AAA Bank

Assessment di sicurezza
del perimetro esterno e dei sistemi interni

Milano

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
1.0	04 Gennaio 2007	Prima emissione.
2.0	05 Gennaio 2007	Completamento della parte interna e definizione dei piani di breve termine e medio-lungo termine.
//	//	//

INFORMAZIONI		
Data di Emissione	05 Gennaio 2007	
Versione	2.0	
Tipologia Documento	Documento di Assessment	
Numero di Protocollo	//	
Numero Pagine	58	
Numero Allegati	3	
Descrizione Allegati	A	Approccio di assessment
	B	Metodologia di assessment
	C	Politiche di sicurezza
Redatto da	Julian Rrushi Gianluca Vadruccio	
Approvato da	Valeriano Bedeschi	

INDICE

INDICE DELLE FIGURE

INDICE DELLE TABELLE

1 Introduzione

1.1 Obiettivo

L'obiettivo dell'attività commissionata ad Hacking Team dal cliente AAA Bank è la valutazione dello stato di sicurezza dei propri sistemi perimetrali ed interni. La tipologia di attività richiesta comporta una forte collaborazione tra il personale delle due società al fine di individuare le vulnerabilità presenti e redigere insieme un piano di intervento di breve e medio periodo.

L'attività di analisi della sicurezza perimetrale è stata condotta in modalità black-box (blinded-attack) su tutto il boundary raggiungibile da internet; l'attività di analisi della sicurezza interna è stata invece portata a termine congiuntamente con il personale interno e con la conoscenza della rete e dei sistemi sotto esame.

A conclusione dei lavori verrà presentato il documento di assessment contenente la descrizione delle attività eseguite, dei controlli effettuati, della lista delle minacce esistenti e del piano di intervento consigliato.

Il filo conduttore dell'intera attività non è stato prettamente tecnologico; più che individuare asetticamente le vulnerabilità presenti, si è rivolta l'attenzione maggiore a quegli aspetti che più sono rischiosi per il cliente e che quindi rappresentano una reale minaccia di sicurezza. Tale modalità di procedere a portato quindi all'individuazione di scenari attraverso i quali un attaccante seriamente intenzionato può arrecare un danno reale al sistema/business del cliente.

1.2 Target

1.2.1 Target esterno

Parte esterna (TBD)

1.2.2 Target interno

L'assessment interno è stato condotto avendo conoscenza dello schema di rete. Sulla base di questo schema e delle considerazioni emerse dal personale dipendente di AAA Bank si è ritenuto opportuno focalizzare maggiormente l'attenzione sulle seguenti reti:

- Area CORE
  - 172.28.252.0/22
    - 172.28.253.0/24
    - 172.28.254.0/24

- Area DMZ
  - 10.28.254.0/24
  - 192.168.20.0/24
  - 192.168.40.0/24
  - 192.168.200.0/24
  - 192.168.204.0/24
  - 192.168.205.0/24
- Area WAN
  - 172.28.1.0/24
  - 10.28.252.0/24

Lo schema di massima di interconnessione delle reti indicate è mostrato nella seguente figura:

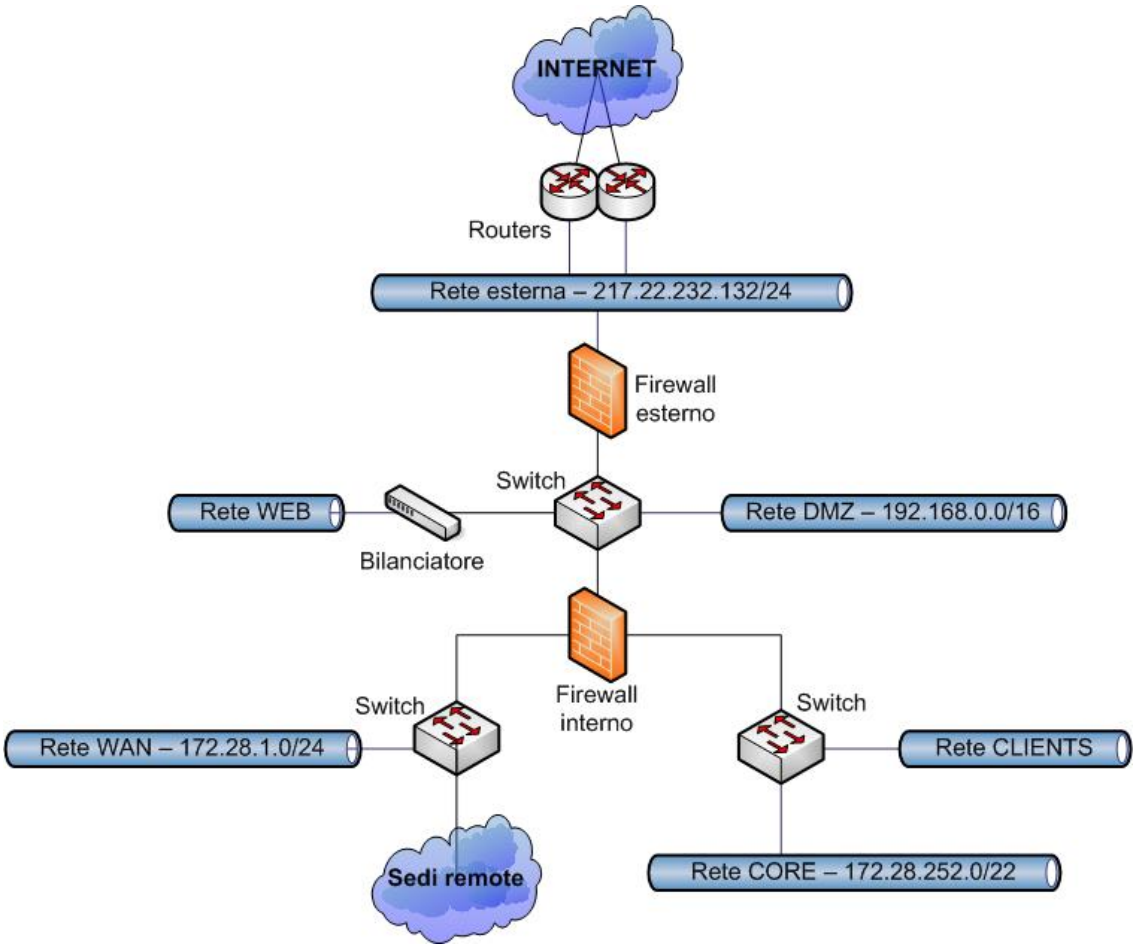


Figura 1 - Schema di massima delle interconnessioni di rete

A livello applicativo si sono analizzati secondo una criticità dettata dal personale interno di AAA Bank i seguenti server:

- 192.168.205.1
- 172.28.252.97
- 172.28.252.99
- 172.28.252.134
- 172.28.252.205
- 172.28.252.211
- 172.28.1.3
- 172.28.1.68

1.3 Ambiente di attacco

1.3.1 Ambiente esterno

Parte esterna (TBD)

1.3.2 Ambiente interno

Per il conseguimento dell'attività di ethical hacking dei sistemi di AAA Bank è stata utilizzata una conessione di rete interna appartenente all'area Core. Il posto fisico da dove sono effettuati i test di intrusione è comunemente usato per ospitare personale esterno in riunioni oppure attività lavorative di consulenza. I tentativi di intrusione ed i relativi tool di attacco sono stati eseguiti mediante dei computer portatili di proprietà Hacking Team con piattaforma Linux e/o Windows XP. Al fine di velocizzare il processo di valutazione della sicurezza dei sistemi di AAA Bank, al personale tecnico di Hacking Team è stato consegnato del materiale topologico relativo alla strutturazione della rete interna di AAA Bank. L'attività di ethical hacking è stata effettuata senza la conoscenza di credenziali di nessun tipo nè a livello applicativo nè a livello di sistema operativo.

1.4 Tools utilizzati

Durante l'attività di ethical hacking dei sistemi di AAA Bank è stato eseguito uno scanning automatico il quale è stato complementato da un'analisi manuale di tutte le vulnerabilità identificate. Gli strumenti di attacco utilizzati sono i seguenti:

- ***Scanner applicativi***: sono tool che eseguono in modo automatico la navigazione (crawling) delle pagine dell'applicazione target, riducendo il tempo necessario per ricostruire la struttura completa dell'applicazione web. Permettono inoltre di identificare, mediante confronto con un database di pattern di attacco noti, potenziali vulnerabilità. I scanner applicativi utilizzati in questo progetto sono stati *N-Stealth* e *Nikto*.

- ***System Vulnerability Scanner:*** Sono tool di scansione automatica di sistemi operativi e reti che hanno come obiettivo la rilevazione di vulnerabilità note. I tool in questione generalmente utilizzano dei plugin appositamente codificati. Durante questo progetto il tool utilizzato è stato *Nessus*.
- ***Forensic tools:*** Sono tools utilizzati per effettuare una valutazione della quantità di informazione utenibile mediante delle debolezze di configurazione come per esempio i NULL sessions. Il tool utilizzato in questo progetto è stato *hunt* di Foundstone.
- ***Network mapping tool:*** Sono tool che eseguono una scansione di singoli sistemi oppure intere reti al fine di determinare le porte aperte, le applicazioni che sono in ascolto in quelle porte, il tipo e la versione approssimata del sistema operativo, ecc. Durante questo progetto il tool utlizzato è stato *Nmap.*
- ***Tools di Forza Bruta:*** Sono tool che implementano attacchi di forza brutta oppure a dizionario contro l'autenticazione di diversi protocolli. In questo progetto il tool utilizzato è stato Hydra.
- ***Web proxy***: sono tool di intercettazione del traffico fra browser e server, che permettono di analizzare e modificare *header* e *body* di ogni singola richiesta/risposta HTTP. Gli web proxies utilizzati sono *Achilles* ed *Watchfire Web Proxy.*
- ***HTTP Editor***: Sono tool che permettono la costruzione ed invio a mano di richieste HTTP, e la visualizzazione delle relative risposte HTTP inviate dal web server. In questo progetto è stato utilizzato lo *Watchfire HTTP Editor*.
- ***Encoding/Decoding tool***: Sono tool utilizzati per codificare dei byte da una forma plain in rappresentazioni URL, base64, overlong UTF-8, ecc, e viceversa, decodificare dei byte da tali rappresentazioni in forma plain. Il tool utilizzato durante questo progetto è lo *Watchfire Encoder/Decoder.*
- ***Tool di analisi dei cookies***: Sono tool che servono per analizzare i vari cookies usati dalle applicazioni al fine di valutare la possibilità di implementazione di vari tipi di attacco aventi i cookies come soggetto. I tools utilizzati in questo progetto sono il *CookieDigger* di FoundStone e *Cookie Analyzer* di WatchFire.
- ***Site mapping tool***: Sono tool che effettuano il download di tutti i files da un sito al fine di costruire la sua struttura e permettere un'analisi offline. I tools utilizzati in questo progetto sono *BlackWidow* and *wget.*
- ***Database Scanning tool***: Sono tool che rivelano l'esistenza di database server direttamente raggiungibili in una rete, ed assistono nell'implementazione di attacchi diretti verso tali server.

1.5 Vincoli di progetto

L'unico vincolo presente sulle attività riguarda gli attacchi DoS (Denial of Service); sono stati omessi quindi tutti quei controlli e quele verifiche che avrebbero potuto generare dei disservizi. In un progetto successivo si consiglia comunque di rendere lo studio completo effettuando anche l'analisi dei DoS, possibili fonti di attacco con conseguente indisponibilità dei servizi e delle macchine.

