V.I.S.A.

VoIP Infrastructure Security Assessment

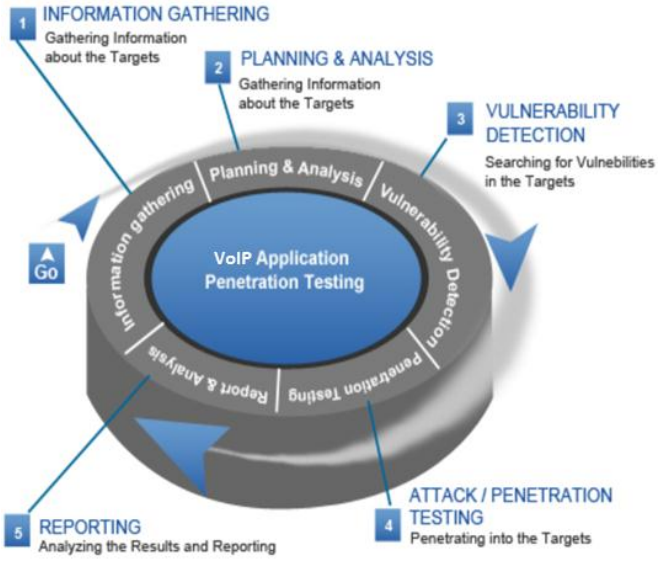
NCP – Networking Competence Provider Srl
Sede legale: Via di Porta Pertusa, 4 - 00165 Roma
Tel: 06-88816735, Fax: 02-93660960
info@ncp-italy.com

Introduzione

Il *penetration testing*, conosciuto anche come ***ethical hacking***, ha come obiettivo quello di simulare le tecniche di attacco adottate per compromettere i sistemi. Esso mette a nudo le vulnerabilità ICT che possono esporre le aziende a serie minacce da parte di hacker senza scrupoli. E' l'arte del *legal/ethical hacking* dove una squadra di specialisti, denominato Red Team o **Tiger Team**, verifica e documenta il livello di sicurezza di un sistema. **V.I.S.A**. è un metodo ideato da NCP, che applica le più moderne metodologie e le più efficaci *best practices* dell'*ethical hacking* ai sistemi VoIP.

V.I.S.A.

- V.I.S.A. è un servizio per la valutazione dello stato di sicurezza di un sistema VoIP.
- V.I.S.A. ha lo scopo di **evidenziare le debolezze**, **valutare l'entità dei rischi**, **offrire concreti rimedi**.
- V.I.S.A. è una soluzione sviluppata a partire da metodologie riconosciute a livello internazionale, in particolare, **OSSTMM** che maggiormente si focalizza sulla sicurezza ICT.
- V.I.S.A. produce **risultati reali misurabili** basati sull'indice RAV.
- V.I.S.A. assicura risultai concreti di utilità pratica: qual è la prima cosa da proteggere, qual è il reale grado di esposizione ai pericoli, qual è la superficie di attacco, qual è il rapporto spesa/benefico relativo all' adozione di una specifica soluzione di sicurezza.
- V.I.S.A. offre al management **report chiari e precisi** che facilitano la comprensione.
- V.I.S.A. è costituito da due momenti principali, denominati ***Vulnerability Assessment/Detection*** (ciclo passivo) e ***Penetration Test*** (ciclo attivo), inseriti in un processo ben collaudato composto da 5 fasi successive, che iniziano con la raccolta dei dati e terminano con la produzione dei report.



