CENTRO STUDI CYBER DEFENSE

CERBEYRA

your safe digital future

Penetration Test

Servizi professionali avanzati per un futuro digitale sicuro

Premessa

Le informazioni sono un bene che aggiunge valore ad una organizzazione e le soluzioni di sicurezza rappresentano sempre di più un nuovo mezzo per arricchire la relazione tra processo di business e tecnologia.

Le decisioni e le strategie di security non devono essere vissute come un obbligo ma come un investimento, la protezione di dati confidenziali da possibili furti o distruzione fa si che un'organizzazione aumenti la propria competitività e protegga quindi con successo dati "riservati" come quelli dei propri clienti, dell'innovazione su nuovi prodotti, strategie di mercato ed altro.

La sicurezza aiuta a proteggere l'immagine di un'azienda. Il Penetration Test e Hacking Etico di Cerbeyra offre un servizio professionale per l'analisi e l'individuazione di falle nella sicurezza delle informazioni nelle infrastrutture ICT e nei processi delle organizzazioni, siano essi di livello logico, fisico o organizzativo.

Pen Test e Hacking Etico (PTHE)

Il PTHE è un servizio che consiste in una serie di verifiche, tecnologiche ed organizzative del grado di adeguatezza ed efficacia operativa delle misure di protezione esistenti nell'infrastruttura ICT di fronte a potenziali minacce provenienti dall' esterno della propria struttura o derivanti da debolezze o criticità dei processi interni di gestione del sistema.

Il servizio emula scenari di attacco sofisticati che possono avere un impatto sull' organizzazione secondo un preciso schema di "Kill Chain". I risultati dei test di penetrazione vengono raccolti in un report dettagliato, che oltre ad evidenziare gli eventuali punti deboli, fornisce indicazioni utili sulle azioni necessarie per eliminare le vulnerabilità, e raccomandazioni tattiche e strategiche per la gestione dei processi deboli. Al fine di fornire una valutazione ragionata e più efficace dello stato di vulnerabilità della struttura ICT, il servizio PTHE prevede un approccio "gray box" dove cioè l'audit viene svolto attraverso una cooperazione riservata e limitata tra il Red Team di Cerbeyra, addetto al PTHE, e solo alcune figure aziendali opportunamente individuate dalla direzione.

Le attività di analisi sui sistemi sono condotte secondo un approccio metodologico composto dalle seguenti fasi principali:

- **Ricognizione (Information Gathering)** dell'infrastruttura ICT e dell'organizzazione oggetto di analisi;
- **Scansione (Weaponization)**, verifica delle superfici di attacco e preparazione dei test personalizzati di vulnerabilità dei sistemi attraverso l'utilizzo di strumenti software semiautomatici, pen-test dimostrativi fisici e organizzativi;
- **Simulazione di attacchi (Attack)** automatici e manuali anche con attività non convenzionali;
- **Analisi delle evidenze**, analisi e correlazione dei risultati prodotti dalla fasi precedenti, al finedi migliorare la conoscenza in merito a possibili vulnerabilità;
- **Presentazione Report** finale e raccomandazioni.

Tipologie di Test

Il PTHE è un servizio che dispone di tre tipologie di test:

- **PTHE Logico** a sistemi ICT (network, sistemi e applicativi on premise e in cloud);
- **PTHE Cognitivo** attività di Social Engineering sull'organizzazione oggetto di analisi;
- **PTHE Fisico** accesso aree riservate, impersonificazione ed attacchi tramite dispositivi fisici.

PTHE LOGICO

I Penetration Test Logici vengono effettuati attraverso due modalità:

- **Automatica**: utilizzando la nostra piattaforma CTI Cerbeyra che effettua test automatici approfonditi ed estensivi su tutte le vulnerabilità note e descritte dagli enti internazionali di certificazione NIST e MITRE;
- **Manuale**: utilizzando appositi script/applicazioni creati "ad hoc" per l'organizzazione unitamente a tecniche e metodologie manuali non convenzionali.