1.6 Struttura del documento

Il documento presentato descrive l'attività commissionata ad Hacking Team, le tecniche utilizzate per lo studio, i risultati trovati e le contromisure consigliate suddivise in due piani: quello di breve termine e quello di medio-lungo termine.
Il contenuto importante del documento è inserito nei seguenti capitoli:

- Sintesi di alto livello dei risultati e degli impatti: capitolo 2
- Analisi e risultati relativi alla parte architetturale e logica: capitolo 3
- Analisi e risultati relativi allo studio di sicurezza esterno: capitolo 4
- Analisi e risultati relativi allo studio di sicurezza interno: capitolo 5
- Sintesi tecnica dei risultati e degli impatti: capitolo 6
- Strategia di fixing (piano di breve termine): capitolo 7
- Security plan (piano di medio-lungo termine): capitolo 8

1.7 Rappresentazione e classificazione delle vulnerabilità

Le vulnerabilità trovate verranno sintetizzate secondo una tabella le cui colonne sono di seguito descritte:

- #n: identificativo univoco della vulnerabilità
    - E-Axx: codice relativo alle **vulnerabilità architetturali esterne** (xx è un numero progressivo)
    - I-Axx: codice relativo alle **vulnerabilità architetturali interne** (xx è un numero progressivo)
    - E-RSxx: codice relativo alle **vulnerabilità reti e sistemi esterne** (xx è un numero progressivo)
    - I-RSxx: codice relativo alle **vulnerabilità reti e sistemi interne** (xx è un numero progressivo)
    - E-APPxx: codice relativo alle **vulnerabilità applicative esterne** (xx è un numero progressivo)

  - I-APPxx: codice relativo alle **vulnerabilità applicative interne** (xx è un numero progressivo)
- Livello: criticità della vulnerabilità
  - H: classificazione **alta**
  - M: classificazione **media**
  - L: classificazione **bassa**
- Nome: dicitura sintetica della debolezza
- Descrizione: spiegazione della debolezza
- Impatto: descrizione delle possibili minacce che la debolezza porta alla luce ed eventuali impatti sul sistema informativo aziendale
- Skill: livello di conoscenza o di esperienza che deve avere un attaccante per poter sfruttare con successo la vulnerabilità
  - H: conoscenza e/o esperienza **alta**
  - M: conoscenza e/o esperienza **media**
  - L: conoscenza e/o esperienza **bassa**

Le vulnerabilità riscontrate sono raffigurate secondo lo schema di classificazione illustrato di seguito (rosso: elevata criticità, arancione: media criticità, giallo: bassa criticità, verde: punto di lieve attenzione).

I due quadranti in alto rappresentano le vulnerabilità ritenute critiche: si consiglia di porre rimedio a breve termine per quelle di sinistra (di facile esecuzione); basta invece una pianificazione di copertura per quelle di destra (di difficile esecuzione).

V		LEVEL OF EFFORT TO EXECUTE	
		LOW	HIGH
DEGREE OF RISK/EASE OF EXPLOIT	HIGH	***Red flag: fix immediately***	***Red flag: plan to remediate***
	LOW	***Yellow flag: fix at customer's discretion***	***Green flag: bear risk***

2 Executive Summary

2.1 Parte esterna

(TBD)

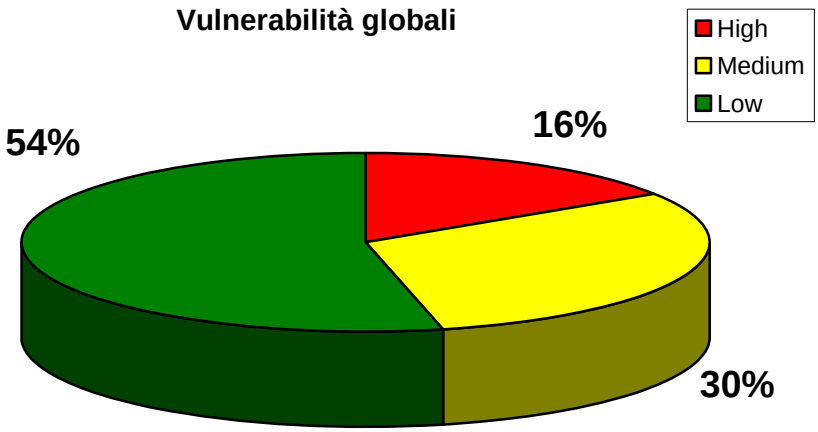


Figura 2 - Sintesi grafica delle vulnerabilità esterne

2.1.1 Classificazione delle minacce principali

V		LEVEL OF EFFORT TO EXECUTE	
		LOW	HIGH
DEGREE OF RISK/EASE OF EXPLOIT	HIGH	***Red flag: fix immediately***	***Red flag: plan to remediate***
	LOW	***Yellow flag: fix at customer's discretion***	***Green flag: bear risk***

Figura 3 - Classificazione delle minacce esterne

(TBD)

2.1.2 Analisi degli impatti

(TBD)

#n	Livello	Nome	Descrizione	Impatto

2.2 Parte interna

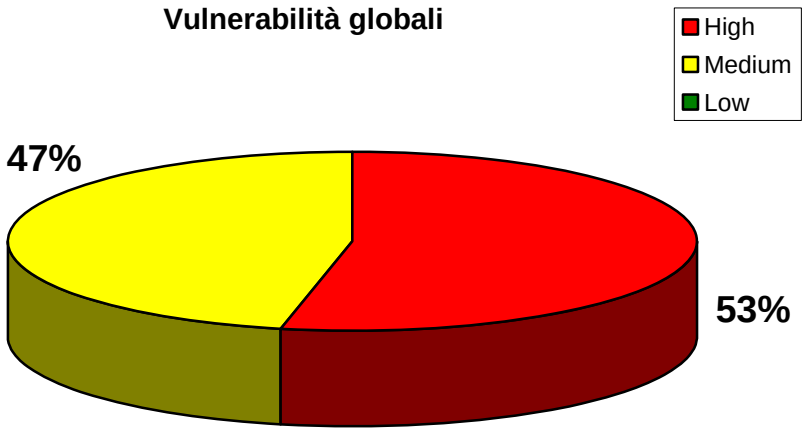


Figura 4 - Sintesi grafica delle vulnerabilità interne

2.2.1 Classificazione delle minacce principali

V		LEVEL OF EFFORT TO EXECUTE	
		LOW	HIGH
DEGREE OF RISK/EASE OF EXPLOIT	HIGH	***Red flag: fix immediately***	***Red flag: plan to remediate***
	LOW	***Yellow flag: fix at customer's discretion***	***Green flag: bear risk***

Figura 5 - Classificazione delle minacce interne

(TBD)

2.2.2 Analisi degli impatti

#n	Livello	Nome	Descrizione	Impatto
I-RS01	H	Mancanza di autenticazione nel server di base di dati MySQL	Il server della base di dati in questione non richiede una passord per alcune utenze tra le quali *root* e *anonymous*	Chiunque abbia la possibilita' di connettersi al server di base di dati MySQL potrebbe accedere in esso ed eseguire delle query SQL
I-RS02	H	Mancanza di autenticazione in Oracle tnslsnr	Il programma tnslsnr che rappresenta l'interfaccia tra i client ed il server della base di dati Oracle non e' protetto da una password	Chiunque abbia la possibilita' di connettersi al programma tnslsnr potrebbe spegnere il server della base di dati Oracle e negare il servizio ad altri utenti leggittimi
I-RS03	M	Command injection in Oracle	Il server della base di dati Oracle e' vulnerabile ad una estensione maligna delle query SQL esguite su di esso	Tale vulnerabilita' permette un utente non privilegiato della base di dati Oracle di eseguire delle query SQL delle quali esso non e' autorizzato
I-RS04	M	Buffer overflow in Oracle	Il server di base di dati Oracle contiene del codice vulnerabile al buffer overflow	Un'utente non privilegiato potrebbe ottenere pieno controllo della base di dati in questione oppure eseguire del codice arbitrario sul sistema operativo dove il server di base di dati Oracle e' in esecuzione
I-RS05	H	Malconfigurazione in tnslsnr	Il programma tnslsnr che rappresenta l'interfaccia tra i client ed il server della base di dati Oracle e' vulnerabile	Un attaccante potrebbe scrivere su tutti i file per i quali il programma tnslsnr possiede privilegi in scrittura
I-RS06	H	Buffer Overflow in BrightStor ARCServe DBA server	BrightStor ARCServe DBA server contiene del codice vulnerabile al buffer overflow	Un attaccante potrebbe eseguire del codice arbitrario sul sistema operativo dove il BrightStor ARCServe DBA server e ' in esecuzione
I-RS07	H	Utenza di default nel server di base di dati SQL	La base di dati Microsoft SQL e' accessibile mediante l'utilizzo dell'utenza *admin* e la password *admin*	Un attaccante potrebbe accedere nella base di dati in questione ed eseguire delle query SQL arbitrarie
I-RS08	H	Vulnerabilita' multiple nel server web Apache	Il server web Apache contiene del codice vulnerabile ad errori di programmazione	Un attaccante potrebbe eseguire del codice arbitrario sul sistema operativo in cui Apache e' in esecuzione oppure rendere il processo non disponibile
I-RS09	M	Sessioni NULL e Guest	Il sistema permette il logon mediante una sessione nulla	Un attccante potrebbe effettuare un logon sul sistema vulnerabile oppure enumerare utenti locali e di dominio, servizi in esecuzione, cartelle condivise, ecc
I-RS10	H	Buffer overflow in Computer Associate Licence	Il programma che fornisce un modo per prodotti software di autorita' di	Un attaccante potrebbe eseguire del codice arbitrario sul sistema dove tale programma e' in

		Application	certificazione di registrare le proprie licenze software via rete, e' vulnerabile ad errori di programmazione	esecuzione
I-APP01	H	Debole autenticazione in HP JetDirect Printer	La password di amministrazione della stampante HP JetDirect e' recuperabile da remoto. L'applicativo web per la gestione della stampante in questione non e' protetto da nessun sistema di autenticazione	Un attaccante potrebbe recuperare la password di amministrazione e/o ottenere pieno controllo sulla configurazione della stampante in questione
I-APP02	H	Mancanza di autenticazione in phpadmin	La procedura web che serve per l'amministrazione del server di base di dati MySQL non e' protetta da password	Un attaccante potrebbe eseguire delle query arbitrarie sulla base di dati MySQL
I-RS11	M	File sensitivi in server FTP	In un server ftp sono stati trovati file contenenti dei dati di configurazione	Un attaccante potrebbe risalire ad una configurazione approssimata di proxies e firewalls.
I-RS12	H	Buffer overflow in Server Message Block	SMB che e' un protocollo di condivizione di files, stampanti, porte seriali, ecc., e' vulnerabile ad errori di programmazione	Un attaccante potrebbe eseguire del codice arbitrario sul sistema dove SMB e' in esecuzione
I-RS13	H	Buffer overflow in Sendmail	Sendmail che e' un agente di spedizione di e-mails e' vulnerabile ad errori di programmazione	Un attaccante potrebbe eseguire del codice arbitrario sul sistema dove Sendmail e' in esecuzione
I-RS14	H	Buffer overflow in Samba	Samba che e' un programma il quale offre dei servizi di file e di stampa e' vulnerabile ad errori di programmazione	Un attaccante potrebbe eseguire del codice arbitrario sul sistema dove Samba e' in esecuzione
I-RS15	H	Buffer overflow in BIND	Il risolutore di nomi ed indirizzi di rete e' vulnerabile ad errori di programmazione	Un attaccante potrebbe eseguire del codice arbitrario sul sistema dove Bind e' in esecuzione
I-RS16	H	Buffer overflow nel servizio Server	Il servizio Server e' vulnerabile ad errori di programmazione	Un attaccante potrebbe eseguire del codice arbitrario sul sistema dove Server e' in esecuzione

Tabella 1 - Analisi degli impatti relativi alle vulnerabilità interne

2.3 Parte interna logico-architetturale

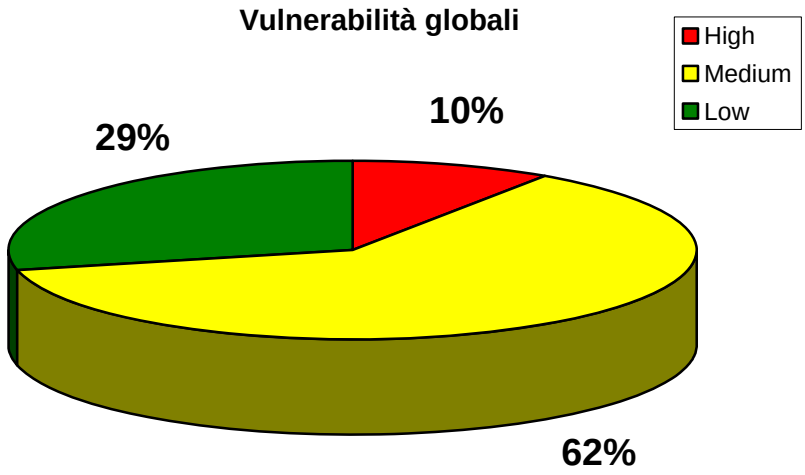


Figura 6 - Sintesi grafica delle vulnerabilità logico-architetturali interne

2.3.1 Classificazione delle minacce principali

V		LEVEL OF EFFORT TO EXECUTE	
		LOW	HIGH
DEGREE OF RISK/EASE OF EXPLOIT	HIGH	***Red flag: fix immediately***	***Red flag: plan to remediate***
	LOW	***Yellow flag: fix at customer's discretion***	***Green flag: bear risk***

Figura 7 - Classificazione delle minacce logico-architetturali interne

(TBD)

2.3.2 Analisi degli impatti

#n	Livello	Nome	Descrizione	Impatto

(TBD)

3 Analisi topologica ed architetturale

3.1 Studio rete esterna

(TBD)

3.2 Studio rete interna

3.2.1 La rete e i dispositivi

La rete interna è suddivisa da due firewall (uno interno ed uno esterno non in cluster) e le subnet interne sono segmentate logicamente in VLAN attraverso degli apparati di layer 2 con funzionalità di routing di livello 3. La rete è parzialmente replicata in un sito di disaster recovery con funzionalità di bilanciamento per alcuni servizi e di alta affidabilità per altri.
Non è presente alcun access point ed alcuna rete wireless.
I principali punti nevralgici della rete sono controllati da uno sniffer (Ethereal) con funzionalità di debugging del traffico. Sono state dismesse le sonde IDS network-based. Non sono presenti sui server nessun tipo di sonde IDS host-based nè alcun tipo di controllo dell'integrità del file system.
La rete presenta due livelli di firewall: entrambi installati su piattaforma SUN, con sistema operativo Solaris 8 e con CheckPoint NG-AI. I due nodi firewall sono due cluster hot stand-by realizzati da Stonebit FullCluster con schede di rete configurate in antispoofing (ad eccezione di casi isolati specifici vincolati al funzionamento applicativo).

