Vulnerability scanning

Metodi e strumenti per la Sicurezza informatica

Claudio Telmon
claudio@telmon.org

Vulnerability assessment vs Penetration testing

- Si tendono a distinguere in funzione di quanto il tester “si mette nei panni” di un vero attaccante
  - Time consuming, non sempre vale la pena
- Si possono considerare tutte le gradazioni
- Parametri:
  - Collaborazione (anche “eccessiva”) da parte del personale
  - Verifiche non tecniche
    - Organizzazione, Social Engineering, sicurezza fisica, dumpster diving...
- Un pen-test sfrutta più canali, ma è più vincolato
  - es. se la sicurezza fisica è “efficace”, non si va oltre
  - Può richiedere di causare danni

Vulnerability scanning

- Parte di entrambi gli approcci
- Attività svolta dalla rete
- Rete interna
  - Per la ricerca diretta di vulnerabilità
- Rete esterna
  - Più “simile” al penetration testing
- Richiesto da alcuni standard (es. PCI-DSS)

Limiti concettuali

- Si rilevano le vulnerabilità del software presenti e rilevabili al momento del test
  - Dipendente dalle politiche di patch management
  - Dipendente da condizioni temporali ecc.
    - funzioni che sono attivate solo in determinati istanti
    - Condizioni che si presentano occasionalmente
- Si verificano le vulnerabilità note
  - Al momento del test
  - Al tester (ma sono tutti bravi...)

Limiti pratici

- Le condizioni non sono le stesse di un attaccante
  - Non si devono danneggiare i sistemi in esercizio
  - Non si possono attaccare terzi
- È facile disturbare l'analisi
  - es. nmap vs. firewall
- Non sempre si possono testare tutte le funzionalità
  - es. attività autenticate “non reversibili”

Usi

- L'uso corretto è una verifica dopo un vulnerability assessment con accesso completo
  - Può sempre sfuggire qualcosa, almeno si rilevano gli errori grossolani
- Altri usi
  - Audit: può dare una “sensazione generale” dello stato della rete
    - L'audit dà generalmente priorità ai problemi più gravi
  - Awareness: utile per “dare una scossa”

Rischi

- “Se non ci sono vulnerabilità, il sistema è sicuro”
- “Mostrami delle vulnerabilità e crederò che il sistema non è sicuro”
- Sono affermazioni corrette o sbagliate in funzione del livello di sicurezza che si vuole raggiungere, ovvero del rischio che si è disposti ad accettare
  - Forse adatto ad una tipica PMI
  - Inadatto a contesti più critici
- Affidabilità del tester

Affidabilità del tester

- Si mette una persona in condizione di attaccare liberamente sistemi in esercizio
  - Causerà danni?
  - Ci racconterà tutto?
  - Quanto sa? Come ha ottenuto le sue competenze? Come le mantiene?
- “Soluzione”: attività monitorata su sistemi aziendali

Rilevanza degli “zero day”

- Gli zero-day di oggi sono vulnerabilità note di domani
  - È utile conoscerli oggi?
  - Rientrano nel perimetro di un test di questo tipo?
- La protezione deve essere architetturale
- La loro rilevanza è sempre minore: gli attacchi si spostano verso il livello applicativo e le personalizzazioni

Metodologia

- Raccolta indiretta di informazioni
- Raccolta diretta di informazioni
- Test ai diversi livelli

- Riferimento generale: OSSTMM, good practice accettata
  - L'uso di metodologie accettate è importante per dare credibilità alle verifiche, specialmente rispetto a terzi

www.osstmm.org

Uso di “appliance” ad hoc

- Ci sono diversi prodotti che hanno come scopo automatizzare una serie di test di base
  - Compliance a determinati standard/requisiti
- Vantaggi:
  - non serve una competenza specifica
  - possono essere usati periodicamente
  - Sono aggiornati dal produttore
- Limiti:
  - Solo test molto standard (ma spesso basta)

Raccolta indiretta di informazioni

- DNS
- Whois
- Google
- ...
- Tutto quello che può fornire indirizzi IP, punti di accesso, nomi, email, e spesso interi domini “dimenticati”

Raccolta diretta

- Strumenti tradizionali
  - Ping, telnet, treceroute, snmp...
- Strumenti specializzati
  - Nmap, hping...
- Strumenti di network discovery
  - Principalmente da rete interna
- Tutti questi strumenti “si fanno notare”, chi più chi meno

NMAP

uso