DNS

Il citofono della tua organizzazione

Salvatore Todaro

Università degli Studi di Messina

DNS, il citofono della tua organizzazione

”Conosci il nemico come conosci te stesso. Se farai così, anche in mezzo a cento battaglie non ti troverai mai in pericolo”.

”Se non conosci il nemico, ma conosci soltanto te stesso, le tue possibilità di vittoria saranno pari alle tue possibilità di sconfitta”.

”Se non conosci te stesso, né conosci il tuo nemico, sii certo che ogni battaglia sarà per te fonte di pericolo gravissimo”.

“Se conosci il tuo nemico e conosci te stesso, la vittoria non sarà in discussione."

Sun Tzu, L’arte della guerra

DNS, il citofono della tua organizzazione

”L’insicurezza dei protocolli internet deriva dalla cultura hippie”

(Corrado Giustozzi)

Nel 2022 la nostra visione del ruolo della security dei servizi e delle infrastrutture è cambiata?

La nostra comunità (persone) ha abbandonato la visione di un “mondo hippie”?

DNS, il citofono della tua organizzazione

”Depende, da che depende? Da che punto guardi il mondo tutto depende” (Jarabe de Palo)

Un servizio DNS, i dati esposti possono essere usati leggittimamente:

- Per far usare i servizi (pubblici?)

Illeggittimamente per raccogliere informazioni:

- Per conoscere meglio la vittima prima dell’attacco

I ladri, probabilmente, prima di fare una rapina in appartamento fanno esattamente la stessa cosa

DNS, il citofono della tua organizzazione

Fase 1 di un attacco: la ricognizione / raccolta delle informazioni

- Attiva (contatto il bersaglio)
  - Il bersaglio potrebbe avere sentore dell'attività
  - Potrebbe fare "Rumore" e far scattare delle campanelle

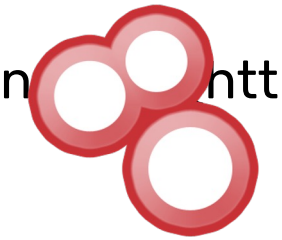
- Tool: DNSRecon, dnsenum etc

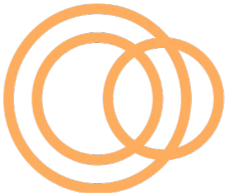
dnsrecon -d miodominio
dnsrecon -d miodominio -k
(cerca anche i certificati emessi per il dominio)
dnsrecon -r rangeip (fa ricerca inversa)

DNS, il citofono della tua organizzazione

Fase 1 di un attacco: la ricognizione / raccolta delle informazioni

- Passiva (ottengo informazioni da fonti servizi OSINT)
  - Il bersaglio ha percezione nulla dell'attività
  - Engine fanno scansione di tutta internet
- Motori di ricerca utilizzando (es. google dorks)
- Engine / servizi specializzati:
  - Shodan.io (https://www.shodan.io/
  - Censys (https://www.censys.io/)





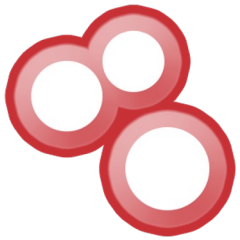
DNS, il citofono della tua organizzazione

Fase 1 di un attacco: la ricognizione / raccolta delle informazioni

Proviamo a verificare la nostra esposizione

https://shodan.io/domain/miodominio

https://search.censys.io/



SHODAN censys

DNS, il citofono della tua organizzazione

Il citofono si trova all'esterno del palazzo

- ha "di norma" la lista degli abitanti
- È interattivo
- Espone delle informazioni
- Raramente espone informazioni funzionali (es. Portiere)

Il DNS si potrebbe trovare all'esterno dell'organizzazione

- Di norma dovrebbe avere la lista dei servizi "pubblici" (per i server pubblici)
- È Interattivo
- Espone delle informazioni

DNS, il citofono della tua organizzazione

La sicurezza non si ottiene attraverso l'oscurità

(quando l'oscurità è l'unico mezzo di difesa)

DNS, il citofono della tua organizzazione

La sicurezza trae giovamento dall'oscurità

rallenta probabilmente l'azione degli attaccanti
(minimo sforzo massimo risultato)

Non si devono nascondere finestre rotte

Si potrebbero/dovrebbero nascondere finestre robuste

DNS, il citofono della tua organizzazione

Cosa succede se si ha curiosità, qualche competenza e tempo libero?