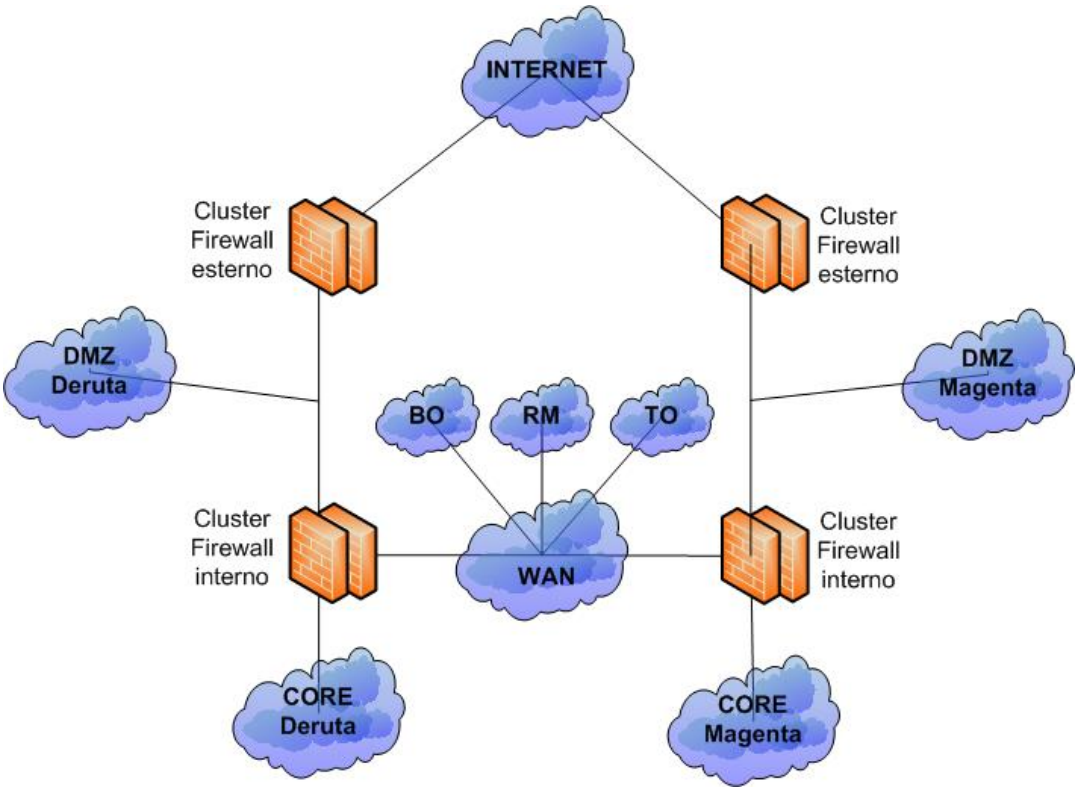


Figura 8 - Il sistema di firewalling

La management risiede in DMZ e gestisce entrambi i cluster. La rule base definita prevede 87 regole con assegnazione ad entrambi i cluster o al singolo cluster a seconda della regola stessa di pertinenza. Il sistema di regole è stato impostato seguendo 3 regole principali:

1. posizionare tra le prime posizioni le regole soggette a maggiore traffico
2. stealth rule in fondo
3. posizionare alcune regole di drop in punti opportuni

È in corso un'attività di pulizia delle regole.

3.2.2 L'utenza e i profili

Gli utenti, gli amministratori e gli eventuali consulenti sono attestati su switch di piano che confluiscono in una VLAN dedicata. A nessun portatile esterno è consentito l'accesso alla rete attraverso la configurazione port secure degli switches basata su mac address. Le altre porte degli switch libere sono in stato disabled. L'indirizzo IP è assegnato dal DHCP server attraverso un abbinamento statico IP-mac address.

Le postazioni degli utenti sono realizzate mediante un'immagine ghost già hardenizzata; i privilegi sono quelli di domain users Active Directory 2000. Solo gli amministratori godono dei privilegi di

administrator locale e di dominio. È impostata una politica active directory restrittiva sull'utilizzo delle postazioni client.

Su tutte le postazioni è installato un sistema antivirus e antispyware TrendMicro (sia client che server) e la posta è controllata a livello di content filtering da SurfControl. Lo stesso livello di sicurezza non è impostato per la navigazione (tramite proxy Squid) e per la mail via web.

L'accesso in VPN è consentito a dipendenti e a persone esterne attraverso secure client con username e password come sistema di autenticazione.

I portatili non possono collegarsi alla rete interna aziendale e non hanno un sistema di cifratura dei dati sensibili e confidenziali.

A livello fisico, i dipendenti accedono all'edificio mediante un badge RFID e a banda magnetica; le timbrature vengono inviate ad un server dell'ufficio paghe e stipendi. L'accesso alle sale CED è limitato solo ai badge opportunamente configurati[1].

3.2.3 La gestione

Il sistema di update del parco macchine (sia client che server) è realizzato mediante i seguenti macro steps:

- installazione di eventuali patch o configurazioni di sicurezza su un numero ristretto e controllabile di macchine (comunque in produzione)
- verifica dello stato delle macchine e della reazione alle variazioni
- deployment sulle restanti macchine

L'abilitazione di personale dipendente neo-assunto segue l'iter seguente:

- l'ufficio risorse umane comunica all'IT i dati del nuovo dipendente e l'ufficio in cui verrà impiegato
- l'IT genera il suo profilo Active Directory sotto al gruppo relativo all'ufficio di destinazione (ereditandone i diritti)
- l'IT chiede all'ufficio di destinazione della nuova persona che diritti dovrà avere in più di quelli standard del gruppo Active Directory
- l'IT eseguirà le abilitazioni in base a quanto indicato dal responsabile del neo-assunto

Non viene mantenuta una traccia delle abilitazioni, neanche durante cambiamenti di incarico o di ufficio. La fase di de-provisioning consiste nell'eliminazione da Active Directory ma non dalle abilitazioni ad hoc. Non è presente un meccanismo di controllo delle credenziali non più utilizzate e la pulizia degli accounts viene fatta saltuariamente e a mano.

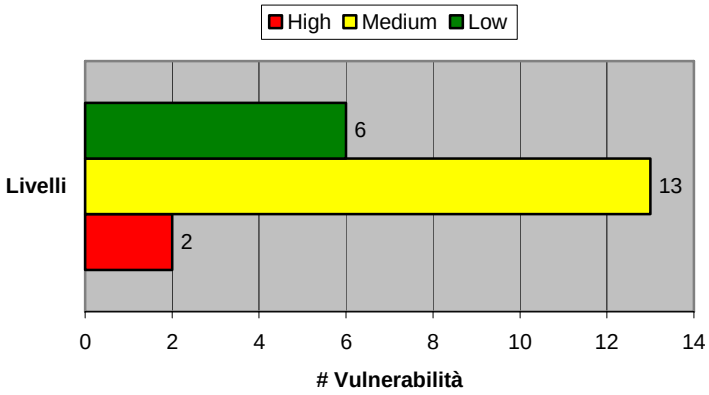
[1] Non è di pertinenza della presente attività lo studio relativo alla modifica, sostituzione, clonazione, falsificazione ed utilizzo del badge aziendale. Rientra in un'attività più completa erogabile da Hacking Team e denominata social engineering.

Il monitoraggio della rete, dei sistemi e dei servizi avviene su protocollo SNMP e riguarda fault di tipo hardware o di tipo sistema operativo. Vengono inoltre monitorati con un sistema free linux-based tutti i dispositivi di rete (routers e switches).
La centralizzazione dei log avviene per la parte firewalling e proxying verso un database SQL sul quale avvengono i controlli mauali e saltuari. Non è prevista alcuna regola di correlazione.
L'allarmistica è affidata a qualche regola impostata sui sistemi oggetti di monitoraggio che spedisce un alert via mail a fronte di fault o malfunzionamenti.

3.2.4 Politiche e procedure

Le politiche non sono mai state consegnate ufficialmente e non vengono quindi divulgate. Quanto in esse stabilito è stato implementato nelle seguenti procedure: alimentazione archivio informatico, gestione degli acquisti IT, gestione dei backup, gestione dei log, gestione dei profili utente, gestione delle password, help desk, incident response, inventario IT, nuove implementazioni. Anche le procedure sopra menzionate non sono adeguatamente divulgate e manutenute.
Il DPS è esistente.

3.3 Vulnerabilità architetturali



#n	Livello	Nome	Descrizione
I-A01	M	Separazione utenza	Utenti, amministratori e consulenti appartengono alla stessa vlan ed allo stesso switch di piano.
I-A02	M	Integrità dei server critici	È consigliabile avere un sistema di controllo dei cambiamenti/sostituzioni di files e modifica dei privilegi almeno sui server critici.
I-A03	L	IDS	Opportunamente configurate e "tunate", le sonde IDS network-based sono utili per rilevare attacchi e comportamenti non aderenti alle policy aziendali. I devices in-line consentono inoltre di bloccare proattivamente azioni pericolose senza generare falsi positivi.

I-A04	L	Accesso alla rete	L'accesso ad una presa di rete è controllato da port secure sulla base del mac address che è facilmente modificabile.
I-A05	L	BIOS Setup password	Non è consentito l'utilizzo di porte USB nè di bootare da CD ma senza password di protezione del setup del BIOS.
I-A06	M	Hardening delle postazioni e dei server	È consigliabile controllare lo stato di blindatura delle postazioni client (e quindi ricostituire una nuova immagine ghost) e, singolarmente, dei server critici. Unitamente a questo, è importante controllare anche le politiche active directory di restrizione delle attività sui client.
I-A07	L	Posta via web	Essendo consentito il traffico mail via web ai propri dipendenti, sarebbe utile avere un meccanismo di controllo che analizzi il contenuto della posta. Questo costituirebbe una seconda linea di difesa rispetto al giuà presente sistema client di antivirus e antispyware.
I-A08	M	Navigazione sicura	La navigazione è consentita e realizzata attraverso un proxy Squid senza content filtering e con un url filtering manuale basato su black-list.
I-A09	M	Strong Authentication	L'accesso da remoto è ben protetto ma viene autenticato mediante la coppia username-password.
I-A10	M	Cifratura dati sui portatili	Informazioni critiche e dati sensibili potrebbero essere presi da malintenzionati considerando il fatto che non è previsto un sistema di cifratura degli stessi.
I-A11	L	Verifica patch e variazioni	Le prove delle patch o delle variazioni di configurazione vengono testate su macchine in produzione (sia per la parte client che per la parte server).
I-A12	M	Deployment patch e variazioni	La procedura di aggiornamento prevede di eseguire il deployment sul parco macchine restante una volta verificato con successo l'esito su un numero ristretto. Questo può andare bene per la parte client ma non per la parte server, data l'eterogeneità del software installatovi.
I-A13	L	Tracciabilità del provisioning	La globalità delle abilitazioni effettuate verso gli utenti non è conservata.
I-A14	M	De-Provisioning	Non vi è una garanzia che gli account non più utilizzati vengano rimossi. Non essendoci un sistema di controllo in tal senso, la pulizia viene affidata ad operazioni non proceduralizzate e manuali.
I-A15	M	Monitoraggio	Non esistono controlli real-time sugli eventi legati alla sicurezza informatica.
I-A16	M	Centralizzazione log	È un'attività che avviene solamente per la parte di firewall e proxy. Sono controllati manualmente e saltuariamente.
I-A17	H	Security Operation Center	Non ci si accorge dell'accadimento di eventi legati alla sicurezza, non si correlano gli eventi a livello business, non si centralizzano/mantengono i log di sicurezza, non è definito un sistema di allarmistica e quindi neanche una gestione degli incidenti (incident handling).

