]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 Ethical Hacking

Obiettivo

E' richiesta dal cliente un'analisi della sicurezza di una applicazioni Web, sia in modalità black box sia in modalità white box

Target of evaluation (TOE)

- 1 Applicazione WEB.

Assunzioni

- Si assume che le web applications pubblicate in internet 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 esterna.
- Si assume che la rete interna non abbia alcun tipo di meccanismo di protezione che potrebbe rallentare sensibilmente l'attività di hacking interna.
- Le attività verranno effettuate dai laboratori HT. Per la parte interna verrà inserito in rete un device controllato remotamente da HT (previa approvazione da parte del cliente).

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

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.

Attività previste sul TOE#1

- Web application assessment sia in modalità black-box, senza credenziali, sia in modalità white box, con credenziali fornite dal cliente.
    - La metodologia seguita è descritta nella parte "Metodologia di web application assessment"
    - Delivery: report tecnico e documento di sintesi

Metodologia di ethical hacking su reti e sistemi

- 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

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

"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 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.

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

- 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.
  - ✓ Covering traces and creating backdoors (NON richiesta): prima di abbandonare il sistema "conquistato" vengono cancellati gli eventuali logs che hanno registrato la presenza clandestina ed eventualmente installati trojan o back-doors che consentano di rientrare facilmente sulla macchina in un secondo momento. Può essere utile anche installare tools nascosti quali sniffers o keyloggers al fine di catturare altre password del sistema locale o di altri sistemi ai quali utenti ignari si collegano dalla macchina controllata.

Metodologia di web application assessment

- Authentication brute forcing and bypassing: accesso alle aree riservate da parte di utenti non in possesso di opportune credenziali
  - ✓ Descrizione: consiste nella sottomissione, spesso con l'ausilio di tools automatici, di un grande numero di credenziali (ad esempio coppie username, password), fino ad ottenere una risposta di autenticazione riuscita dal sistema.
- Web application Assessment
  - ✓ Cross-site scripting*:* furto d'identità ai danni di utenti di applicazioni web che fanno uso di cookie per la gestione delle sessioni.
    - o Descrizione: si tratta di una tecnica che, mediante l'inserimento di elementi di scripting nei parametri inviati all'applicazione, provoca l'esecuzione degli stessi da parte del browser della vittima. In alcuni casi particolari le stesse tecniche e le stesse vulnerabilità applicative possono essere sfruttate per provocare l'esecuzione di codice sul server (esempio: Server Side Include, ecc.). Gli

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

elementi di scripting causano l'invio dei cookie settati dall'applicazione target sul browser della vittima verso server un HTTP sotto il controllo dell'attaccante. Solitamente l'obiettivo dell'attacco è il cookie di sessione della vittima. La conoscenza di questo cookie permette infatti di sottoporre richieste all'applicazione utilizzando l'identità della vittima.

- ✓ SQL injection: gli attacchi basati su SQL injection possono avere diversi obiettivi: accesso ad informazioni riservate memorizzate sui database server che costituiscono il data layer dell'architettura applicativa attaccata; accesso non autorizzato all'applicazione, aggirando il meccanismo di autenticazione; esecuzione di comandi sui server del data layer.
  - Descrizione: si tratta di tecniche di manipolazione dei parametri in input utilizzati dall'applicazione per eseguire query SQL sul database. Lo scopo è sovvertire la logica della query in modo da ottenere:
    - messaggi di errore contenenti informazioni sulla struttura del database utilizzato;
    - informazioni differenti da quelle che la query dovrebbe estrarre;
    - recordset vuoti o tali da produrre un malfunzionamento dei meccanismi di autenticazione, allo scopo di accedere all'applicazione senza essere in possesso di credenziali valide;
    - esecuzione di comandi di sistema tramite stored procedure.
- ✓ Path Traversal: browsing di directory presenti sul web server ma non appartenenti alle applicazioni web pubblicate su di esso, per le quali non è previsto l'accesso da parte degli utenti.
  - Descrizione: un attacco di path traversal consiste nella sottomissione di richieste verso il web server per risorse il cui URL contiene path non appartenenti alle applicazioni web pubblicate su di esso. Poiché in generale tali path non sono noti all'attaccante, essi vengono specificati in forma relativa, partendo dalla posizione di risorse note ed utilizzando sintassi del tipo "../../" per navigare a ritroso il file system.
- ✓ OS Command Injection: esecuzione di comandi di sistema sulle macchine su cui insiste l'applicazione.

