]HackingTeam[

HT S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946

Allegato Tecnico

Progetto di Analisi della Sicurezza

Obiettivo

E' richiesta dal cliente un'analisi della sicurezza reti/sistemi del perimetro internet ed un'analisi della sicurezza relativa ad applicazioni Web. L'obiettivo principale è quello di rilevare potenziali minacce alla sicurezza informatica impattanti sul business aziendale e sulla proprietà intellettuale relativa a i propri progetti.

Non viene richiesta un'analisi approfondita e di elevato dettaglio bensì un'attività mirata ad evidenziare potenziali minacce facilmente sfruttabili al business del cliente.

Target of evaluation (TOE)

- TOE#1 - Rete esterna:
  - ✓ massimo 31 indirizzi IP raggiungibili, suddivisi in 3 sedi.
- TOE#2 – Applicazioni :
  - ✓ 2 applicazioni Web.

Assunzioni

- Si assume che il perimetro esterno verso internet non abbia alcun tipo di meccanismo di protezione che potrebbe rallentare sensibilmente l'attività di hacking.
- Le attività verranno effettuate dai laboratori HT.

Vincoli

- E' necessaria la sottoscrizione da parte del cliente di una liberatoria che autorizzi HT a poter effettuare azioni di hacking altrimenti non consentite.

HT S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946

- Qualora alcuni asset del target fossero in gestione o in hosting presso un outsourcer è necessaria la sottoscrizione da parte di quest'ultimo della liberatoria che autorizzi HT a poter effettuare azioni di hacking altrimenti non consentite.
- HT dovrà sottoscrivere un NDA (Non Disclosure Agreement) a tutela delle informazioni di cui è venuta in possesso prima e durante le attività.

Metodologia di ethical hacking seguita

- Analisi non invasiva
  - ✓ Information Gathering e footprinting: questa fase ha lo scopo di raccogliere il maggior numero di informazioni sull'obiettivo che si intende attaccare senza "toccare" l'obiettivo stesso, ovvero effettuando una cosiddetta "analisi non invasiva". In particolare in questa fase si cerca di determinare: *domini, blocchi di rete e indirizzi IP dei sistemi direttamente collegati a Internet*. Gli strumenti utilizzati sono: Search Engine, Whois server, Arin database, interrogazione DNS, ecc.
  - ✓ Scanning: l'obiettivo dello scanning è ottenere una mappa più dettagliata possibile del sistema da attaccare. Ciò significa acquisire informazioni su quali indirizzi IP dei blocchi di rete trovati nella fase precedente siano effettivamente "contattabili" dall'esterno (IP discovery), quali servizi siano "attivi" (TCP/UDP port scan) e, infine, quali sistemi operativi "posseggano". Gli strumenti utilizzati sono: interrogazioni ICMP (gping, fping, ecc.), scansione delle porte TCP e UDP (strobe, netcat, nmap, ecc.), fingerprint dello stack (nmap, ethercap).
- Analisi invasiva
  - ✓ Enumeration: con questa fase si inizia l'"analisi invasiva". Si effettuano, infatti, connessioni dirette ai server e "interrogazioni" esplicite. Tali attività potrebbero, a seconda della configurazione presente sui sistemi target, originare dei logs sui sistemi (tipicamente su sistemi di controllo). Attraverso

HT S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946

l'enumerazione si vuole giungere a identificare, sulle macchine riscontrate come raggiungibili, account validi (list user accounts), risorse condivise (list file shares) e applicazioni attive sulle porte in ascolto (identify application). Le tecniche utilizzate variano a seconda dei sistemi operativi delle macchine che vogliamo analizzare.

- Attacco
  - ✓ Gaining Access: una volta ottenute le informazioni del punto precedente, inizia il vero e proprio attacco che ha come obiettivo riuscire a "entrare" nel sistema remoto. I metodi utilizzati anche in questo caso dipendono dal sistema operativo della macchina target, ma si basano sostanzialmente sulla ricerca di password corrispondenti agli utenti trovati (password guessing), sullo sfruttamento di errori progettuali delle applicazioni e servizi attivi sul server (buffer overflows, attacchi data driven, ecc.) o del sistema operativo stesso.
  - ✓ Escalating Privileges: l'obiettivo di questa fase è sfruttare i risultati ottenuti nella fase precedente per ottenere il pieno controllo del sistema remoto attaccato. Ciò si ottiene, per esempio, reperendo i files presenti sul sistema che contengono le password (/etc/passwd, SAM, ecc.) e tentando di decifrare le password in essi contenute (password cracking), oppure utilizzando appositi exploits.
- Consolidamento
  - ✓ Pilfering: se si giunge a questa fase significa che si è ottenuto il pieno controllo del sistema target. Quindi è bene valutare la configurazione del sistema stesso al fine di capire se, dove e cosa il sistema registra (logs). I sistemi di auditing saranno eventualmente disabilitati (es. con Win NT mediante auditpol). A questo punto la macchina in oggetto può diventare una "testa di ponte" per attaccare altre macchine. In tal caso saranno reperite informazioni riguardanti altri sistemi.

HT S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946

Attività previste relative al TOE#1

- Ethical hacking

Attività previste relative al TOE#2

- Web application assessment