I-A18	H	Politiche di sicurezza	Le politiche di sicurezza non sono complete e non sono state rese ufficiali nè adeguatamente divulgate. Tra le politiche più utilizzate (vedere Allegato C – Politiche di sicurezza) ne mancano molte importanti come ad esempio acceso remoto, analisi dei rischi, business continuity, trattamento dei dati sensibili, gestione degli incidenti, monitoraggio, utilizzo degli strumenti aziendali, formazione, sensibilizzazione.
I-A19	M	Procedure di sicurezza	Le procedure di sicurezza non sono complete e non sono scritte in maniera tale da garantire continuità in caso di turn-over.
I-A20	M	Posizionamento management del firewall	Il server di gestione di entrambi i cluster firewall è posizionato in DMZ.
I-A21	M	Ottimizzazione regole firewall	Il sistema di regole dei firewall deve essere rivisto, pulito ed ottimizzato.

Tabella 2 - Vulnerabilità della parte architetturale interna

4 Studio esterno

(TBD)

4.1 Elenco delle vulnerabilità

Viene presentato di seguito l'elenco delle vulnerabilità riscontrate comprensivo della loro descrizione. Successivamente ogni rete verificata avrà:

- un riassunto grafico delle proprie vulnerabilità
- un elenco di IP soggetti ad ognuna delle vulnerabilità

4.1.1 Vulnerabilità 1

Descrizione

4.1.2 Vulnerabilità 2

Descrizione

4.1.3 Vulnerabilità 3

Descrizione

4.2 Rete 1

4.2.1 Sintesi della criticità

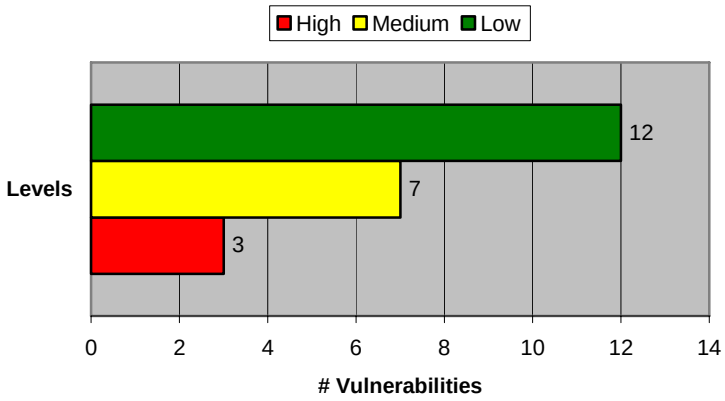


Figura 9 - Criticità della rete 1

4.2.2 Vulnerabilità riscontrate

#n	Livello	Nome	Descrizione

4.3 Rete 2

4.3.1 Sintesi della criticità

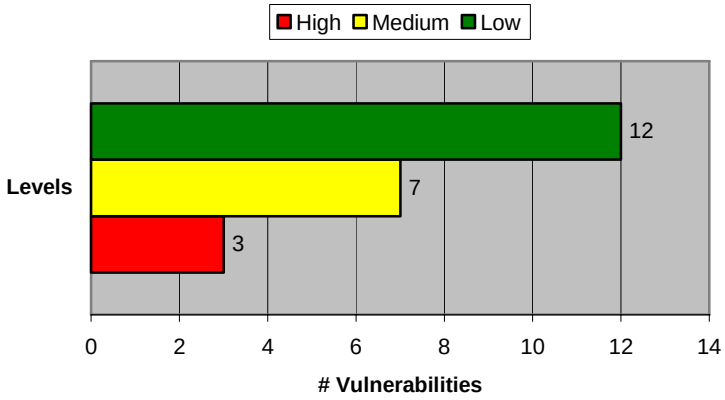


Figura 10 - Criticità della rete 2

4.3.2 Vulnerabilità riscontrate

#n	Livello	Nome	Descrizione

5 Studio interno

5.1 Elenco delle vulnerabilità

Viene presentato di seguito l'elenco delle vulnerabilità riscontrate comprensivo della loro descrizione. Successivamente ogni rete verificata avrà:

- un riassunto grafico delle proprie vulnerabilità
- un elenco di IP soggetti ad ognuna delle vulnerabilità

5.1.1 I-RS01 Mancanza di Autenticazione in MySQL Server

In alcuni servers di basi di dati MySQL sono state trovate abilitate delle utenze come per esempio *root* e *anonymous* per le quali i DB servers in questione non effettuano nessuna autenticazione.

5.1.2 I-RS02 Mancanza di Autenticazione in Oracle tnslsnr

Al programma listener di Oracle Enterprize Server (*tnslsnr*) non è stato assegnato una password mediante il commando SET PASSWORD. Di conseguenza un attaccante potrebbe spegnere il server in questione negando il servizio ad altri utenti legittimi.

5.1.3 I-RS03 Command Injection in Oracle

La base di dati Oracle appare vulnerabile ad un tentativo di command injection. Tale vulnerabilità è esploitabile da un attaccante il quale possiede un account sulla base di dati obiettivo, e potrebbe permetterlo di eseguire dei commandi arbitrari sul sistema.

5.1.4 I-RS04 Buffer Overflow in Oracle

La base di dati Oracle appare vulnerabile ad un buffer overflow nella query CREATE DATABASE LINK. Un attaccante in possesso di un'utenza non privilegiata nella base di dati obiettivo potrebbe esploitarla al fine di ottenere pieno controllo sulla base di dati in questione e/o ottere una shell sul sistema operativo che ospita la base di dati in questione.

5.1.5 I-RS05 Malconfigurazione in Oracle tnslsnr

Il programma *tnslsnr* permette ad un attaccante di scrivere del contenuto arbitrario ovunque esso, cioè *tnslsnr*, abbia permessi in scrittura.

5.1.6 I-RS06 Buffer Overflow in BrightStor ARCServe DBA server

Il BrightStor ARCServe DBA server è vulnerabile ad diversi buffer overflows. Un attaccante potrebbe esploitare da remoto ciascuna di queste vulnerabilità e come conseguenza eseguire del codice arbitrario sul sistema operativo che ospita il server di basi di dati in questione.

5.1.7 I-RS07 Default Account in Microsoft SQL Server

In alcuni server di basi di dati Microsoft SQL l'utente di default *admin* è abilitato. In più, a tale utente corrisponde la password di default *admin*. Un attaccante potrebbe utilizzare tale utenza per accedere alla base di dati in questione, quindi leggere e/o scrivere dei dati.

5.1.8 I-RS08 Vulnerabilità Multiple in Apache Web Server

Alcuni server web Apache sono vulnerabili ad un buffer overflow residente nella parte di codice che è responsabile della elaborazione di una URL inviata via Ipv6. Un buffer overflow ed un format string sono presenti in Apache mod_ssl module. In più questi server sono vulnerabili ad una condizione di denial of service creabile da un attaccante eseguente dei commandi DAV LOCK.

5.1.9 I-RS09 Sessioni NULL e Guest

È stato possibile recuperare il Security Identifier (SID) emulando una chiamata alla funzione *LsaQueryInformationPolicy()* mediante una sessione NULL. In diversi sistemi è stato possibile effettuare un logon mediante il commando Net Use utilizzando una sessione NULL oppure identificandosi come utente Guest. In più, le sessioni NULL e emulazioni di chiamate alla funzione *LsaQueryInformationPolicy()* permettono di individuare gli utenti di dominio, gli utenti locali, vari servizi in esecuzione, cartelle condivise, ecc.

5.1.10 I-RS10 Buffer Overflow in Computer Associate License Application

L'applicazione di Computer Associate Licence nella sua versione appare vulnerabile a vari buffer overflows che potrebbero permetter un attaccante di eseguire del codice arbitrario sul sistema operativo obiettivo come utente SYSTEM.

5.1.11 I-APP01 Debole Autenticazione in HP JetDirect Printer

La password di amministrazione di HP JetDirect printer (*CLOPNUDI=108*) è recuperabile inviando delle definite richieste SNMP. L'applicativo web per la gestione di JetDirect è utlizzabile senza nessuna autenticazione dando la possibilità ad un attaccante di modificare la configurazione della stampante ed effettuare ulteriori abusi. In più, il server ftp nei sistemi che permettono di gestire JetDirect è apperto a tutti.

5.1.12 I-APP02 Mancanza di Autenticazione in phpadmin

La procedura *phpadmin* la quale permette di operare via HTTP su una base di dati MySQL è risultata utilizzabile senza autenticazione. Questa vulnerabilità potrebbe permettere ad un attaccante di eseguire delle SQL query arbitrarie sulle tabelle della base di dati in questione.

5.1.13 I-RS11 File Sensibili in ftp Server

Diversi file caricati su un ftp server che permete accesso anonimo sono risultati di natura sensitiva. Sono stati recuperati diversi file il cui contenuto sembra essere la configurazione di squid proxy, firewall, ecc. Un attaccante potrebbe facilmente recuperare tali files ed utilizzare le informazioni in essi contenute.

5.1.14 I-RS12 Buffer Overflow in SMB

L'implementazione del Server Message Block è vulnerabile ad un buffer overflow. Un attaccante esploitandolo potrebbe eseguire del codice arbitrario sul sistema operativo che ospita il server in questione.

5.1.15 I-RS13 Buffer Overflow in sendmail

I server sendmail sono vulnerabili a diversi buffer overflows la cui esploitazione potrebbe permetter e un attaccante di eseguire come root del codice arbitrario sul sistema operativo che ospita i server in questione.

5.1.16 I-RS14 Integer Overflow e Buffer Overflow in Samba Server

Un attccante potrebbe causare un integer overflow in SAMBA server inviando al obiettivo un pacchetto malformato contenente moltissime access control lists (ACLs). L'integer overflow in questione causa a sua volta un buffer overflow che potrebbe permettere un attaccante di eseguire del codice arbitrario sul sistema obiettivo. L'attaccante ad ogni caso avrebbe bisogno di una utenza per poter esploitare gli overflow in questione.

5.1.17 I-RS15 Buffer Overflow in BIND DNS Server

Le funzioni risolutrici facenti parte delle librerie DNS resolver e responsabili del look up di nomi ed indirizzi di rete sono vulnerabili a vari buffer overflows che potrebbero permettere un attaccante di eseguire codice arbitrario su una macchina obiettivo.

5.1.18 I-RS16 Buffer Overflow in Server service

Il servizio Server è vulnerabile ad uno stack based buffer. La vulnerabilità viene esploitata mediante l'invio al servizio Server di un messaggio maligno di remote procedure call.

5.2 Rete CORE

5.2.1 Sintesi della criticità

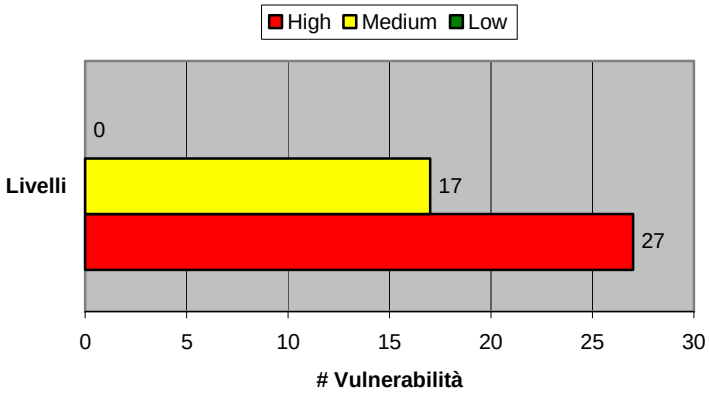


Figura 11 - Criticità della rete CORE

5.2.2 Vulnerabilità riscontrate

#n	Livello	Nome	Indirizzi IP	Descrizione
I-RS01	H	Autenticazione mancante	172.28.252.97	MySQL server non effettua l'autenticazione su alcuni utenti come root e anonymous
I-RS02	H	Autenticazione mancante	172.28.252.97 172.28.252.110 172.28.252.111 172.28.252.145 172.28.252.146 172.28.252.237	Il programma tnslsnr non è protetto da una password
I-RS03	M	Command injection in Oracle	172.28.252.97 172.28.252.110 172.28.252.111 172.28.252.145 172.28.252.146 172.28.252.237	È possibile effettuare injection di commandi arbitrari in query SQL
I-RS04	M	Buffer overflow	172.28.252.97	Oracle è vulnerabile ad un buffer overflow nella CREATE DATABASE query
I-RS05	H	Malconfigurazione di tnslsnr	172.28.252.97	È possibile scrivere dei files mediante tnslsnr
I-RS06	H	Buffer overflow	172.28.252.134 172.28.252.135 172.28.252.187	BrightStor ARCServe DBA server è vulnerabile ai buffer overflows
I-RS07	H	Utenza di default abilitata	172.28.252.135	È possibile accedere a Microsoft SQL Server utilizzando l'utenza admin/admin

