Come sta la tua rete?
Tutto bene, grazie

Pisa, 20181026

Chi sono e dove lavoro

- Ho lavorato per qualche anno come amministratore/responsabili di rete di alcuni dipartimenti dell'Università di Bologna
- Dal 2005 sono security analyst presso CERT-UniBo. In pratica analizzo il traffico di rete alla ricerca di anomalie che possono compromettere il buon funzionamento della stessa (mal configurazioni, dispositivi compromessi, usi impropri).

Qualche numero sulla rete dell'Università di Bologna:

- link a 10G
- 30-50K dispositivi connessi negli orari di punta
- Dislocata geograficamente sul territorio dell'Emilia Romagna da Bologna in giù con sedi nelle città di Bologna, Ravenna, Faenza, Forlì, Cesena, Cesenatico, Rimini, ecc...

Parliamo di prevenzione...

- **Def.:** La prevenzione è l'insieme di azioni finalizzate a impedire o ridurre il rischio, ossia la probabilità che si verifichino eventi non desiderati. Il concetto ha validità ed è presente in diversi ambiti. Gli interventi di prevenzione sono in genere rivolti all'eliminazione o, nel caso in cui la stessa non sia concretamente attuabile, alla riduzione dei rischi che possono generare dei danni all'incolumità di persone, animali o infrastrutture. (wikipedia: https://it.wikipedia.org/wiki/Prevenzione)

Come si fa la prevenzione di una rete informatica?

Un buon punto di partenza sono le misure minime di sicurezza per le PA e il GDPR

Fare prevenzione è sufficiente?

Ovviamente no. O meglio la prevenzione è un processo continuo. Infatti occorre verificare l'efficacia delle policy e delle tecnologie adottate, ma occorre anche cercare di scoprire cosa ci accade intorno per continuare l'opera di prevenzione.

Gli attori/attaccanti

Proviamo a vedere cosa circola di malevolo nelle reti:

- cyberarmy: vari stati anche UE si stanno dotando di un esercito cibernetico
- cybercrime: la criminalità organizzata ha parecchi soldi da spendere, ne guadagna tanti in rete e non è facile identificarla
- hacktivist: sono motivati da una ideologia
- altro: solitamente sono fonte di rumore

Smettiamo di usare la parola hacker in modo improprio: chi commette un reato informatico non è necessariamente un hacker ma è sicuramente un cyber criminale

Le "infezioni" a cui le reti sono soggette

- Ransomware
- DDOS: brevi e intensi: secondo il GARR, la quasi totali dei DDoS subiti hanno durata inferiore ai 30 minuti con un picco intorno alla durata di cinque minuti. Quelli con durata superiore ai 30 min sono il 5% e la maggior parte di questi non supera l'ora. Di recente a UniBo abbiamo "visto" la scansione di una nostra classe B in meno di mezzo secondo.
- Browser exploit
- phishing/spam
- Brute force attack
- Scanning
- Web application exploiting
- mining
- attacchi mirati
- malware: smettiamola di chiamarli virus
- ecc....

Come fare analisi

Lo scopo dell'analisi è l'identificazione di anomalie nell'uso delle rete (non solo attacchi ma anche mal configurazioni o usi spregiudicati).

I metodi e gli strumenti sono tanti. Proviamo a dare una semplice classificazione che si basa sulla tipologia di dato che viene analizzato:

- analisi del traffico di rete: tipica dei sistemi di intrusion detection (DPI - Deep Packet Inspection)
- analisi a posteriori dei log (Threat Hunting)

Per un analisi efficace, il team che se ne occupa deve essere dedicato esclusivamente a questa attività (full time).

Analisi del traffico di rete...

Può essere passiva (non influenza il traffico volta sola alla detection), o attiva in questa caso assume il ruolo di prevention.

