W19D4 – analisi di rete con Wireshark

Esercizio obbligatorio.

La cattura con Wireshark potrebbe essere relativa ad un attacco in corso e il principale IOC che lo fa pensare è la presenza di richieste TCP ripetute, effettuate un ampio range di porte sia common ports sia high ports. Queste richieste TCP sono molto numerose e su varie porte sempre diverse. Non è possibile individuare uno specifico vettore di attacco, ma si può trattare di una scansione sul target, magari effettuata con Nmap con lo switch -sS, dato che il three ways handshake non viene completato e si vedono solo flag SYN, ACK, RST. Questa scansione è dunque più furtiva di una scansione con lo switch -sT e quindi potrebbe far pensare ad un tentativo da parte dell'attaccante di fare una scansione della macchina vittima e capire quali porte sono aperte per poter poi organizzare un exploit di una vulnerabilità. A riprova che si potrebbe trattare di una scansione, alcune porte sono aperte e vi sono delle risposte positive SYN + ACK, mentre altre porte risultano chiuse e si vedono i flag RST + ACK, a segnalare che la porta è chiusa. Per ridurre gli impatti di questa scansione e per limitare possibili attacchi a seguito di questa scansione, la soluzione migliore consiste nella configurazione di policies del firewall che blocchino l'accesso a tutte le porte della macchina vittima da parte della macchina attaccante, per bloccare l'accesso dell'attaccante. L'IP dell'attaccante da bloccare è 192.168.200.100 e la vittima, con IP 192.168.200.150, dovrebbe usare questa policy del firewall per bloccare il traffico in entrata che abbia origine dall'IP dell'attaccante. Si potrebbero usare anche degli IDS oppure degli IPS in grado di riconoscere oppure bloccare in tempo reale un tentativo di scansione da parte di un attaccante, oppure ancora limitare il numero di nuove connessioni che un IP può fare al secondo, per evitare che avvenga una scansione. Si possono anche abilitare i cookie SYN per limitare gli attacchi SYN Flood e ridurre l'efficacia di scansione SYN che possono essere la prima fase di un attacco più strutturato. Si può abilitare anche il port knocking per controllare gli accessi e le scansioni alle porte e in questo può essere d'aiuto anche la Single Packet Authorization SPA.

Esercizio facoltativo

CSIRT sta per Cyber Security Incident Response Team ed è un team di esperti di cybersecurity organizzato per gestire incidenti informatici di vario tipo e preparato per prevenire, mitigare e risolvere eventuali incidenti informatici. È bene che ogni organizzazione, sia essa pubblica o privata, si doti di una struttura simile ed è stato costituito CSIRT Italia, che ossia un CSIRT nazionale presso l'ANC, che è l'Agenzia per la Cybersicurezza Nazionale. CSIRT Italia aiuta a proteggere gli enti pubblici e privati dagli attacchi cyber, fornendo indicazioni pratiche per la sicurezza informatica, aiutando le aziende a rispondere a questo tipo di problematiche e collaborando anche con altre organizzazioni per migliorare la sicurezza informatica. CSIRT Italia, essendo un'unità dell'Agenzia per la Cybersicurezza Nazionale, svolge compiti di primaria importanza definiti nel Decreto Legislativo 18 maggio 2018 n.65 e dal Decreto del Presidente del Consiglio dei Ministri dell'8 agosto 2019, nell'articolo 4. Si occupa di monitorare gli incidenti di sicurezza a livello nazionale, di

emettere preallarmi, allerte, annunci e dare informazioni alle parti interessate riguardo a possibili rischi ed incidenti, di intervenire direttamente in caso di incidente, di analizzare dinamicamente rischi ed incidenti, di sensibilizzare riguardo all'importanza della sicurezza informatica e di collaborare con la rete dei CSIRT e con altri organismi europei ed internazionali. Tra gli annunci che emette CSIRT Italia vi è l'esempio di annuncio proposto nell'esercizio, riguardo alla campagna di phishing a tema "Sondaggio Trenitalia". Si basa su una email di phishing che fornisce un link per un sondaggio Trenitalia, al termine del quale il cliente fortunato riceve un pass annuale e deve inserire i propri dati personali e di pagamento per riscattare questo pass. Tra le azioni di mitigazione suggerite, figura ovviamente un controllo scrupoloso delle email, controllando i domini per capire se la mail proviene effettivamente dai domini ufficiali di Trenitalia, ossia @trenitalia.it o @fsitaliane.it. Bisogna anche evitare di cliccare su link o risorse esterne se non si è sicuri della loro provenienza, tenendo presente che un sondaggio ufficiale di Trenitalia dovrebbe portare gli utenti direttamente nel sito di Trenitalia e bisogna anche essere sicuri dei siti nei quali si inseriscono dati personali, tenendo presente che nessun sondaggio richiede di inserire dati sensibili come le informazioni personali e il pagamento. È importante continuare a sensibilizzare riguardo al phishing, per istruire il personale a trovare email sospette ed applicare tutto il Threat Intelligence life cycle. CSIRT fornisce anche un file Excel con degli IOC specifici per questa minaccia da implementare ed applicare nei propri sistemi, fermo restando che un'azienda può applicare anche altre azioni di mitigazione aggiuntive in base alla propria situazione.