I-RS08	H	Buffer overflow	172.28.252.146	Apache web server risulta vulnerabile ai buffer overflows
I-RS09	M	Null sessions	172.28.252.1 172.28.252.97 172.28.252.134 172.28.252.135 172.28.252.187 172.28.253.27 172.28.253.152 172.28.254.49 172.28.254.51	Diversi sistemi permettono NULL sessions utilizzabili da un attaccante per prelevare dai sistemi obiettivo i security identifiers,a loro volta utilizzabili per enumerare utenti, cartelle e servizi
I-RS10	H	Buffer overflow	172.28.252.187	L'applicazione di Computer Associate Licence risulta vulnerabile ai buffer overflows
I-APP01	H	Autenticazione debole	172.28.253.57 172.28.253.58 172.28.253.118 172.28.253.119 172.28.253.120 172.28.253.121 172.28.253.180 172.28.253.185 172.28.253.186	La password di amministrazione di HP JetDirect printer non è abilitata oppure è facilmente prelevabile. L'utilizzo dell'applicativo web per la gestione di HP JetDirect Printer ed il relativo ftp server non richiedono nessuna autenticazione
I-APP02	H	Mancanza di autenticazione	172.28.252.97	La procedura phpadmin utilizzata per l'amminstrazione su HTTP di MySQL non è protetta da un sistema di autenticazione
I-RS11	M	Abuso di ftp upload	172.28.253.1	Diversi file caricati da utenti leggittimi su un ftp server risultano contenere informazioni sensitive accessibili da chiunque si possa connettere ad esso
I-RS12	H	Buffer overflow	172.28.253.152	L'implementazione del Server Message Block è vulnerabile ad un buffer overflow
I-RS16	H	Buffer overflow	172.28.253.152 172.28.254.50	Il servizio Server è vulnerabile ad un buffer overflow

Tabella 3 - Vulnerabilità della rete CORE

5.3 Rete DMZ

5.3.1 Sintesi della criticità

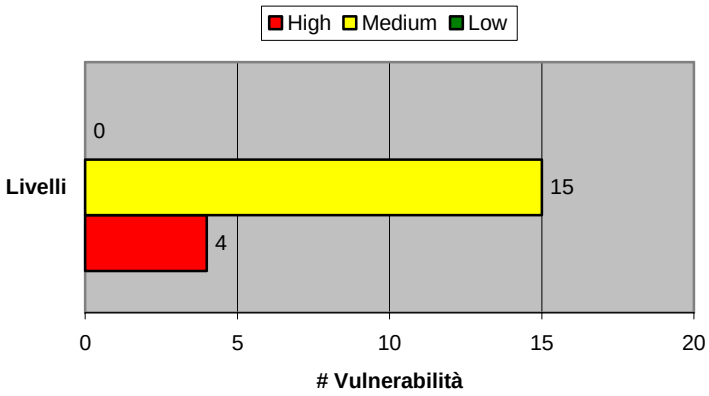


Figura 12 - Criticità della rete DMZ

5.3.2 Vulnerabilità riscontrate

#n	Livello	Nome	Indirizzi IP	Descrizione
I-RS09	M	Null sessions	192.168.200.128 192.168.200.129 192.168.200.208 192.168.200.209 192.168.205.17 192.168.205.18 192.168.205.25 192.168.205.26 192.168.200.128 192.168.200.129 192.168.200.208 192.168.200.209 192.168.205.17 192.168.205.25 192.168.205.26	Diversi sistemi permettono NULL sessions utilizzabili da un attaccante per prelevare dai sistemi obiettivo i security identifiers,a loro volta utilizzabili per enumerare utenti, cartelle e servizi
I-RS13	H	Buffer overflow	192.168.20.22	Sendmail è vulnerabile ad un buffer overflow
I-RS14	H	Buffer overflow	192.168.40.1 192.168.40.17	Samba server è vulnerabile ad un integer overflow che a sua volta causa un buffer overflow
I-RS15	H	Buffer overflow	192.168.40.1	L'implementazione di BIND è vulnerabile ai buffer overflows

Tabella 4 - Vulnerabilità della rete DMZ

5.4 Rete WAN

5.4.1 Sintesi della criticità

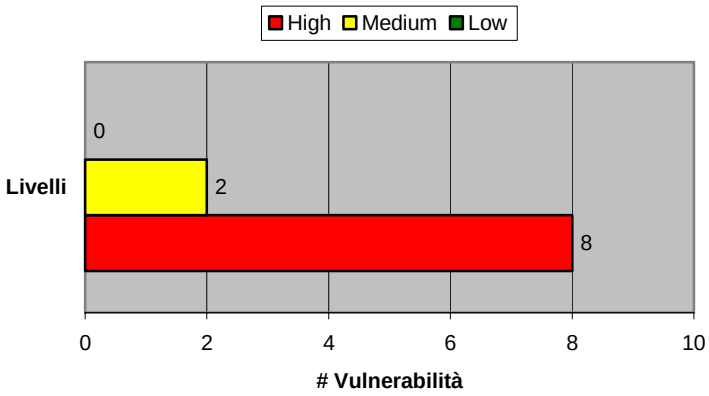


Figura 13 - Criticità della rete WAN

5.4.2 Vulnerabilità riscontrate

#n	Livello	Nome	Indirizzi IP	Descrizione
I-RS08	H	Buffer overflow	172.28.1.66 172.28.1.67 172.28.1.70 172.28.1.71 172.28.1.66 172.28.1.67 172.28.1.70 172.28.1.71	Apache web server risulta vulnerabile ai buffer overflows oppure format strings
I-RS09	M	Null sessions	172.28.1.33 172.28.1.35	Diversi sistemi permettono NULL sessions utilizzabili da un attaccante per prelevare dai sistemi obiettivo i security identifiers,a loro volta utilizzabili per enumerare utenti, cartelle e servizi

Tabella 5 - Vulnerabilità della rete WAN

6 Sintesi dei risultati

6.1 Sintesi delle vulnerabilità della parte esterna

#n	Livello	Nome	Impatto	Skill

6.2 Sintesi delle vulnerabilità della parte interna

#n	Livello	Nome	Impatto	Skill
I-RS01	H	Autenticazione mancante in MySQL	Permette l'accesso alla base di dati. Nel caso un attaccante accede come utente root potrebbe eseguire sulla base di dati compromessa tutte le operazioni possibili.	L
I-RS02	H	Autenticazione mancante in Oracle tnslsnr	Un attaccante potrebbe spegnere il server di base di dati Oracle e causare quindi un disservizio.	L
I-RS03	M	Command injection in Oracle	Un attaccante che possiede un'utenza limitata sulla base di dati Oracle potrebbe eseguire commandi arbitrari su di esso	M
I-RS04	M	Buffer overflow in Oracle	Un attaccante il quale possiede un'utenza sulla base di dati Oracle potrebbe eseguire commandi arbitrari su di essa oppure ottenere il commando totale del sistema operativo	M/H
I-RS05	H	Malconfigurazione di tnslsnr	Un attaccante potrebbe scrivere in tutti i files o directories dove il programma tnslsnr possiede i privilegi di scrittura.	M/H
I-RS06	H	Buffer overflow BrightStor ARCServe DBA server	Un attaccante potrebbe eseguire del codice arbitrario sul sistema operativo che ospita un BrightStor ARCServe DBA server vulnerabile.	M/H
I-RS07	H	Utenza di default abilitata in Microsoft SQL Server	Un attaccante potrebbe ottenere un accesso privilegiato nella base di dati Microsoft SQL Server.	L
I-RS08	H	Buffer overflow in Apache	Un attaccante potrebbe eseguire del codice arbitrario sul sistema operativo che ospita un server web apache vulnerabile oppure rendere quest'ultimo indisponibile.	M/H
I-RS09	L/M	Null sessions	Un attaccante potrebbe prelevare il security identifier del sistema ed utilizzarlo per enumerare utenti locali e di dominio, servizi in esecuzione, e cartelle condivise. In più un attaccante potrebbe effettuar un logon mediante il comando net use.	L
I-RS10	H	Buffer overflow in Computer	Un attaccante potrebbe esguire codice arbitrario sul sistema operativo che ospita un	M/H

		Associate License Application	Computer Associate License Application vulnerabile.	
I-APP01	H	Autenticazione debole in HP JetDirect Printer	Un attaccante potrebbe utilizzare l'applicazione web per cambiare la configurazione di HP JetDirect printer oppure rendere quest'ultimo indisponibile.	L
I-APP02	H	Mancanza di autenticazione in phpadmin	Un attaccante potrebbe utilizzare l'applicazione web phpadmin per eseguire delle query arbitrarie su una base di dati MySQL.	L
I-RS11	M	Abuso di ftp upload	Un attaccante potrebbe parzilamente dedurre la configurazione di proxies, firewalls, ecc	L
I-RS12	H	Buffer overflow in Server Message Block	Un attaccante potrebbe eseguire del codice arbitrario sul sistema operativo che ospita un SMB vulnerabile.	M/H
I-RS13	H	Buffer overflow in Sendmail	Un attaccante potrebbe eseguire codice arbitrario sul sistema operativo che ospita un server sendmail vulnerabile.	M/H
I-RS14	H	Buffer overflow in Samba Server	Permette un'errata valorizzazione di una variabile il cui tipo di dato è un intero, e come conseguenza causa una vulnerabilità di buffer overflow che a sua volta potrebbe abilitare un attaccante di eseguire codice arbitrario su un sistema vulnerabile.	M/H
I-RS15	H	Buffer overflow in BIND	Permette l'esecuzione di codice arbitrario su un sistema operativo che ospita un DNS vulnerabile.	M/H
I-RS16	H	Buffer overflow nel servizio Server	Permette l'esecuzione di codice arbitrario su un sistema operativo in cui esegue un servizo Server vulerabile.	M/H

La parte maggiormente vulnerabile della rete di AAA Bank è risultata essere la rete Core nella quale si è verificata la presenza della maggior parte delle vulnerabilità complessivamente identificate. Le vulnerabilità più serie sono rappresentate da mancanza di autenticazione e/o utenze di default abilitate in server di basi di dati, e buffer overflows in vari servizi. L'impatto dal punto di vista tecnico che le vulnerabilità identificate potrebbero avere sulla rete di AAA Bank è considerabile in quanto le vulnerabilità in questione generalmente permettono tra l'altro l'esecuzione di query SQL sui basi di dati vulnerabili, l'esecuzione di codice arbitrario sui sistemi operativi ospitanti servizi vulnerabili ai buffer overflows, e negazione di servizio. Le vulnerabilità di mancata autenticazione e/o utenze di default in server di basi di dati sono esploitabili da un attaccante con una preparazione tecnica relativamente bassa, mentre le vulnerabilità di buffer overflow e format string sono esploitabili da una categoria di attaccanti più preparati. L'esploitazione dei buffer overflow è facilitato dal fatto che il codice di attacco è spesso disponibile in rete e scaricabile da tutti. Nella maggior parte dei casi comunque il codice di attacco in questione richiede lievi modifiche per essere utilizzabile.

7 Fixing Plan

Fase	Azioni	Copertura
F1	Qualora non fossero utilizzate, le utenze di default vanno eliminate; in alternativa andrebbero cambiate le relative password.	I-RS07 I-RS08
F2	Il sistema di autenticazione va abilitato, generalmente assegnando una password all'utente di amministrazione.	I-RS01 I-RS02 I-RS09 I-APP01 I-APP02
F3	Ciascuna delle vulnerabilità indicate andrebbe sistemata con l'installazione della eventuale patch normalmente rilasciata dal vendor del software. Analizzare possibili work-around qualora la patch non fosse ancora disponibile o rilasciata dal vendor.	I-RS03 I-RS04 I-RS05 I-RS06 I-RS10 I-APP01 I-RS12 I-RS13 I-RS14 I-RS15 I-RS16
F4	Stabilire le politiche di sicurezza mancanti che si reputano indispensabili per la banca e divulgarle formalmente. Ufficializzare le politiche esistenti.	I-A18
F5	Analizzare le possibilità di rendere confidenziale e proteggere lo scambio di files attraverso il server FTP accedibile anche in modalità anonymous.	I-RS11
F6	Studiare un nuovo posizionamento per la macchina di management del sistema firewall.	I-A20
F7	Ottimizzare le regole del firewall eseguendo operazioni di pulizia e di impostazione modulare dello schema.	I-A21