Vulnerability Assessment (ciclo passivo)

- La metodologia di **Vulnerability Assessment** è un processo volto a valutare il livello di sicurezza dei sistemi senza portare attacchi. Lo scopo è quello di trovare le falle di uno specifico sistema attraverso una **analisi passiva**, basata principalmente sulla raccolta dei dati. **Produce come output un documento che elenca le vulnerabilità e ne propone i rimedi**.
- L'utilizzo del VA si rende necessario più volte durante l'arco di un anno, in quanto gli strumenti di attacco aumentano con il progredire la tecnologia. Le **fasi tipiche** di un VA sono:

- Pre-Assessment Analysis
- Information Gathering
- Port Scanning
- Enumeration
- Threat Profiling & Risk Identification
- Network Vulnerability Assessment
- System Vulnerability Assessment
- VoIP Infrastructure Security Assessment
- Engagement Analysis
- Mitigation Strategies
- Report Generation
- Support

ID	Rischio	Classificazione
Predisposizione		
A.1	Traffico RTP non cifrato	Alto
A.2	Possibilità registrazione conversazioni tra endpoint	Alto
A.3	Possibilità accesso a firmware configurazioni endpoint	Alto
A.4	Possibilità falsificazione interno chiamante	Alto
A.5	Possibilità di ascoltare messaggi presenti in segreteria telefonica	Alto
A.6	Possibilità di effettuare chiamate da utenze fittizie	Alto
A.7	Possibilità di eludere controlli del dialplan	Alto
A.8	Enumeration utenze sip registrate	Medio
A.9	Possibilità di interruzione di servizio (Denial of Service – DoS)	Medio
A.10	Possibilità accesso a server web integrato negli endpoint	Basso

A.1 – Traffico RTP non cifrato.	
Situazione rilevata: Il trasporto "end to end" di dati audio avviene attraverso l'utilizzo del protocollo RTP. Non risultano essere presenti particolari accorgimenti di sicurezza nella gestione del traffico VOIP.	
Rischio: Il protocollo non comprende forme di crittografia esponendo il payload (audio) alla problematica di registrazione o ascolto fraudolento delle conversazioni tra endpoint. Questo potrebbe causare: ▪ Perdite finanziarie dirette o indirette dovute ad un utilizzo non lecito della registrazioni o delle informazioni carpite. ▪ Perdita di immagine nel caso in cui informazioni riservate vengano rese di dominio pubblico. ▪ Impossibilità di identificazione di una avvenuta frode/dolo se non ex-post.	
Controlli di Mitigazione già in essere: Nessuno.	
Valutazione dell'Impatto:	Alto
Valutazione della Probabilità:	Medio
Valutazione del Rischio Specifico:	Alto
Raccomandazioni: • introduzione protocollo SRTP per la cifratura del traffico dati (voce). • Valutare aggiornamento PBX.	
Costo Stimato:	Medio (necessità di una valutazione approfondita sia degli endpoint, sia dei media gateway utilizzati)

Esempi di report tipici prodotti da un VA.

Penetration Test (ciclo attivo)

- In informatica, il **Penetration Test** è il processo operativo di valutazione della sicurezza di un sistema che simula un vero attacco. L'**analisi è di tipo attivo**, comprende più fasi ed ha come obiettivo evidenziare le debolezze della piattaforma fornendo il maggior numero di informazioni sulle vulnerabilità. L'analisi è condotta dal punto di vista di un potenziale attaccante e consiste nello sfruttamento delle vulnerabilità rilevate al fine di ottenere più informazioni possibili per accedere indebitamente al sistema.
- Tutti i problemi di sicurezza rilevati vengono quindi presentati al cliente assieme ad una valutazione del loro impatto nel sistema in relazione al business aziendale, fornendo inoltre una rapporto tecnico che presenta proposte di migrazione e/o mitigazione del sistema. Le fasi tipiche di un PT sono:

- Exploit Research & Development
- Exploitation
- Privilege Escalation
- Network Propagation
- Retaining Access
- Engagement Analysis
- Mitigation Strategies
- Report Generation
- Support