I metodi utilizzati nel PTHE Logico si basano sulle "best practices" internazionali e su tre standard tecnologici:

- **OSSTMM** il manuale dell'Institute for Security and Open Methodologies;
- **OWASP** l'organizzazione indipendente per diffusione della sicurezza delle applicazioni WEB;
- **PTES** la metodologia Penetration Testing Execution Standard.

PTHE COGNITIVO

Il Penetration Test Cognitivo viene effettuato attraverso attacchi di manipolazione delle informazioni ed impersonificazione, o più comunemente noto come Social Engineering, in particolare il PTHE Cognitivo può utilizzare le seguenti tipologie di attacco:

- **computer based**: utilizzo di campagne di spear phishing progettate in maniera specifica per l'organizzazione;
- **mobile based**: utilizzo di campagne di spear phishing su dispositivi mobili, progettate in maniera specifica per l'organizzazione;
- **human based**: basate sul contatto diretto tra attaccante e vittima attraverso sistemi di comunicazione remota (ad es. telefono, social network, etc.), o fisicamente.

Obiettivo dell'attacco è l'esfiltrazione di dati attraverso inoculamento di malware o dataleak.

- L'aggressore identifica la vittima
- Vengono raccolte informazioni sulla vittima
- Gli aggressori cercano il metodo migliore per hackerare la vittima

- Fornire alla vittima informazioni fittizie
- Creazione di una storia ingannevole
- Adescare la vittima in trappola

- Investire tempo e risorse per guadagnarsi la fiducia della vittima
- Lanciare l'attacco
- Ottenere i dati necessari

- Dopo la falla, uscire senza provocare dubbi
- Cancellare malware
- Copertura

PTHE FISICO

Il test di penetrazione fisica si concentra su test di controllo della sicurezza fisica, per individuare sistemi, procedure e/o comportamenti anche non intenzionali fallibili.

Il test di penetrazione fisica viene attuato tramite le seguenti principali tipologie di attacco:

- **Piggybacking**: tentativo, attraverso la persuasione e l'empatia, di convincere una terza persona autorizzata a concedere l'accesso ad aree riservate e/o documenti riservati;
- **Tailgaiting**: sfruttare l'accesso di utenti autorizzati per accedere ad aree riservate e/o documenti riservati;
- **Reverse Social Engineering**: generare scenari "artefatti" in cui il red team viene autorizzato dall'organizzazione stessa ad accedere aree riservate e/o documenti riservati.

Cyber Security Center

I **Servizi PTHE** sono direttamente erogati dal **Centro Studi Cyber Defense Cerbeyra**. Il Centro Studi nasce internamente al progetto **Cerbeyra** (la nostra piattaforma di Cyber Threat Intelligence), nel **polo di Cyber Security** del gruppo Vianova, operatore nazionale di rete fissa e mobile, di servizi voce e dati avanzati ed integrati per le imprese.

Il Centro si occupa di analizzare e studiare le cyber minacce ed i potenziali scenari di attacco che possono compromettere la sicurezza delle informazioni dei nostri clienti. Il Centro è formato da diversi team di analisti ed esperti in cyber security e collabora attivamente con realtà esterne di ricerca (ad es. università, community di sicurezza informatica, etc.).

Il Red Team è il team del centro studi deputato all'erogazione dei servizi PTHE, si avvale di personale altamente qualificato e referenziato, Ethical Hacker, Security Analyst, Computer Forensic Investigator, system e network engineer e sviluppatori sw con almeno 15 anni di esperienza sul campo, in possesso sia di certificazioni professionali in ambito ICT Security (ECSA, CEH, CompTIA Security+, MCITP Security, etc.) sia di specifiche certificazioni in ambito sistemistico (CCNA, MCSA, MCITP, LPIC - Linux prof. Cert., etc.). Tali certificazioni garantiscono, oltre alla competenza tecnica, anche l'alto profilo etico delle figure professionali impiegate.

CERBEYRA
your safe digital future

Cerbeyra S.p.A. - Gruppo Vianova S.p.A
Via Libeccio 48/F - Z.I. Cotone
55049 Viareggio (LU)
P.IVA e CF 01766360463

www.cerbeyra.com | info@cerbeyra.com | 0584.43671