Tabella 6 - Piano di sicurezza a breve termine

8 Security Plan

Fase	Azioni	Copertura
S01	Ottimizzare il sistema di gestione delle password e dei profili, definire regole più stringenti per la loro assegnazione e provvedere all'implementazione di un adeguato controllo che verifichi e che faccia rispettare quanto definito.	Fixing – F1 Fixing – F2
S02	Definire e strutturare un sistema di monitoraggio degli eventi, un sistema di logging centralizzato con adeguate regole di alerting ed alarming. Arrivare quindi ad avere un adeguato security operation center che possa rilevare e gestire gli incidenti informatici e monitorare gli eventi sia tecnici che di business (event correlatiion e business monitoring).	I-A15 I-A16 I-A17
S03	Ottimizzare, formalizzare, manutenere e controllare le attività di hardening sia del parco macchine client che del parco macchine server.	I-A05 I-A06
S04	Provvedere a rendere più sicuro il traffico posta via web e la navigazione (filtraggio e controllo del contenuto) per proteggere l'azienda da qualsiasi tipologia di malware: trojans, keyloggers, spyware, backdoors…	I-A07 I-A08
S05	Rivedere il sistema di test delle patch e definire un corretto deployment sul parco macchine comprensivo di eventuale gestione del cambiamento e roll-back.	I-A11 I-A12
S06	Rivedere il sistema di profilatura, definire l'associazione tra ruolo aziendale e profili informatici in maniera tale da: o rendere operativo il prima possibile un neo-assunto o rendere operativo il prima possibile un dipendente che cambia ruolo o sede o eliminare tempestivamente i profili e le abilitazioni per quei dipendenti che cambiano sede o ruolo o eliminare tempestivamente i profili e le abilitazioni per i dipendenti dimissionari o avere in sintesi un sistema di abilitazione ed accesso alle risorse efficiente e sicuro	I-A10
S07	Definire quali sono i dati sensibili residenti sui portatili o su qualsiasi dispositivo utilizzato anche al di fuori della sede di lavoro e provvedere alla loro cifratura.	I-A06
S08	Implementare un nuovo sistema di autenticazione alla rete che preveda l'accesso solo al personale con determinati requisiti e segreghi in una lan temporanea e molto limitata chi non si trova ad essere conforme alle politiche definite.	I-A01 I-A04
S09	Rendere più fruibili ed utilizzabili le procedure esistenti ed introdurre quelle ritenute più importanti e mancanti. Questa attività dipende fortemente dalle politiche di sicurezza definite e quindi dalla fase F4 della strategia di fixing (piano a breve termine).	I-A19
S10	Progettare e rendere operativo un adeguato sistema di	I-A02

	rilevamento delle intrusioni, soprattutto per quelle relative ai server critici e a qualsiasi tipologia di variazione del loro stato.	I-A03
S11	Implementare un sistema di strong authentication per l'accesso remoto ed in generale per l'accesso alle risorse aziendali critiche.	I-A09

Tabella 7 - Piano di sicurezza a medio-lungo termine

9 Considerazioni finali e sviluppi futuri

Sensazione generale.

Giudizio parte esterna.

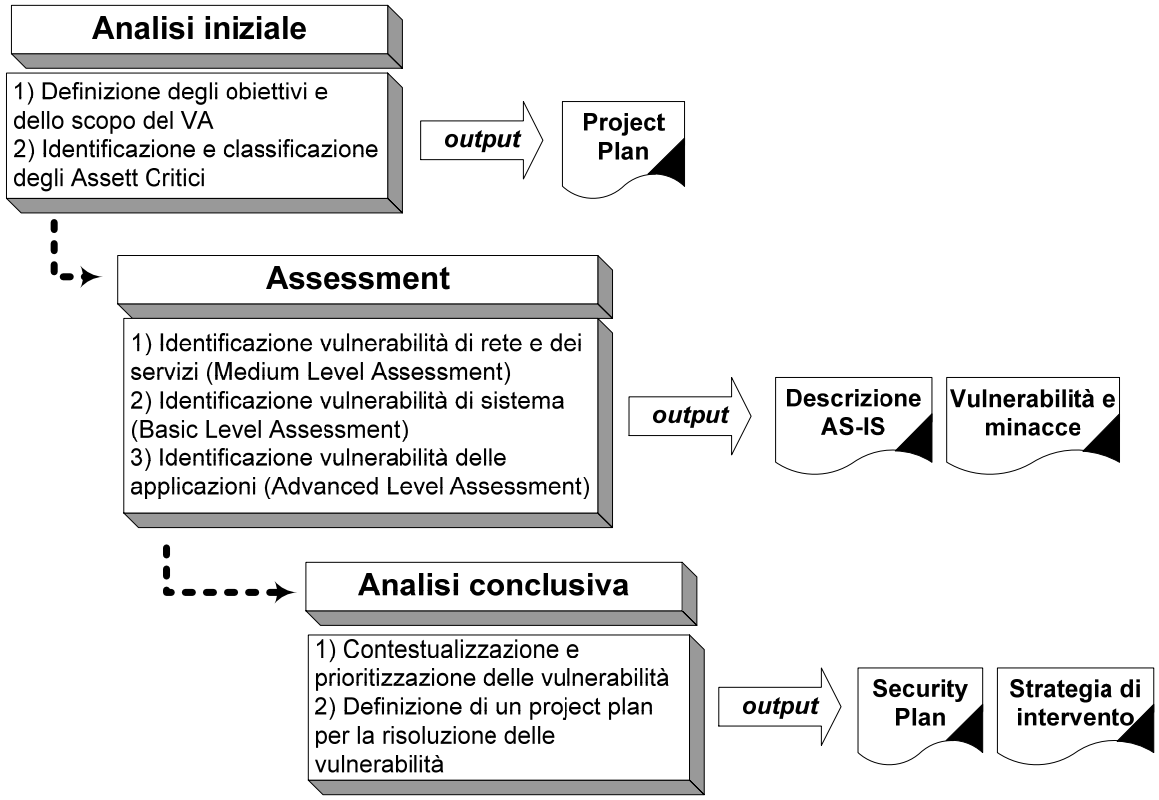
Giudizio parte interna.

Giudizio parte logico-architetturale interna.

Studio mancante: applicativa in depth, sistemistica, code review, stress test.

10 Allegato A – Approccio di assessment

Hacking Team ha adottato una metodologia di "Vulnerability Assessment" che prevede tre distinte fasi, schematizzate nella figura seguente: **Analisi Iniziale, Assessment e Analisi Conclusiva**.



10.1 Analisi Iniziale

L'analisi iniziale è la prima fase che caratterizza un assessment e consiste nel definire con precisione gli obiettivi di tale attività. Come per ogni servizio deve essere chiaro sia al committente, sia al mandatario, quali sono i risultati attesi dalla prestazione fornita. A tale scopo è importante definire e pianificare con precisione diversi aspetti:

- **L'oggetto dell'assessment**: è necessario identificare i confini entro cui condurre l'attività in termini di sistemi informativi coinvolti.
- **Il contesto operativo**: è necessario definire la modalità e i tempi secondo cui sarà condotta l'attività sia in termini di strumenti, sia in termini di risorse coinvolte da entrambi le parti.

- **Il livello di accuratezza**: è necessario stabilire il dettaglio che si intende raggiungere con l'assessment al fine di pianificare correttamente le attività successive. Questo aspetto è in parte già chiarito nel paragrafo degli obiettivi del presente documento: il livello di approfondimento garantito è quello specificato nella Fase 1.
- **Deliverables**: è necessario definire a priori il modello e la tipologia di documentazione che l'assessment produrrà al fine di soddisfare le esigenze della parte committente. Solitamente la documentazione prodotta è la seguente:
    - Documento di progetto
    - Security Plan (piano di intervento e contromisure a copertura delle vulnerabilità)

Sulla base di questa analisi iniziale saranno pianificate le varie attività che caratterizzeranno le due fasi successive: assessment e analisi conclusiva. È importante sottolineare che per valutare correttamente l'importanza delle vulnerabilità riscontrate durante la fase di assessment, i soli aspetti tecnici non sono sufficienti. Questo perchè la vulnerabilità deve essere ponderata sulla base della criticità degli asset coinvolti. L'importanza di identificare gli asset critici è ancora più evidente nella definizione del piano di risoluzione, dove la priorità e la modalità degli interventi deve essere relazionata al valore dell'asset stesso.

10.2 Assessment

Questa parte della metodologia è ampiamente dettagliata nei rispettivi paragrafi 11.1 Assessment sistemistico, 11.2 Assessment di rete e dei servizi, 11.3 Assessment applicativo.
Ovviamente a seconda dello scenario e del target che si presentano, l'assessment si occuperà di uno di questi tre livelli oppure di un misto dei tre nel caso di analisi complesse e diversificate.

10.3 Analisi conclusiva

L'analisi conclusiva, come si evince dal termine stesso, ha lo scopo di concludere l'assessment, fornendo la documentazione contenente i log di evidenza dell'attività svolta, i report delle varie tipologie di vulnerabilità riscontrate e il piano d'intervento consigliato.
La parte di documentazione relativa ai report delle vulnerabilità sarà strutturata secondo la classificazione descritta precedentemente e pesata sulla base delle criticità definite durante

l'analisi iniziale. La gravità di una vulnerabilità sarà quindi frutto sia del livello d'importanza in termini tecnici (pericolosità[2]), sia in termini di business aziendale (criticità[3]).

Il security plan ed il piano d'intervento saranno, in modo analogo alla classificazione delle vulnerabilità, redatti tenendo in considerazione la gravità delle lacune riscontrate. Il Security Plan, che contiene il piano di intervento, è invece di più ad alto livello e comprende la strategia di sicurezza che il cliente porterà avanti con l'intento di aumentare il livello di sicurezza globale (reti, sistemi, applicazioni e procedure).

[2] Con pericolosità s'intende quanto la vulnerabilità in questione comporti la possibilità di compromissione dei parametri di disponibilità, riservatezza e integrità dell'asset. Ad esempio, un *denial of service* è sicuramente meno pericoloso di un'escalation a diritti di amministrazione del sistema di un server critico.

[3] Con criticità s'intende quanto la vulnerabilità in questione possa avere un impatto sul business aziendale. Ad esempio, un exploit remoto sarà più grave se legato a un server dove è presente il database dei clienti, rispetto al PC della segreteria non ospitante dati sensibili.

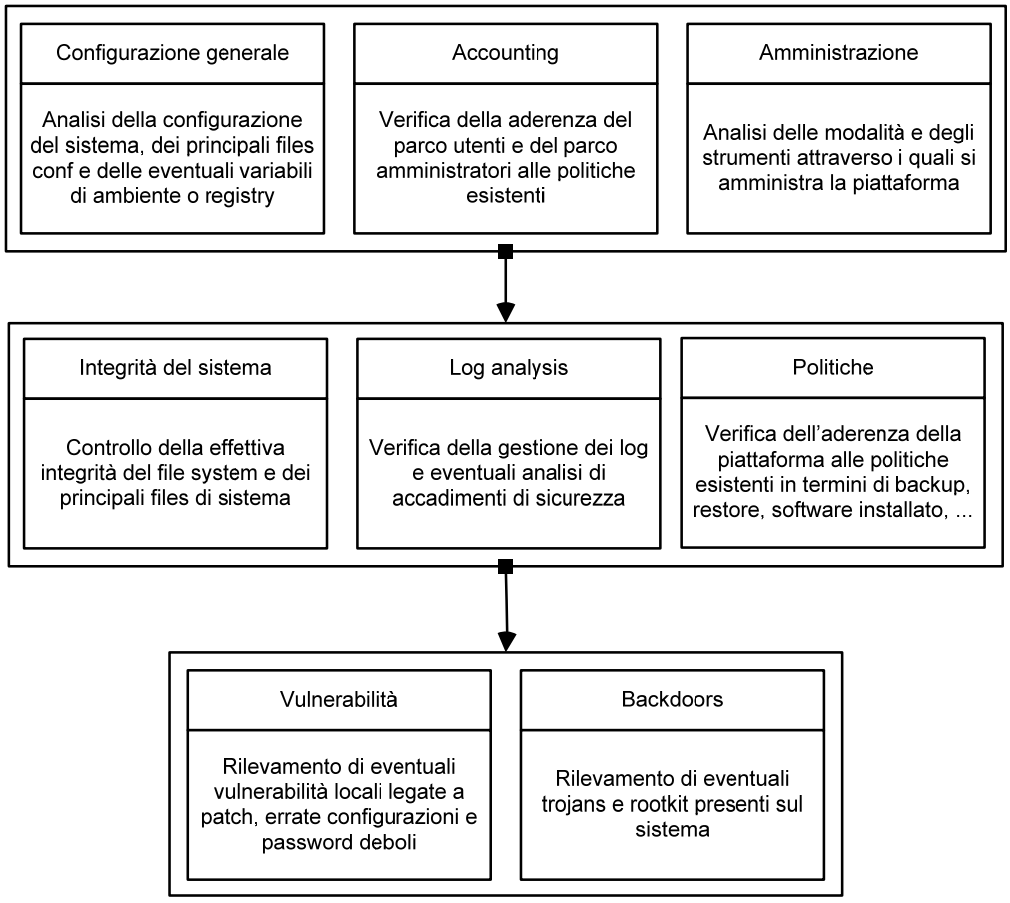
11 Allegato B – Metodologia di assessment

11.1 Assessment sistemistico (non oggetto di questa attività)

Questo genere di assessment richiede una notevole esperienza in ambito sistemistico; infatti le figure professionali che vengono coinvolte sono esperti conoscitori dei sistemi e delle piattaforme, abituati a focalizzare maggiormente l'attenzione sugli aspetti di sicurezza.

