittente presupposto.
  - Oggi la gran parte dei sistemi non risponde più a messaggi ICMP non unicast ma vi sono ancora eccezioni.
- Attacchi provenienti da computer compromessi

Distributed DoS

- Non sempre distribuzione passiva ma a volte volontaria
  - Net strike ovvero richiesta di pagine web da parte di una grossa massa di utenti
  - Mail bombing ovvero invio di una gran massa di e-mail di protesta da parte di un gran numero di persone con l'obiettivo di bloccare i servizi di e-mail dell'attaccato

Distributed DoS

- L'unica cura è il possesso di risorse maggiori di quelle degli attaccanti e l'intervento tempestivo di blocco degli IP intrusi non solo sul firewall ma anche da parte dei rispettivi ISP

Debolezze RPC /UDP

- Remote Procedure Call sviluppata per rendere più flessibili l'erogazione di servizi in rete
- Permette di far passare più protocolli tramite una sola porta UDP

Debolezze RPC /UDP

- Impossibile il controllo del servizio tramite il controllo della porta
- Unica difesa è il blocco del protocollo UDP
  - Eccezione per la porta 53 usata da BIND

Virus

- Codice maligno che si riproduce infettando altri file
- In origine introdotti tramite floppy/CD
- Oggi sempre più spesso via e-mail
  - Spoofing del tipo MIME
- Spesso tramite pagine HTML
  - Tramite inclusione di file .eml o .nwg apribili tramite client di e-mail contenenti allegati con spoofing del tipo MIME

WORM

- Non un virus ma codice che si replica reinviandosi tramite rete
- Anche i virus possono replicarsi reinviandosi via rete

WORM

- La differenza è che i virus esistono ed operano solo infettando dei programmi mentre i worm sono loro stessi dei programmi e non hanno bisogno di attaccarsi ad altri programmi
- I worm possono essere anche inoffensivi ma spesso causano DoS a causa della loro attività in rete

Trojan

- Programmi che si presentano differentemente da quello che sono
  - Falsi pannelli di richiesta password
- Programmi che fanno qualcosa di differente da quello che si pensa facciano
  - Ad esempio aprire porte e spedire file
  - Oppure rimanere in attesa di un segnale per partecipare ad un DdoS
  - Oppure rimanere in attesa di comandi dalla rete