

Footprinting, scansione enumerazione

Massimo Danieli

Footprinting

- Letteralmente impronta
- Raccogliere tutte le possibili informazioni su un possibile obiettivo (*nomi di dominio, blocchi di rete, IP sistemi operativi, hardware di rete ecc*)

Footprinting Internet

- Sito istituzionale
- Enumerazione della rete
- Indagine sulla rete
- Tool: Google ;) host, whois, wget, teleportpro, samspace, traceroute

Scansione

- Determinare su un range di IP o su un singolo le porte ed i servizi in esecuzione
- First step: scansione IP E ICMP
- Tool: nmap, fping, hping, pinger, PingSweep

Scansione TCP

- Scansione di porte
- Alla ricerca di servizi
- Tool: nmap, strobe, nc, NetScanTools, SuperScan, cheops
- Sul riconoscimento dei SO
<http://www.insecure.org/nmap/nmap-fingerprinting-article-it/stackf.html>

Enumerazione

- Identificazione dei punti deboli
- Maggiore intrusività rispetto alla scansione
- E' fortemente legate al SO
- Tre categorie
 - risorse e condivisioni di rete
 - utenti e gruppi
 - applicazioni e banner

Ambiente win

- Sessioni nulle (net use \$target\ipc\$ "" /u"")
- risorse di rete nbstat
- enumerazione SNMP
- Tools DumpSec, Legion, NAT, userinfo, getacc ecc...

Enumerazione Unix

- Gruppi e utenti: finger rwho
- Applicazioni e banner: rpcinfo, nmap
- Enumerazione SNMP: snmpwalk, nmap