Gli strumenti solitamente utilizzati sono IDS (Intrusione Detection System, passivi), IPS (intrusion Prevention System, attivi), ADS (Anomaly Detection System). Potreste trovare anche le sigle NIDS, BADS o NBADS. Significa che l'analisi si riferisce al network. La B negli ADS sta per Beaviour (Comportamentale).

...Analisi del traffico di rete...

Gli IDS sono strumenti che si basano su signature (regole) che identificano (DPI: Deep Packet Inspection) un anomalia.

- reagiscono efficacemente a ciò che le signature descrivono il resto lo ignorano
- possono generare alert su anomalie riscontrato durante l'ispezione
- per massimizzare la loro efficacia è ncessario conoscere bene cosa devono proteggere al fine di usare il corretto insieme di signature e rendere più efficace la detection
- esistono parecchie tecniche di evasione: un lavoro di qualche anno fa le stimava nell'ordine di qualche miliardo: su link ad alto traffico, una tecnica di evasione efficace è quella di creare dei diversivi
- il settaggio è complesso
- il dimensionamento è complesso: su link ad alto traffico possono richiedere molte risorse
- Per link ad elevato traffico (10Gbps) il costo può aggirarsi intorno ai 100K€, se te lo costruisci con prodotti open +3K€

...Analisi del traffico di rete

IDS open source sono: **snort, suricata e bro**

I BADS solitamente lavorano sulle sessioni, processano i dati netflow.

- sono molto efficaci per verificare cosa sta passando sulla rete e quindi adatti al policy enforcement
- sono facilmente influenzabili (fluttuazioni), si adattano lentamente al cambiamento della rete

Non sono a conoscenza di BADS open source anche se bro può essere usato in tale modalità.

Bro non è un ids classico ed è facilmente programmabile. Usa molte risorse.

Installare un IDS è un operazione complicata a causa della quantità di componenti da cui è composto e la loro necessaria configurazione. Una distro/repository che aiuta in questo compito è Security Onion

Threat Hunting

- L'idea alla base è quella di non mettere in piedi un sistema di analisi del traffico di rete che può risultare molto costoso in termini di risorse economiche e conoscenze. Ma di usare dati che già si possiedono (log di apparati, applicazioni, client, ecc..) e cercare in questi le anomalie:
- richiede un “contenitore” per log adeguatamente dimensionato
- di facile scalabilità
- richiede creatività nella creazione e gestione degli allarmi
- gli allarmi richiedono molta personalizzazione e non sono facilmente esportabili
- Adatto all’identificazione degli spostamenti laterali (lateral movement)

Cosa scegliere

L'ideale è un sistema ibrido (che usi sia DPI che TH) i cui allarmi permettano l'approfondimento dell'analisi di rete:

- se trovo una anomalia col TH posso, grazie all'analisi del network posso identificare tutte le macchine che ne sono state influenzate
- se trovo una compromissione grazie all'analisi del traffico di rete col TH posso cercare di capire come e quando è avvenuta e magari come si sta evolvendo (lateral movement)

Semplificando, gli IDS "agiscono" come degli antivirus (reagiscono bene a ciò che conoscono). Gli ADS scatenano allarmi al superamento di una soglia.

Tutto questo basta? No ci vuole altro

Intelligence

Il termine fa un po' sorridere ma è così. Occorre che chi fa analisi/ricerca condivida i suoi risultati (ruolo di producer) e/o possa accedere a risultati di analisi attendibili (ruolo di consumer).

L'idea di fondo è che facilmente due analisti che non hanno nulla in comune se non la loro attività, si troveranno a lavorare sullo stesso caso ma con risultati diversi. Punti di vista diversi migliorano la visione del problema. Se questi punti di vista sono più o meno pubblici, se viene creata una rete di informazione, le analisi possono essere più efficaci e meno prone ad errori (information sharing).