In un assessment completo è importante tenere in considerazione anche questa tipologia, che evidenzia vulnerabilità e minacce presenti, anche se non *raggiungibili* dal perimetro esterno. In questo caso (che costituisce solo un esempio di una moltitudine di casistiche possibili), l'attacco potrebbe essere portato a compimento dall'interno, cioè dalla parte in cui la vulnerabilità si *rende visibile*.

Le principali aree tematiche da tenere in considerazione durante un'analisi di sicurezza sistemistica sono evidenziate dai passi mostrati sinteticamente nella seguente figura.



Configurazione generale

Ci si occupa della piattaforma in generale, partendo dai parametri di configurazione di sistema, dei dispositivi, dei files principali e di conf, ed arrivando alle variabili di ambiente e dei registri (in caso di sistema operativo microsoft). Si terranno in considerazione, come linee guida, le *best practices* relative alla piattaforma in oggetto e lo stato dell'arte della sicurezza al momento dell'esecuzione dell'assessment.

Accounting

Il focus della presente tematica riguarda gli utilizzatori locali e remoti della piattaforma esaminata: si controlleranno le configurazioni e le profilature assegnate al parco utenti, al parco amministratori e a qualsiasi altro profilo esistente sulla macchina. Verranno analizzate la procedura e gli strumenti di autenticazione ed eventuali scostamenti rispetto alle politiche scritte o definite e volute dal cliente.

Amministrazione

Con l'ausilio di brevi interviste e di verifiche sul campo, si procederà a rilevare le modalità e gli strumenti di amministrazione della piattaforma esaminata, nell'ottica di evidenziare vulnerabilità di tipo procedurale oppure vulnerabilità legate alla tipologia di gestione scelta. Ovviamente questo tipo di studio verrà eseguito sia per l'amministrazione locale sia per l'eventuale amministrazione remota.

Integrità del sistema

In questa parte si verifica lo stato di sicurezza del file system dal punto di vista della sua integrità, ricorrendo ad analisi locali specializzate che, in azioni di assessment ripetute, possono coincidere anche con gap analysis rispetto all'ultima azione effettuata. Qualora il cliente abbia una politica che definisca una base integra di partenza, la verifica dell'integrità potrebbe essere condotta in riferimento a quanto stabilito e voluto per quella determinata macchina.

Log analysis

Per particolari tipologie di assessment di tipo basic, potrebbe esserci la necessità di risalire ad un particolare evento passato oppure di rilevare una particolare situazione anomala. Questo è il caso in cui si ricorre all'analisi dei log di sistema. Qualora questa attività non sia necessaria o non sia richiesta, ci si limiterà a verificare che la configurazione e la gestione del sistema di logging sia aderente a quanto definito.

Politiche

Questa parte riguarda la presenza di eventuali politiche definite dal cliente su tutto iul parco macchine e/o sulla machina specificatamente analizzata. Si controllerà insieme al cliente l'effettiva

aderenza a quanto da lui stesso voluto, verificando ad esempio la procedura di backup/restore della configurazione, il salvataggio e la protezione di eventuali dati sensibili, …
È questa la fase in cui si identificano anche installazioni estranee o non autorizzate rispetto a quanto stabilito esserci sulla macchina di riferimento.

Vulnerabilità

Si esegue il rilevamento di vulnerabilità esistenti localmente e relative ad errate configurazioni oppure alla necessità di patch evolutive o di sicurezza. È questa la parte in cui si verificherà inoltre la presenza di eventuali password deboli.

Backdoors

Un ruolo importante è assunto da questa fase, che consiste nel rilevamento di eventuali troiani o rootkit presenti sulla macchina ed esistenti a fronte di un attacco avvenuto in passato. La loro individuazione e rimozione è fondamentale per negare al possibile attaccante la possibilità e l'enorme vantaggio di avere una backdoor in suo favore.

11.2 Assessment di rete e dei servizi

Le attività di Ethical Hacking (vulnerability assessment e penetration test) da noi eseguite tentano di emulare al 100% il comportamento di un vero hacker.

Analisi non invasiva

1. 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.

2. 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

3. 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

4. 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.

5. ESCALATING PRIVILEGES[4]

   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

6. 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

[4] Vogliamo specificare che, considerata la natura della presente offerta, le nostre attività *non si spingeranno in nessun caso oltre questo punto (ESCALATING PRIVILEGES) a meno di una specifica autorizzazione in tal senso da parte del cliente.* In altre parole, si cercherà di **dimostrare l'effettiva possibilità di assumere il controllo dei sistemi senza apportare alcuna modifica agli stessi.**

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.

7. COVERING TRACES AND CREATING BACK DOORS

   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.

11.3 Assessment applicativo

Questa analisi è costituita da una serie di tentativi d'attacco che coinvolgono solo i protocolli di comunicazione utilizzati dagli utenti finali per interagire con le applicazioni.

Nel caso specifico delle applicazioni web, tali attacchi sono basati su manipolazioni dei pacchetti HTTP che vengono scambiati fra i browser degli utenti ed il web server. Esistono diverse categorie di attacchi verso applicazioni web, che possono portare alla compromissione di uno o più layer dell'intera infrastruttura applicativa: web server, application server, data tier.

Caratteristica comune a tutti gli attacchi applicativi è la completa trasparenza ad ogni sistema di difesa perimetrale (firewall, ids, ecc.): manipolazioni dei protocolli di layer 7 (applicativi) non possono essere rilevate da dispostivi che analizzano il traffico a layer 3 (network).

Il test sarà condotto in modalità anonima ed in "user-mode". Ciò significa che, preventivamente, dovrà essere creato un account tramite le usuali procedure di attivazione al fine di permettere a Hacking Team di accedere come utente autorizzato. Non saranno accettati account di altro tipo (di test interno, amministrativi, etc.) poichè non fornirebbero la corretta valutazione circa il rischio che un utente registrato possa cercare di accedere in modo fraudolento ad informazioni per cui non è autorizzato. L'attività comprende l'analisi dell'applicazione in termini architetturali, verranno analizzate le configurazioni delle macchine interessate, sia a livello di sistema operativo che applicativo.

In generale, le vulnerabilità di livello applicativo sono spesso legate ad errori contenuti nel codice delle applicazioni. Esistono due classi di errori, che richiedono differenti strategie per essere identificati e rimossi: errori logico-architetturali ed errori di implementazione.

Errori logico-architetturali

Gli errori logico-architetturali consistono nel mancato utilizzo di meccanismi di sicurezza, oppure nell'utilizzo di meccanismi non adeguati a raggiungere lo scopo desiderato. Tali errori sono imputabili ad una non corretta definizione dei requisiti di sicurezza e/o ad una inadeguata progettazione dell'architettura.

Gli errori logico-architetturali più comuni sono i seguenti:

- gestione non corretta delle sessioni;
- uso di meccanismi di autenticazione deboli, che
  - permettono agli utenti di utilizzare password *guessable;*
  - rilasciano informazioni che permettono di restringere lo spazio di ricerca per attacchi di tipo *brute force*;
- trasmissione di informazioni sensibili su canali non cifrati;
- assunzioni errate in merito all'attendibilità e veridicità di input ricevuti dall'utente;
- assunzioni errate in merito alla funzionalità di sistemi e/o applicazioni *client-side* (ad esempio, browser web) che si trovano sotto il controllo dell'utente (o dell'attaccante!).

Errori implementativi

Questi errori si originano in fase di sviluppo, quando specifiche di alto livello, corrette dal punto di vista logico, vengono tradotte in codice che non gestisce correttamente tutti i casi i possibili; i malfunzionamenti che si verificano in casi particolari possono essere sfruttati per indurre nelle applicazioni comportamenti non previsti e/o non desiderati.

La grande maggioranza degli errori implementativi è dovuta ad una non corretta validazione dei parametri in ingresso, oppure alla gestione non corretta di alcuni input particolari, non previsti dal programmatore. La loro natura rende estremamente difficile prevederne l'impatto: in alcuni casi, questi errori possono avere conseguenze gravi sulla sicurezza di una applicazione, anche se gli elementi di codice interessati non sono direttamente legati a funzionalità critiche.

Gli attacchi di livello applicativo sfruttano vulnerabilità (sia di natura logico-architetturale, sia di natura implementativa) per indurre nelle applicazioni comportamenti anomali, le cui conseguenze possono essere le più disparate: crash dell'applicazione, furto di dati, accesso ai sistemi su cui le applicazioni sono eseguite, ecc.

Allo scopo di inquadrare il tema della sicurezza del livello applicativo, sia in termini di "opportunità" offerte all'intrusore, sia di minacce per le potenziali vittime di intrusioni, si dà una sintetica descrizione delle principali tecniche di attacco utilizzate nell'ambito delle applicazioni web.

I concetti e la terminologia introdotti saranno utilizzati nel presente documento per descrivere i risultati dell'assessment svolto.

11.3.1 Authentication brute-forcing

- ***Obiettivo***: accesso aree riservate ad utenti in possesso di opportune credenziali.
- ***Attaccanti***: chiunque non sia in possesso di credenziali valide ed abbia interesse ad accedere alle informazioni contenute nelle aree riservate, oppure chi, pur possedendo credenziali valide, intende accedere all'area riservata con l'identità di un altro utente.
- ***Descrizione***: consiste nella sottomissione, spesso con l'ausilio di tool automatici, di un grande numero di credenziali (ad esempio coppie username,password), fino ad ottenere una risposta di autenticazione riuscita dal sistema. La generazione delle credenziali può prevedere l'uso di regole (ad esempio, generazione di tutte la password di sei caratteri costituite da soli caratteri alfanumerici) oppure di dizionari preesistenti.
- ***Condizioni necessarie per l'attacco***: ogni sistema che dispone di un sistema di autenticazione è esposto a questo attacco.
- ***Probabilità di successo***: dipende dalla dimensione dello spazio delle credenziali.
- ***Contromisure***[5]: gli attacchi di tipo brute force non possono essere prevenuti, ma esistono tecniche efficaci per ridurne drasticamente la probabilità di successo:
    - limitazione del numero massimo di tentativi di autenticazione falliti per ogni connessione;
    - adozione di controlli che vietano l'uso di password guessable o troppo semplici;
    - eliminazione dei messaggi di errori informativi.

11.3.2 Cross site scripting (XSS)

- ***Obiettivo***: furto d'identità ai danni di utenti di applicazioni web che fanno uso di cookie per la gestione delle sessioni.
- ***Attaccanti***: chiunque sia interessato al furto dell'identità di un utente autorizzato (che abbia stabilito una sessione con l'applicazione web).
- ***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,

[5] Le contromisure indicate in questo come in tutti gli altri casi sono da intendersi ovviamente come generiche. Caso per caso potranno essere o smentite, o confermate oppure rese più precise e puntuali.

ecc.). Gli 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. Gli attacchi di cross site scripting sono possibili quando l'applicazione web restituisce al browser (per normale logica di funzionamento o a causa di una condizione di errore) parametri sottoposti dall'utente in una precedente richiesta.

- ***Condizioni necessarie per l'attacco***: assenza di controlli sull'input ricevuto ed errori relativi all'escaping di metacaratteri nell'HTML ritornato al browser.
- ***Probabilità di successo***: questo attacco richiede l'uso di tecniche di social engineering per indurre la vittima a stabilire una sessione con l'applicazione target e sottoporre ad essa una richiesta contenente il codice malizioso. Frequentemente questo viene fatto per mezzo di email che invitano a seguire un link verso l'applicazione target. La probabilità di successo di tali attacchi è solitamente bassa.
- ***Contromisure***: gli attacchi di tipo XSS possono essere neutralizzati mediante le seguenti tecniche:
  - filtraggio dei parametri in input, mediante filtri che eliminano dall'input i metacaratteri utilizzati in HTML e linguaggi di scripting client-side (<, >, apici, ecc.);
  - escaping dei metacaratteri contenuti nei parametri in input che devono essere inseriti in pagine HTML restituite al browser degli utenti.

11.3.3 SQL Injection

- ***Obiettivo***: 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.
- ***Attaccanti***: utenti autorizzati che mirano ad accedere ad informazioni per le quali non possiedono diritti di accesso; utenti non autorizzati.
- ***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.

