IP Network Security Assessment

Sun Microsystems©, una delle più grandi e innovative aziende tecnologiche, aveva un motto: “The Network is the computer”. La frase è stata coniata per la prima volta nel 1984 da John Gage, il 21° dipendente di Sun Microsystems, a cui è stato attribuito il merito di aver costruito la visione di Sun attorno a "La rete è il computer". e ora è un marchio di Cloudflare©, una delle più grandi aziende che fornisce rete di distribuzione di contenuti e servizi di mitigazione DDoS. Questo la dice lunga sull'importanza della sicurezza di rete nel nostro mondo perennemente interconnesso. Ma quando si parla di Network Security, tutti pensano a firewall o ai penetration testing per verificare il loro stato attuale, ignorando ciò che accade realmente all'interno delle reti aziendali e delegando tutto ad un dispositivo che protegge solo dal mondo esterno. Ironico, non è vero? Ransomware, furti di dati e violazioni della sicurezza sono così tanti nelle notizie di tutti i giorni che ormai non fanno più notizia, è routine. **Fino a quando non sei colpito direttamente.**

Che cos'è un IP Network Security Assessment e perché è diverso da un penetration test ?

Un comune penetration-test, o anche il cosiddetto "Security Assessment", di solito include solo l'analisi delle vulnerabilità del sistema e della loro possibilità di essere sfruttate da un utente malintenzionato. È fondamentalmente un'istantanea delle possibili superfici di attacco di uno o più sistemi in un determinato momento. Ciò potrebbe includere anche i firmware dei dispositivi di rete e le patch di sistema e, a seconda delle capacità tecniche di chi effettua il test (e del costo della valutazione), potrebbe davvero mostrare cose e modi interessanti per risolverli. In breve, è fondamentalmente un'istantanea della vostra situazione di sicurezza su un insieme di sistemi in un determinato momento. Che è probabilmente soggetta a cambiamenti nel tempo, ed anche abbastanza rapidamente, perché le tecnologie cambiano e si evolvono a ritmi frenetici.

Un IP Network Security Assessment è abbastanza diverso. Non ha lo scopo di verificare le vulnerabilità sui sistemi interni (è quello che fa il penetration-test), ma cerca di farti comprendere come la tua infrastruttura di rete viene utilizzata dai tuoi utenti e dai tuoi sistemi interni per trovare pattern, comportamenti errati e segni di possibile compromissione. Troppo spesso la sicurezza della rete interna viene sottovalutata e la maggior parte (se non tutta) la sicurezza della rete è delegata al firewall perimetrale. Potrebbe esserci un IDS/IPS nella maggior parte degli scenari di sicurezza, ma nel tempo fa fatica a stare dietro alla crescita della larghezza di banda disponibile. Inoltre, i SIEM non sempre riescono nel loro mestiere, poiché le aziende raramente hanno le risorse disponibili per controllare tutti i log e c'è letteralmente un oceano di dati in cui cercare.

È qui che il punto di vista a volo d'uccello ti aiuta a trovare le cose giuste da controllare.

Cosa è Fl0wer ?

Ecco perché uno strumento come Fl0wer può davvero aiutare il tuo team di rete ad accelerare i tempi di risposta del team di sicurezza alle minacce attuali e future. Sfruttando le tecnologie di sintesi di flusso più utilizzate e consolidate (Netflow, IPfix, sFlow) e l'archiviazione dei dati OLAP, può davvero identificare rapidamente ciò che sta accadendo sulla tua rete interna praticamente in real-time. Fl0wer può essere alimentato con i dati forniti da un enorme elenco di dispositivi (un elenco breve e incompleto può essere trovato su http://downloads.fl0wer.me/Fl0werDeviceMatrix.pdf)
Può aiutarti a identificare rapidamente IOC (Indicators of Compromise) come:

- connessioni TOR
- connessioni P2P
- possibili Covert Channels
- scansioni verticali su un target host (come un obiettivo da violare)
- scansioni orizzontali per un servizio (come un worm, un malware o un ransomware)
- violazioni delle policy per i servizi core interni come NTP, DNS, BGP, SNMP, VPN, SDN, etc.
- connessioni a reti Bogon o indirizzi in Blacklist su Internet
- traffico fuori matrice
- traffico relativo a criptovalute
- traffico relativo ai social network nel vostro datacenter
- traffico probabilmente indesiderato

Il servizio di IP Network Security Assessment

Il servizio di IP Network Security Assessment funziona concettualmente più o meno come un test di penetrazione, fornendoti un'istantanea di una settimana (o più) di traffico della tua rete interna, per capire cosa sta realmente accadendo, facendo uso dello strumento Fl0wer. Tutti i dati necessari vengono raccolti direttamente dai dispositivi dalla tua rete interna configurando correttamente l’esportazione dei flussi dove possibile (o fornendo temporaneamente tap di rete dedicati se le configurazioni non possono essere toccate) e archiviati per ulteriori analisi e report. Alla fine del periodo di osservazione, viene generato un report e tutti i dati raccolti vengono consegnati come file CSV (Comma Separated Value) per la massima flessibilità ed ulteriori analisi.

What is needed ?

I servizi di IP Newtork Security Assessment effettuati con Fl0wer non necessitano di troppe informazioni. In un incontro di pre-configurazione verranno richiesti::

- una mappa generale della topologia dell’infrastruttura di rete
- il dettaglio delle reti interne (IPv4/IPv6) compresi i nomi e le netmask e delle zone di sicurezza
- l’elenco delle risorse aziendali formali in termini di DNS, NTP, BGP, concentratori VPN, etc.
- considerazioni particolari su come classificare determinate tipologie di traffico note
- definizione dei punti di osservazione della rete abilitabili all’uso dei protocolli Netflow V1,V5,V9,IPFix ed sFlow

Fl0wer viene quindi concesso in licenza e ne viene effettuato il deployment in una VM (Virtual Machine) per essere ospitato su un Hypervisor del cliente on-premise (o su hardware fisico noleggiato se necessario) ed i dispositivi di rete vengono configurati per esportare i dati di traffico verso Fl0wer (o eventualmente vengono installati dei network tap a noleggio se necessario). Viene eseguito un controllo di due giorni per verificare la corretta configurazione dell'infrastruttura di analisi, quindi inizia il periodo di osservazione.
Al termine del periodo di osservazione, il report viene consegnato e discusso con il team di rete e sicurezza dei clienti, verificando i risultati e l'esito del report Fl0wer e ragionando sulle possibili soluzioni alle eventuali problematiche riscontrate.

Per ulteriori informazioni: https://fl0wer.me – info@fl0wer.me