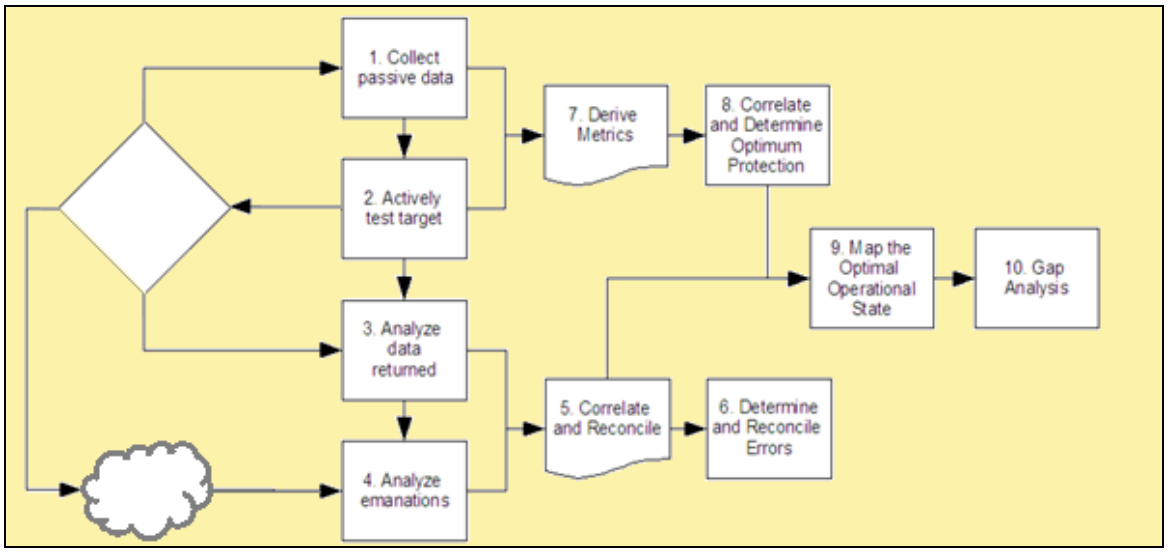
A.2 Enumeration SIP User	
TipologiaAttacco	Attacco Interno/Esterno
Grado di rischio	Medio
0-Day	Si
Uri per la risoluzione	Nd
Problema di sicurezza	Identificazione username registrata
Effetto	Accesso con credenziali di terzi
Analisivulnerabilità	
Effettuando una craft REGISTER è stato possibile notare che il PBX risponde in modo diverso in conformità all'esistenza o meno del utente sip. Si riporta esempio: *REGISTER sip:500@127.0.0.1 SIP/2.0* *CSeq: 123 INVITE* *Via: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK78xdb2cd-0671-e011-81e1-e1816009ce7e;rport* *From: <sip:500@127.0.0.1>;tag=642a29cd-0671-e011-81e1-e1816009ce7e* *Call-ID: 571579d6e5814df04ec7cd42672738r* *To: <sip:500@127.0.0.1>* --- *Method: REGISTER* --- *Valid user (user 500)* *Response:* --- *SIP/2.0 401 Unauthorized* --- *Invalid user (user 501)* *Response:* --- *SIP/2.0 484 Address Incomplete*	
Soluzione	
• Aggiornare il sistema PBX alla nuova versione • Modificare il file di configurazione variando le direttive necessarie all'hardening (es: alwayauthreject) • Abilitare TLS	

Esempio di report tipici prodotto da un PT.

OSSTMM - Open Source Security Testing Methodology Manual

- Uno standard internazionale per i test e le analisi di sicurezza
- Una metodologia basata su metodi scientifici
- Un mezzo per misurare la sicurezza operativa oggettivamente
- Un processo concreto per essere funzionali e realmente sicuri
- Un mezzo per ridurre in modo sostanziale i falsi positivi ed i falsi negativi

La metodologia OSSTMM, al fine di garantire la massima copertura del perimetro, comprende cinque canali: Human, Physical, Wireless, Telecommunications e Data Networks.



- OSSTMM introduce una scala metrica per la misurazione del livello di sicurezza ed esposizione, permettendo quindi una **valutazione oggettiva del rischio tecnologico** legato al contesto oggetto di analisi.
- Questa metrica di sicurezza è definita **RAV, acronimo per *Risk Assessment Value***, la quale trova un suo naturale impiego nell'instaurare un dialogo tra chi valuta gli aspetti tecnologici della sicurezza e chi, invece ne tocca gli aspetti più orientati ai processi.