E il *firewall* mormorò: "Non passa lo straniero!"

Ovvero: c'è vita intelligente *al di là dei firewall...*[1].

Mattia Monga

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

Milano, 13 giugno 2014

[1]

Sicurezza delle reti == *firewall*?

La sicurezza informatica è spesso dominata dall'idea di controllo dell'accesso.
Nelle reti, in particolare, ci si è concentrati sull'accesso ai canali di comunicazione:

- *firewall*: controlli *di frontiera*, per lo piú *stateless* su metadati della comunicazione
- *Intrusion Detection (IDS)*: controlli per lo piú *stateful* sul contenuto della comunicazione

Retorica sicuristica

Si tratta purtroppo piú di suggestioni retoriche piuttosto che di effettiva efficacia difensiva. Vedi: *È dell'informatica il fin la meraviglia. Metafore per la sicurezza e sicurezza delle metafore*, Informatica Umanistica 4 4/2011, `http://www.ledonline.it/informatica-umanistica/Allegati/IU-04-10-Monga.pdf`

Firewall e IDS sono utili per:

- Isolare il traffico
- Identificare attacchi noti
- Contenere pericoli generici

Sicurezza informatica

Ma la sicurezza dei sistemi informatizzati è molto di piú e molto molto piú complicata della pura sicurezza perimetrale.

- Attacchi mirati
- Considerazioni di costo/efficacia/esternalità
- La comunicazione di "dati" è indistinguibile dalla comunicazione di "computazioni"
- Conflitti di interesse

Opinione personale: è impossibile fare buona sicurezza informatica senza una solida (e tecnica) competenza informatica!

Gare di intrusione

Le gare di intrusioni sono un ottimo (e divertente!) modo per rendersi conto di cosa significhi difendere un sistema, anche se principalmente ci si concentra sull'attacco

- Competizione $\rightsquigarrow$ situazioni conflittuale
- Pensiero laterale, regole del gioco e "giocare le regole"
- Eleganza ed efficacia
- Sapere è potere intrusivo

DEF CON CTF

La prima e tuttora piú famosa competizione formalizzata è il *Capture the Flag* (CTF) di DEF CON.

- Nata nel 1996
- In presenza a Las Vegas, 48 ore
- Qualificazioni internazionali (+500 squadre) in maggio (Unimi si è qualificata nel 2008 con `Guard@MyLAN0`)
- Qualificazioni basate su "*challenge*"

Shitsco

Proviamo!

http://services.2014.shallweplayaga.me/shitsco_c8b1aa31679e945ee64bde1bdb19d035
is running at:
shitsco_c8b1aa31679e945ee64bde1bdb19d035.2014.shallweplayaga.me:31337
Capture the flag.

Traccia

- Abbiamo il binario
- Abbiamo l'ambiente d'esecuzione
- Analisi di alto livello
- Bruteforce
- Analisi di dettaglio
- Exploit

Riferimenti

- https://github.com/ctfs/write-ups/tree/master/def-con-ctf-qualifier-2014/shitsco
- https://blog.skullsecurity.org/2014/defcon-quals-writeup-for-shitsco-use-after-free-vuln
- http://www.endgame.com/blog/defcon-capture-the-flag-qualification-challenge-1.html