Vulnerabilità e Rischi effettivi

Cos'è un Vulnerability Assessment & Penetration Test

È un'analisi che impiega tecniche di hacking avanzate per valutare la sicurezza informatiche delle organizzazioni rilevando le vulnerabilità, mostrandoti evidenze sugli impatti e relative azioni di rimedio da intraprendere.

Perchè attuare un VA/PT

- Scoprire la propria esposizione digitale (OSINT)
- Testare le configurazioni degli apparati di difesa
- Identificare le aree compromettibili
- Valutare la sicurezza dei sistemi informativi
- Verificare i sistemi di sicurezza come antivirus e firewall

Come Funziona

L'attività prevede una mappatura del perimetro digitale, identificando apparati interni ed esterni (esposti su internet), tali apparati vengono inoltre scansionati al fine di rilevare le possibili vulnerabilità da sfruttare, attraverso tecniche usate dal cyber crime andiamo a rilevare il rischio reale a cui un'organizzazione è esposta, fornendo un report dettagliato comprensivo di rimedi tecnici ed evidenze di compromissione.

Title	Microsoft Windows SMB Server Multiple Vulnerabilities-Remote				
Reference	R01	Risk Rating	Critical	192.168.1.1	9.5
Technical Overview	La seguente vulnerabilità presente nel servizio SMB permette ad utente malintenzionato di inviare messaggi malformati al servizio di Microsoft Server Message Block (SMB) consentendo l'esecuzione di codice come utente privilegiato SYSTEM I dettagli della vulnerabilità risultano pubblici, inoltre sono disponibili tool (exploit) per lo sfruttamento della falla.				
Attack Conditions	Attaccante locato in una postazione remota con accesso alla rete internet				
Business Impact	Accesso completo al Server Estrazione di credenziali di Dominio Esfiltrazione e cancellazione di qualunque dato presente sul serve				

Attività della valutazione

* Open Source Intelligence
* Mappatura dei servizi esposti
* Scansione delle vulnerabilità
* Tecniche di compromissione
* Configurazioni di Dominio
* Verificare contesti di Privilege Escalation
* Evidenziare i movimenti laterali possibili
* Azione di rimedio

Michele Vezzoli
Cyber Security Consultant
+39 3280555322
mv@longinoconsulting.net

LONGINO
cyber security consulting

longinoconsulting.net