VA/PT LIGHT

Operations

Is time to rethink security concept!

A great cyber security and development company

VA/PT LIGHT

Operations

RACCOLTA INFORMAZIONI

Il cliente provede a comunicare a SEC4U, attraverso un apposito modulo, alcune informazioni relative alle risorse presenti nella propria infrastruttura. Queste informazioni possono ad esempio comprendere il dominio aziendale e l'ip pubblico principale utilizzato dall'organizzazione, oppure la banda internet e interna a disposizione. Possono anche comprendere informazioni meno tecniche quali il range orario durante il quale il cliente desidera che il VA/PT venga svolto e le figure di riferimento all'interno dell'organizzazione.

MODALITA' DELLA VERIFICA

Il servizio VA/PT Light viene effettuato, salva diversa indicazione, in modalità remota.
Le risorse pubbliche (raggiungibili attraverso la rete Internet) verranno esaminate utilizzando un canale pubblico, mentre le risorse presenti nella rete locale verranno sottoposte a verifica utilizzando un canale privato ad elevato standard di sicurezza (VPN – Virtual Private Network) configurato allo scopo.

RISORSE SOTTOPOSTE A VERIFICA

Le risorse che vengono sottoposte a verifica, nel pacchetto base di VA/PT Light, sono:

- massimo 1 ip pubblico, con analisi dell'esposizione dei vari servizi;
- 1 router che fornisce connettività internet all'organizzazione. Del router, nel caso in cui il cliente sia d'accordo nel fornire a SEC4U le credenziali di autenticazione, viene verificata la configurazione dal punto di vista della security (es. aggiornamento firmware necessario, interfaccia di manutenzione remota abilitata con accesso illimitato, eventuali reti wireless configurate in modo non appropriato, utenti di default configurati,...);
- 1 firewall, se presente. Del firewall, nel caso in cui il cliente sia d'accordo nel fornire a SEC4U le credenziali di autenticazione, viene verificata la configurazione dal punto di vista della security (es. aggiornamento software necessario, servizi di manutenzione remota esposti, utenti di default configurati,...) e la correttezza logica delle ACL (Access Control List) configurate;
- massimo 255 hosts privati (1 network /24), indipendentemente dalla tipologia di dispositivo individuato;
- 1 dominio aziendale, del quale viene verificata l'eventuale esposizione di account dello stesso in database contenenti credenziali oggetto di data breach. Viene data evidenza degli account che risultano compromessi, in modo tale da permettere al cliente una tempestiva strategia di remediation.

Delle varie risorse individuate vengono verificati i seguenti fattori:

- tipologia del device;
- versione del sistema operativo, se individuata;
- tipologia di traffico generato (cifrato, in chiaro,…);
- evidenza del traffico anomalo, se rilevato
- presenza credenziali di default;
- servizi esposti e per ogni servizio esposto:
  - presenza vulnerabilità risconosciute;
  - se concesso, eventuale exploit delle vulnerabilità.

CREAZIONE REPORT

Al termine dell'attività SEC4U redige un report, che viene messo a disposizione del cliente attraverso il modulo **VA/PT Report** della web application **UIDAPO** (www.uidapo.com) e che riassume tutte le operazioni effettuate.

Il report, generato seguendo le linee guida stabilite nel documento NIST SP 800-115, in modo tale da adeguare il report stesso ad uno standard facilmente analizzabile e ripetibile, viene suddiviso nelle seguenti sezioni:

- Sommario Esecutivo
  - Sintesi Dei Risultati
  - Grafico Vulnerabilità

In questa sezione rientrano lo Scope of Engagement della verifica, contenente il

perimetro che è stato individuato per le attività di VA/PT. Inoltre contiene la parte discorsiva del report ed un grafico con la gravità ed il numero di vulnerabilità rilevate, utile per dare un'informazione istantanea alle persone non tecniche dell'organizzazione.

- Report Vulnerabilità

In questa sezione vengono descritte a livello tecnico le singole vulnerabilità rilevate, assegnando per ognuna di essere un valore di impatto (utilizzando lo standard internazionale CVSS), delle referenze, gli eventuali ID di vulnerabilità presenti nei diversi database pubblici (CVE, OSVDB, BID, CERT, CWE,...), un Proof of Concept della vulnerabilità (può trattarsi di uno screenshot oppure di un output di un comando), la lista dei target vulnerabili.

- Piano Di Risanamento
  - Raccomandazioni
  - Livello Di Rischio

Questa è la sezione più importante del report, nella quale vengono consigliate e descritte le operazioni da effettuare al fine di migliorare la postura difensiva dell'organizzazione. Questo può comprendere l'adozione di tecnologie che possono essere d'aiuto per elevare il livello di sicurezza, oppure la necessità di seguire determinate policies per avviare un programma di security che agisca nel continuo, oppure ancora il bisogno di avviare una strategia di formazione per migliorare la security awareness del personale. Viene inoltre stabilito, a fronte delle vulnerabilità rilevate, il livello di rischio dell'organizzazione.

- Appendice A: Dettaglio delle vulnerabilità e loro mitigazione/soluzione

In questa sezione, per ogni vulnerabilità rilevata, viene attribuito un fattore di rischio e viene messa a disposizione una soluzione.

- Allegati Vari

In questa sezione possono trovare spazio eventuali screenshot catturati durante la verifica, oppure l'outputi di comandi eseguiti oppure ulteriori prove e dimostrazioni di quanto effettuato.

- Logs

Questa sezione descrive quali macro attività sono state effettuate da SEC4U in fase di verifica e in fase di stesura del report.

PERSONALE CERTIFICATO

SEC4U esegue le attività di Vulnerability Assessment e di Penetration Test avvalendosi di personale altamente qualificato e certificato CEH (Certified Ethical Hacker) e eCPPT (eLearnSecurity Certified Professional Penetration Tester).