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

- Descrizione: questo attacco può essere effettuato quando la logica applicativa utilizza dati forniti in input dall'utente come parametri per l'esecuzione di comandi di sistema. Se la logica applicativa non esegue correttamente il parsing di tali dati, è possibile provocare l'esecuzione di comandi aggiuntivi e/o differenti da quelli previsti dagli sviluppatori.

- ✓ Cookie poisoning: gli obiettivi possono essere molteplici; essi dipendono dalla logica dell'applicazione attaccata. In generale, le tecniche di cookie poisoning mirano a provocare comportamenti non previsti nell'applicazione attaccata in modo da poter interagire con essa in modi non previsti dal programmatore.
  - Descrizione: le tecniche di cookie poisoning consistono nella modifica dei dati contenuti nei cookie inviati dall'applicazione all'utente, allo scopo di produrre errori e/o portare l'applicazione in stati non correttamente gestiti quando i cookie sono restituiti al server. Per essere in grado di apportare le modifiche opportune, l'attaccante deve conoscere la logica con cui i dati contenuti nei cookie sono processati dall'applicazione.
- ✓ Forceful browsing: accesso non autorizzato a pagine e/o funzionalità dell'applicazione.
  - Descrizione: gli attacchi di forceful browsing consistono semplicemente nella sottomissione di richieste HTTP per URL corrispondenti a pagine protette, senza seguire il percorso di navigazione previsto dal programmatore e, in particolare, aggirando le pagine di autenticazione.
- ✓ Information Leakage: ottenere informazioni sul sistema da attaccare.
  - Descrizione: vengono esaminati i sorgenti HTML delle pagine web ritornate dall'applicazione, allo scopo di individuare informazioni sensibili, come password cablate nel codice, commenti erroneamente lasciati dagli sviluppatori, informazioni su versioni del software utilizzato e configurazione.
- ✓ Parameter tampering
- ✓ Hidden field manipulation
- ✓ Stealth commanding
- ✓ Buffer overflow

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

Precisazioni

- Nel caso in cui il test avvenga su ambienti in produzione occorre utilizzare, dove possibile, un account di test creato appositamente per la scansione.
- Per tale account devono valere le seguenti condizioni:

  - Accesso esclusivamente riservato a record di test nei database di back-end.

  - Ordini di acquisto o altre tipologie di transazioni dovrebbero essere ignorati.

  - Eventuali nuovi record creati da tale account devono essere successivamente cancellati.

  - Qualora le transazioni abbiano un qualche tipo di impatto (per esempio in caso di acquisto/vendita di azioni), il loro effetto dovrebbe riguardare esclusivamente dei record di test.
- Qualora l'applicazione preveda diversi livelli di privilegio, è consigliabile effettuare un'analisi con un numero di credenziali di test pari al numero dei profili esistenti e previsti.
- E' consigliabile preventivare e tenere in considerazione il tempo necessario allo sviluppo di script/procedure di clean-up per ripulire tutti i dati creati/modificati dall'utente di test.
- E' utile identificare e comunicare eventuali script o parametri che invalidino le sessioni al fine di evitare che durante le scansioni tali script o parametri vengano eseguiti dai tool di test automatizzati.
- Unitamente alla documentazione dell'analisi verrà rilasciato l'elenco delle URL sottoposte a scansione.