Prodotti open di questo tipo sono: MISP, The hive project, Minemeld

Esattamente come già fanno gli attaccanti, possiamo fare intelligence su fonti come i social o repository (es. pastebin). I risultati (scraping) una volta elaborati possono essere uno strumento di prevenzione. Un progetto open di questo tipo è AIL

“Nuove” tendenze

Fileless attack: attacchi che non lasciano tracce:

- Spectre, meltdown
- Krack su wifi
- odine per airgapped computer

Abbiamo tutto?

No :-(. La detection così come ve l'ho descritta non indaga su ciò che non conosce. Esistono diversi progetti che portano l'analisi sul piano statistico per evidenziare quei comportamenti automatici tipici delle botnet e che comunque una macchina compromessa deve avere: ogni tanto deve interfacciarsi con chi la sta gestendo. L'approccio statistico non è il solo.

Di seguito alcuni progetti open che trovate che vanno in questa direzione:

Bat: framework per l'analisi statistica e machine learning dei dati presenti nei log di bro (https://github.com/SuperCowPowers/bat)

Opnids: suricata e machine learning (https://www.opnids.io/)

Rita: analisi statistica dei log di bro (https://github.com/ocmdev/rita)

Stratosphere: analisi della ripetitività delle comunicazioni (https://www.stratosphereips.org/)

Un limite comune a questi progetti è l'analisi di un momento e non di un intervallo temporale più ampio (giorni, settimane,...)

Nuovi filoni d'indagine

Si stanno sviluppando nuovi filoni di analisi, molto interessanti e promettenti:

- ETA: Encrypted Traffic Analysis:
  - Man in the middle
  - Analisi delle peculiarità
- Analisi comportamentale dell'utente (ne ho sentito parlare)
- Analisi del DNS (finalmente)

Analisi del DNS

Da una “semplice” interrogazione DNS (richiesta e suo risultato) possiamo scoprire:

- Malconfigurazioni
- Violazioni di policy (uso di dns non ufficiali)
- Compromissioni (DGA, Fastflux, Covert Channel)
- Attacchi di Social Engineering (*Phishing anche tramite IDN, *typosquatting)

L’analisi del dns richiede poche risorse anche se fatta su link ad alto traffico

Ma ntopng? E' tanta roba

Quando si parla di ntopng si pensa solo a ntopng dimenticando che è formato da diversi oggetti. Tra questi forse quello più "sconosciuto" è pf_ring (lunga vita a pf_ring!!!). Con la famiglia ntop potete fare molte delle cose fin qui descritte:

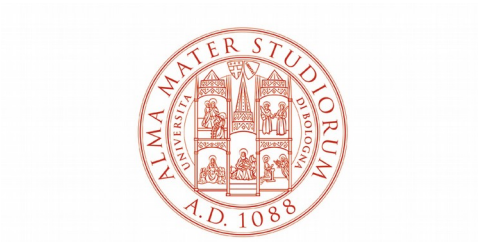
- l'analisi attiva o passiva del network
- non avete un semplice ids/ips/ads, ma avete diverse funzionalità di questi sistemi
- è una famiglia di prodotti che si prefiggono l'analisi di rete da diverse angolazioni
- è OPEN
- usa nDPI, se i prodotti open lo usassero…..
- fa analisi del traffico criptato (ETA, no MITM)
- e tanto altro ancora
- Il team di sviluppo non si stanca mai :-) basta seguire il blog

Consigli e Conclusioni

Concludo lasciandovi queste “perle di saggezza”:

- il vostro strumento più importante è l'analizzatore di protocollo: ngrep, tshark (wireshark)
- mai fidarsi di quanto affermano i vendor: verificate sempre. Come? Con l'analizzatore di protocollo
- un unico strumento di analisi vi da solo un punto di vista. Più sistemi di analisi i cui campi di analisi si intersecano, vi danno, ovviamente, una visione più ampia e chiara dell'anomalia.
- per un analisi efficace, il team di analisti deve essere dedicato esclusivamente a questa attività (full time).

Domande?



Simone Bonetti

CeSIA

simone.bonetti@unibo.it, cert@unibo.it

www.unibo.it