> 5 host fileserver.dominio
> 300 host stampante|printer.mio dominio

> 100 *mysql*.dominio
> 4 organizzazioni usano hibp (txt record)

DNS, il citofono della tua organizzazione

Interrogazioni DNS (inversa) alla ricerca di

- Domini e sottodomini
- Hostname

dnsrecon -r range

- Scansione dei Domini e sottodomini

dnsrecon -d miodominio -k

DNS, il citofono della tua organizzazione

Sia il citofono, che il DNS possono essere usati dai malfattori!!!

Il DNS potrebbe contenere record come:
pcutente.dominio → saprei che quel host è un pc ed è in uso a utente

vm+servizio → saprei che quell'host eroga un servizio/software e si trova su un sistema di virtualizzazione

ilo* → potrebbe trattarsi di una interfaccia di gestione ?

ups qualcosa → saprei che quell'host è un ups e se lo comprometto spengo quasi certamente qualcosa

git qualcosa → è un server git che potrebbe contenere dati importanti

altre keyword interessanti backup, luoghi, mysql, oracle, nas, stampante, printer, marca o modelli di sistemi, schermo, servizio-admin, anticamera etc

DNS, il citofono della tua organizzazione

Sia il citofono, che il DNS possono essere usati dai malfattori!!!

Il DNS potrebbe contenere record come:

Indicarmi le subnet / servizi / host “privati” usati dall’organizzazione

Darmi una idea di insieme sulla “robustezza” e “approccio” dell’organizzazione.

DNS, il citofono della tua organizzazione

Alcune “firme”, quale è la più sicura?

9.11.36-RedHat-9.11.36-3.el8_6.1
9.11.5-P4-5.1+deb10u8-Debian
9.8.33trentinientraronointrento
Ignota!
None
I Do not Know
https://bit.ly/3D3z3DC
Non te lo dico...

DNS, il citofono della tua organizzazione

La firma è un dettaglio apparentemente “banale”

- Se valorizzato di “default” potrebbe esporre dati su:
  - la piattaforma erogante (S.O.)
  - sulla versione
- Se valorizzato custom potrebbe indicare una certa cura per i dettagli “di sicurezza”

DNS, il citofono della tua organizzazione

La firma è un dettaglio apparentemente “banale”

- Se valorizzato di “default” potrebbe esporre dati su:
  - la piattaforma erogante (S.O.)
  - sulla versione
- Se valorizzato custom potrebbe indicare una certa cura per i dettagli “di sicurezza”

DNS, il citofono della tua organizzazione

- Principio del need to know
- Privacy e security by design/default (GDPR)

DNS, il citofono della tua organizzazione

Sul citofono non si inseriscono le tabelle millesimali (che potrebbero dare una idea del valore)

Perchè esporre dati non necessari nei DNS?

Perchè inserire record che non sono disponibili per terzi?

Perchè non utilizzare DNS o zone “locali”?

Il blocco del trasferimento di zona non basta per evitare un leak delle informazioni

Non basta inserire dei blocchi di interrogazione

DNS, il citofono della tua organizzazione

Nei panni di un attaccante :

- Un target di cui conoscete già molto

- Un target che non espone informazioni

Un ladro di appartamento sceglierebbe:

- un bersaglio dove sa dove si trova la cassaforte e conosce molti dettagli del sistema di allarme e di protezione

- Un bersaglio dove tutte le informazioni (cassaforte allarme etc) sono da scoprire

DNS, il citofono della tua organizzazione

Tutto bello interessante!!!

E Quindi? E Allora?

Domande :

- Secondo voi sono paranoide o è un problema reale?
- Se è un problema reale come procedere?
- E' una questione secondaria o importante?
- Quanto sforzo richiede?

DNS, il citofono della tua organizzazione

Salvatore Todaro
salvatore.todaro@unime.it
Università degli Studi di Messina
C.I.A.M. “A.Villari”
U. ORG Sistemi ed Infrastrutture ICT e Rete di Ateneo
U.Op. Sicurezza Informatica
Comitato Tecnico Scientifico IDEM GARR AAI