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 Ethical Hacking

Obiettivo

E' richiesta dal cliente un'analisi della sicurezza reti/sistemi del perimetro internet ed un'analisi della sicurezza applicativa di due applicazioni web interne (una delle quali pubblicata su internet).

Per quanto riguarda il firewalling esterno (1 fw Telecom e 1 fw AtaHotels) è richiesta un'attività di controllo e verifica della presenza di vulnerabilità DoS, ovvero di quelle minacce che se sfruttate potrebbero causare un disservizio.

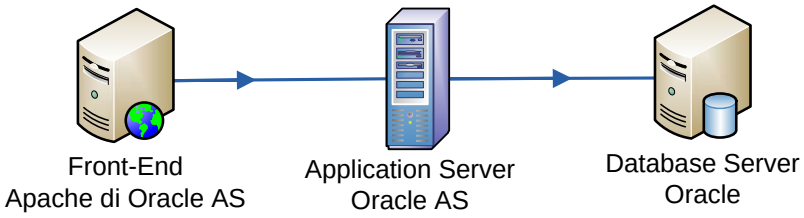
Per quanto riguarda invece la parte applicativa è richiesta l'esecuzione dei test sia in modalità black-box (senza alcuna informazione), sia in modalità white-box (possedendo una tipologia di credenziali per ogni applicazione)

Target of evaluation (TOE)

- TOE#1 - Rete esterna:
  - ✓ massimo 3 indirizzi IP raggiungibili
- TOE#2 - Rete interna:
  - ✓ 2 applicazioni web-based
  - ✓ Ogni applicativo ha una login di accesso
  - ✓ Uno dei due applicativi ha anche una parte pubblica non soggetta ad autenticazione (questa applicazione viene difesa da un firewall applicativo)

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

Architettura applicativa



Assunzioni

- Le pagine con campi di inserimento sono ipotizzate essere al massimo 30 per ognuna delle 2 applicazioni.
- Si assume che le 2 applicazioni sotto esame non abbiano meccanismi di protezione che potrebbero rallentare sensibilmente le attività di hacking. Si ipotizza che non esistano particolari flussi applicativi che regolino l'autorizzazione a vedere o meno parti di applicazione.
- 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. Per la parte interna verrà inserito in rete un device controllato da HT (previa approvazione da parte del cliente).

Vincoli

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

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 TOE#1

- Analisi non invasiva
  - ✓ Information Gathering
  - ✓ Footprinting
  - ✓ Scanning
- Analisi invasiva
  - ✓ Enumeration
- Attacco
  - ✓ Gaining Access
  - ✓ Escalating Privileges
- Consolidamento
  - ✓ Pilfering

Attività TOE#2

- Authentication brute forcing and bypassing
- Web application Assessment
  - ✓ Cross-site scripting
  - ✓ Parameter tampering
  - ✓ Hidden field manipulation
  - ✓ Backdoors e opzioni di debug
  - ✓ Stealth commanding
  - ✓ Forceful browsing
  - ✓ Buffer overflow
  - ✓ Cookie poisoning
  - ✓ Configurazioni errate
  - ✓ Vulnerabilità note
  - ✓ SQL injection
  - ✓ Attacchi Man-in-the-Middle