- ***Condizioni necessarie per l'attacco***: mancanza di filtri di validazione dell'input, che eliminano dai parametri inviati dall'utente token pericolosi, come parole chiave riservate del linguaggio SQL (ad esempio, SELECT, OR, ecc.).
- ***Probabilità di successo***: fortemente dipendenti dalla logica applicativa.
- ***Contromisure***: gli attacchi di tipo SQL injection possono essere neutralizzati mediante le seguenti tecniche:
  - filtraggio dei parametri in input, mediante filtri che eliminano dall'input token riservati e metacaratteri del linguaggio SQL;
  - gestione degli errori di accesso al layer di accesso ai dati, allo scopo di intercettare e bloccare la visualizzazione lato client dei messaggi di errore.

11.3.4 Path traversal

- ***Obiettivo***: 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.
- ***Attaccanti***: questo tipo di attacco può essere portato da chiunque possa stabilire una connessione HTTP verso i server su cui è pubblicata l'applicazione.
- ***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. Poichè 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. Si noti che questo attacco non è in alcun modo correlato alla logica applicativa, ma sfrutta eventuali vulnerabilità del server HTTP.
- ***Condizioni necessarie***: queste tecniche possono essere utilizzate in presenza di web server sui quali non sono installate le security patch opportune; in ogni caso, la loro applicabilità non dipende dalla particolare applicazione pubblicata sul web server.
- ***Probabilità di successo***: dipende dall'accuratezza della manutenzione del web server.
- ***Contromisure***: aggiornamento dei web server mediante applicazione delle opportune patches.

11.3.5 OS command injection

- ***Obiettivo***: esecuzione di comandi di sistema sulle macchine su cui insiste l'applicazione.

- ***Attaccanti***: questo tipo di attacco può essere portato da chiunque possa stabilire una connessione HTTP verso i server su cui è pubblicata l'applicazione.
- ***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.
- ***Condizioni necessarie***: queste tecniche possono essere utilizzate in presenza di componenti dinamici che richiamano comandi di sistema senza effettuare un corretto parsing dei parametri di input.
- ***Probabilità di successo***: dipendenti dall'accuratezza della logica di validazione dei parametri in input.
- ***Contromisure***: gli attacchi di questo tipo possono essere neutralizzati eliminando dai parametri in input token riservati e metacaratteri potenzialmente pericolosi che potrebbero generare ambiguità per l'interprete dei comandi.

11.3.6 Cookie poisoning

- ***Obiettivo***: 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.
- ***Attaccanti***: gli attacchi di cookie poisoning possono provenire da qualsiasi utente sul cui browser l'applicazione setta cookie.
- ***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.
- ***Probabilità di successo***: dipendenti dal livello di conoscenza da parte dell'attaccante della logica di elaborazione dei dati contenuti nei cookie.
- ***Contromisure***: limitare l'uso dei *cookie* alla memorizzazione di informazioni non critiche; nel caso questo non sia possibile, devono essere utilizzate tecniche (ad esempio crittografia) per impedire la modifica dei *cookie*.

11.3.7 Forceful browsing

- ***Obiettivo***: accesso non autorizzato a pagine e/o funzionalità dell'applicazione.

- ***Attaccanti***: chiunque non sia in possesso di credenziali per accedere a tali pagine/funzionalità.
- ***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.
- ***Probabilità di successo***: dipendenti dal livello di conoscenza da parte dell'attaccante della struttura dell'applicativo. Tale livello può essere molto elevato per ex utenti che sono stati disabilitati.
- ***Contromisure***: implementare una logica di controllo dello stato della sessione che impedisca l'accesso ad ogni parte dell'applicazione ad utenti non associati a sessioni autenticate.

11.3.8 Information leaking

- ***Obiettivo***: ottenere informazioni sul sistema da attaccare.
- ***Attaccanti***: chiunque possa navigare il sito.
- ***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.
- ***Probabilità di successo***: dipendenti dal livello di *security-awareness* degli sviluppatori.
- ***Contromisure***: eliminare dati sensibili dal codice HTML delle pagine web ritornate dall'applicazione.

12 Allegato C – Politiche di sicurezza

Accesso remoto
Definisce gli standard e le direttive per permettere ed autorizzare la connessione alla rete dell'organizzazione da parte di host e/o reti esterne ad essa. Dovrebbe contenere anche la parte di *mobile computing* e *storage devices* per stabilire le linee guida atte all'autorizzazione ed al controllo di quei dispositivi che richiedono un accesso alle risorse ed alle informazioni aziendali.
Accesso in dial-in da parte di utenze autorizzate
Definisce l'appropriato utilizzo degli accessi di tipo dial-in ed il loro uso da parte di personale autorizzato.
Accordi di connessione con organizzazioni terze
Definisce gli standard ed i requisiti, inclusi quelli di tipo legale, necessari al fine di interconnettere la rete di un'organizzazione esterna all'infrastruttura di comunicazione della società. Questo tipo di accordo deve essere accettato e sottoscritto da entrambe le parti in causa.
Aggiornamento del parco macchine
Stabilisce le regole e le tempistiche per verificare la presenza di aggiornamenti, le priorità di intervento e la gestione del cambiamento. A seconda della criticità, della location e di altri fattori, il parco macchine avrà delle regole differenti.
Analisi dei rischi
Definisce i requisiti e conferisce l'autorità necessaria al gruppo responsabile per la sicurezza informatica al fine di identificare, analizzare e porre rimedio (o gestire/accettare) ai rischi che sono associati ai dati aziendali ed all'infrastruttura informatica dell'organizzazione. È importante che vengano identificati e ben precisati quali sono gli asset aziendali ritenuti critici e sensibili.
Audit e scansione delle vulnerabilità
Definisce i requisiti e fornisce i poteri al gruppo responsabile della sicurezza informatica per condurre azioni di controllo e verifica dei rischi al fine di assicurare l'integrità delle informazioni e delle risorse aziendali, per investigare sugli incidenti, per assicurare la conformità alla politica di sicurezza e per monitorare l'attività di utenti e sistemi dove ritenuto opportuno.
Business continuity e disaster recovery
Definisce le direttive e i requisiti minimi necessari per affrontare la tematica della business continuity e del disaster recovery. Stabilisce i tempi di indisponibilità accettabili per i vari servizi in relazione al business.
Cifratura dei dati
Definisce i requisiti per gli algoritmi di cifratura usati all'interno dell'organizzazione e verso l'esterno della stessa.
Clean-desk
Stabilisce il comportamento che si deve tenere nella propria postazione di lavoro e cosa non è consentito mantenere esposto a tutti, intermini di divulgazione di dati sensibili o personali. Tale politica contempla anche il comportamento da tenere in merito ad informazioni locali eventualmente presenti nella postazione informatica.
Comunicazioni wireless
Definisce gli standard e le direttive che devono rispettare i sistemi di tipo wireless utilizzati per connettersi all'infrastruttura di comunicazione della società.
Database delle credenziali di accesso
Definisce i requisiti per memorizzare e recuperare in modalità sicura dal database le relative coppie username-password dei vari utenti.
Etica

Definisce le basi per la diffusione di una cultura caratterizzata da apertura, correttezza e integrità nello svolgimento delle normali attività lavorative.
Extranet policy
Definisce i requisiti ai quali le organizzazioni esterne devono attenersi per poter effettivamente ottenere i permessi di accesso corretti.
Formazione
Stabilisce il percorso formativo per i propri dipendenti e i mezzi a disposizione (anche a livello organizzativo) per perseguire gli obiettivi. Definisce inoltre i punti di controllo della formazione e verifica dello stato raggiunto.
Gestione degli apparati posizionati verso l'esterno
Definisce gli standard da soddisfare da parte di tutti gli apparati dell'organizzazione presenti al di fuori dei firewall aziendali verso internet (DMZ) e/o extranet.
Gestione degli incidenti
Definisce il team di incident response, le responsabilità e le modalità di gestione degli incidenti. Consente di realizzare un sistema di allarmistica corretto ed idoneo a quanto regolamentato.
Gestione degli outsourcer
Stabilisce i criteri di sicurezza minimi a cui deve soddisfare un outsourcer per essere considerato idoneo alle caratteristiche richieste dall'azienda.
Gestione dei provider
Stabilisce i criteri di sicurezza minimi a cui deve soddisfare un provider (ISP-Internet Service Provider e/o un ASP-Application Service Provider) per essere considerato idoneo alle caratteristiche richieste dall'azienda.
Gestione del personale esterno
Stabilisce i requisiti minimi a cui deve soddisfare il personale esterno (prevalentemente consulenti) durante l'accesso fisico e durante l'accesso informatico.
Gestione delle acquisizioni
Definisce le responsabilità in merito alle acquisizioni della corporate e stabilisce i requisiti minimi che deve soddisfare il relativo assessment che deve essere completato dal team della sicurezza informatica.
Gestione di eventuali nuove sedi
Definisce le responsabilità in merito alle connessioni al sistema informatico aziendale di reti (LAN, WAN) di nuove sedi. Definisce inoltre i requisiti minimi per il completamento, da parte del gruppo responsabile della sicurezza informatica, di un assessment in merito a tali connessioni.
Laboratori e ambienti di test
Definisce i requisiti per i laboratori interni (o posizionati in altro ambiente), al fine di garantire la confidenzialità dei dati e la salvaguardia della tecnologia, e far sì che i servizi in produzione siano protetti dalle attività di laboratorio. Dovrebbero essere definite direttive differenti a seconda della location dell'ambiente.
Monitoraggio, logging ed allarmistica
Definisce il target del monitoraggio e stabilisce le direttive necessarie per una corretta analisi degli eventi. Consente di realizzare un sistema di reportistica corretto ed idoneo a quanto regolamentato. Stabilisce inoltre le direttive necessarie alla fase di logging degli eventi sulle sorgenti ed alla fase di allarmistica (modalità e metodi di emissione dell'allarme).
Posta elettronica
Definisce gli standard e le regole per prevenire danni all'immagine pubblica dell'organizzazione e regolamenta l'utilizzo della casella di posta aziendale (e, se consentito, anche di quella personale). Stabilisce inoltre quali informazioni inviate e/o ricevute debbono essere memorizzate e per quanto tempo ciò deve avvenire.
Profilatura ed assegnazione equipaggiamento
Stabilisce i criteri secondo i quali si attribuiscono ai vari ruoli aziendali i relativi e i soli permessi

informatici ed assets fisici necessari all'espletamento delle proprie funzioni (provisioning). Definisce inoltre le regole di workflow in caso di approvazioni multiple o di mancanza del personale autorizzativo o in caso di altri accadimenti, nonchè le direttive ed i controlli per le operazioni di de-provisioning (in caso di trasferimento, di cambiamento di ruolo o di dimissioni).
Protezione e gestione dei virus e dei malware
Definisce le linee guida per ridurre in modo reale le minacce derivanti dalla presenza di eventuali virus nella rete dell'organizzazione. Definisce inoltre i requisiti che devono essere soddisfatti da tutti i computer connessi alla rete informatica al fine di assicurare un'efficace individuazione e prevenzione dai virus informatici. Fa parte di queste linee guida anche il comportamento da tenere nello scambio di mail, il gergo adottato e il tipo di informazioni e/o allegati trasmissibili. Si contempla, in questa politica, anche qualsiasi altra tipologia di malware.
Protezione e gestione delle password
Definisce gli standard e le direttive per la creazione, la protezione e la variazione delle password. E questo sia per l'utenza che per l'amministrazione dei sistemi.
Sensibilità e criticità dei dati
Definisce i requisiti per la classificazione e la messa in sicurezza dei dati della società nel modo appropriato al loro livello di sensibilità e di criticità.
Sensibilizzazione
Indica le azioni che l'azienda è intenzionata a perseguire per sensibilizzare i propri dipendenti sulla tematica della sicurezza informatica, degli aspetti legali e del comportamento sicuro da tenere per il beneficio di tutti. Si definisce in tale politica anche le modalità con cui trasferire al personale la conoscenza in termini di frode informatica, diritti di autore, illecito amministrativo, pedopornografia ed altri aspetti di ICT laws.
Sicurezza degli apparati di rete
Definisce gli standard minimali per la configurazione di sicurezza degli apparati di rete (routers, switches etc.) all'interno della infrastruttura di produzione.
Sicurezza delle reti private virtuali (VPN)
Definisce i requisiti per gli accessi remoti effettuati tramite protocollo IPSec, L2TP o SSL verso l'infrastruttura di comunicazione della società.
Sicurezza dei server
Definisce gli standard minimali per la configurazione di sicurezza dei server all'interno dell'infrastruttura informatica.
Uso di linee analogiche e/o ISDN
Definisce gli standard per l'uso di linee analogiche e/o ISDN per invio e ricezione dei fax e per la connessione ad esse dei computer.
Utilizzo dell'equipaggiamento
Definisce il consono utilizzo dell'equipaggiamento in dotazione ai dipendenti e le misure di sicurezza a cui essi devono attenersi per garantire la protezione delle risorse e delle proprietà intellettuale aziendali. Con equipaggiamento si intende qualsiasi asset infomatico in dotazione, anche per la parte di comunicazione come ad esempio mobile phones e voicemail.