Sicurezza dei sistemi e delle reti[1]

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2014/15

Lezione XVI: L'assegnazione automatica di IP

Il DHCP

Il Dynamic Host Configuration Protocol è un elemento critico nelle reti in cui i numeri IP sono **assegnati dinamicamente**.

- Permette configurazioni dinamiche (quindi aggiornate)
- Ma non prevede forme di autenticazione (ipotesi trusted LAN)

Cosa fa DHCP

- Assegna i numeri IP
- Default gateway
- DNS server

Particolarmente adatto nelle reti la cui topologia cambia continuamente (es. ISP)

Funzionamento del protocollo

1. L'amministratore della rete mantiene un pool di configurazioni sul DHCP server
2. Quando un client si connette alla rete (spesso al boot) fa broadcast di una richiesta di configurazione
3. Il server assegna una configurazione del pool, comunicandola al client

Il protocollo

1. Il client fa broadcast `DHCPDISCOVER`
2. Il server risponde con `DHCPOFFER`
3. Se accetta, il client fa broadcast di `DHCPREQUEST` (il broadcast serve a rispondere anche ad eventuali altri server)
4. Il server manda un `DHCPPACK`

Vulnerabilità

Il protocollo lavora a livello di rete locale in cui i nodi

- condividono il mezzo trasmissivo
- sono "identificati" dal MAC

Address starvation

Non essendo prevista nessuna forma di autenticazione, un attaccante:

- manda molte richieste, con MAC differenti
- il pool si esaurisce
- client legittimi non riescono a ottenere una configurazione

Contromisure

Una parziale contromisura già presente nel protocollo è il concetto di leasing: una configurazione viene "noleggiata" solo per un certo tempo, poi ritorna disponibile nel pool.

Contromisure

Una parziale contromisura già presente nel protocollo è il concetto di leasing: una configurazione viene "noleggiata" solo per un certo tempo, poi ritorna disponibile nel pool.

Contromisure

Molti switch permettono di **limitare il numero di MAC** utilizzabili da una determinata borchia: se questo limite è minore della disponibilità del pool, l'attaccante deve controllare piú borchie per essere efficace.

Rogue Server

I client che entrano nella rete non conoscono l'indirizzo del DHCP server (infatti fanno broadcast)

- Un attaccante può allestire un rogue server
- Deve raggiungere il client **prima** del server legittimo

Rogue Server: sostituire il gw

Un rogue server può comunicare un configurazione scorretta.

Sostituirsi al gateway In questo modo intercetta tutto il traffico (senza agire in modalità promiscua)

Rogue Server: sostituire il DNS

Un rogue server può comunicare un configurazione scorretta.

Sostituirsi al DNS In questo modo può manipolare tutte le destinazioni espresse con nome simbolico

Difese

- L'amministratore di rete può monitorare i nodi che fanno da DHCP server o anche forzare che ciò avvenga solo da un borchia determinata
- Esistono estensioni di DHCP con varie forme di autenticazione

Riassumendo

Il protocollo DHCP

- Lavora a livello LAN, con mezzo trasmissivo condiviso e identificazione affidata ai MAC
- Generalmente non sono previste forme di autenticazione sicura
  - Address starvation
  - Rogue server

La protezione del DNS

Il DNS è un servizio fondamentale per il buon funzionamento delle reti.

- È un elemento molto importante nella catena di trust delle transazioni iniziate da un utente umano, che raramente usa direttamente i numeri IP
- È un servizio generalmente **pubblico** e ottenuto in maniera decentralizzata, quindi nessuno ne ha il completo controllo

La protezione del DNS

- Può essere utilizzato anche come strumento di "intelligence" prima di ulteriori attacchi
- Esistono moltissime implementazioni, non tutte curate dal punto di vista della sicurezza
- Per questi motivi è un bersaglio particolarmente attraente

Separazione di servizi DNS

Spesso si allestiscono due server DNS

DNS Esterno Riceve query da utenti **esterni** per informazioni riguardo host pubblicamente accessibili della rete aziendale, incluso l'MX server (il Mail Relay)

DNS Interno Riceve query da utenti **interni** per informazioni su host sia della intranet aziendale che di Internet. Per le query che il DNS Interno non è in grado di risolvere contatta altri DNS (query ricorsive).

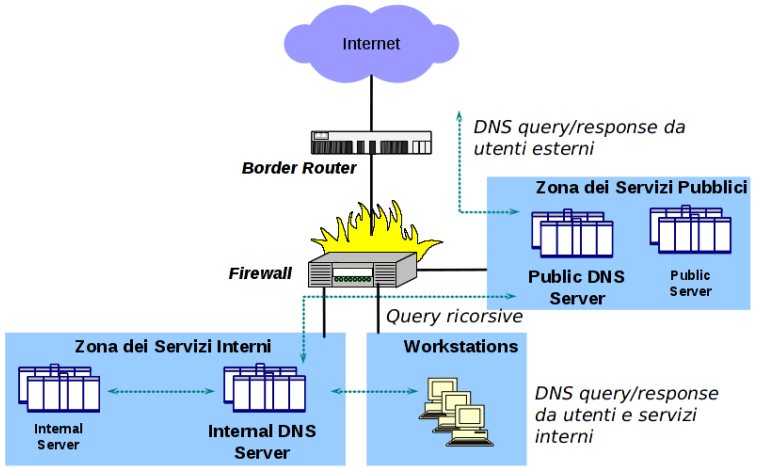
Vantaggi della separazione

I due DNS mantengono informazioni differenti (solo quelle pubbliche l'esterno, tutte quelle della intranet l'interno) e hanno connessioni con zone a diverso grado di sicurezza.

Vantaggi della separazione

- Separazione fisica delle informazioni riguardante servizi pubblici da quelle riguardanti servizi della intranet
- Assegnazione a diverse zone di sicurezza per la protezione delle informazioni
- Isolamento del DNS pubblico dalla rete interna nel caso di compromissione

Separazione DNS



Riassumendo

Il DNS è un servizio altamente critico in una rete

- Il protocollo è privo di feature di sicurezza
- È opportuno strutturarne la difesa in piú livelli