Shorr Kan

digital security

Vulnerability Assessment

PABX 2008

Versione 2.1 – Marzo 2006

Obiettivo

Obiettivo del Vulnerability Assessment

Stabilire eventuali vulnerabilità sul sistema telefonico di Cliente tramite analisi dei seguenti punti :

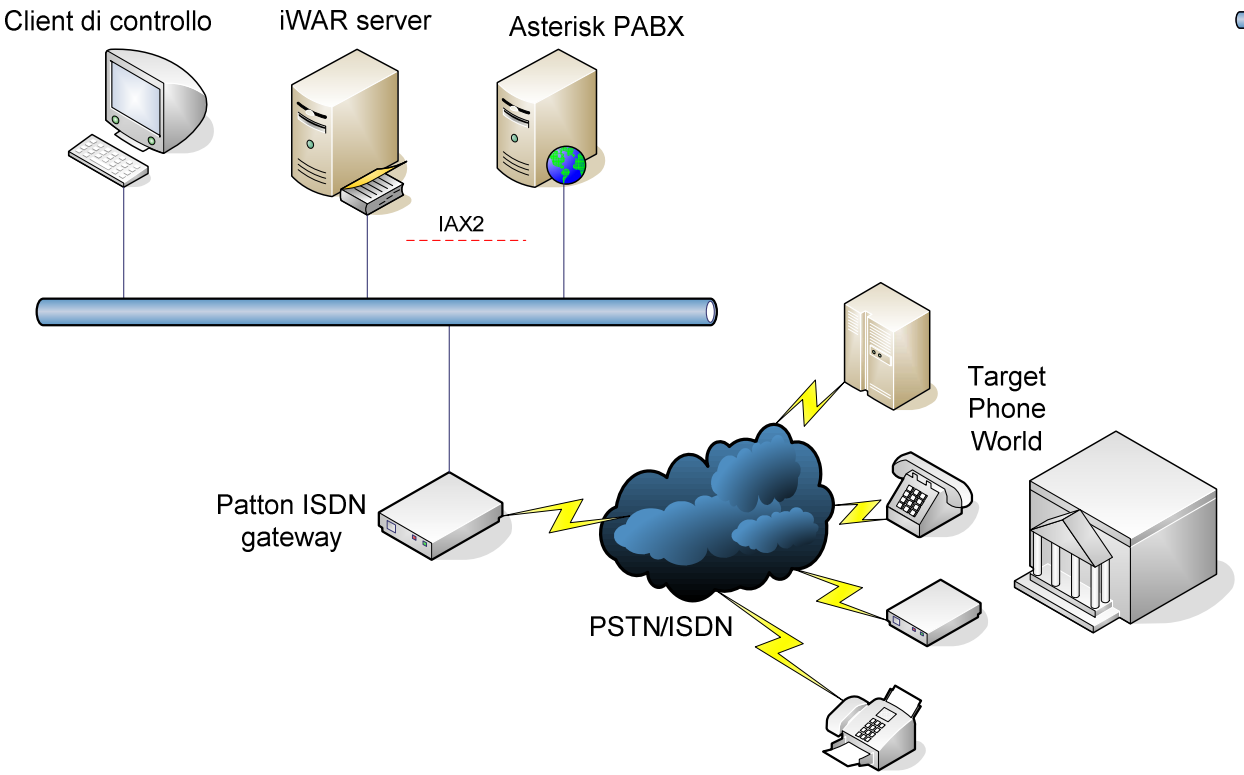
- Dial-in su Linee a campione del vostro range di numerazione 5550.xxx (per analizzare presenza o meno di modem o dialtone di accesso al PABX)
- Dial-in su tutte le linee GSM per analizzare la presenza di dialtone di accesso al PABX
- VoiceMailBox
- IVR
- Trunk tra le sedi
- Gestione remota del PABX via dialtone su canale voce o con client-pc su rete IP interna

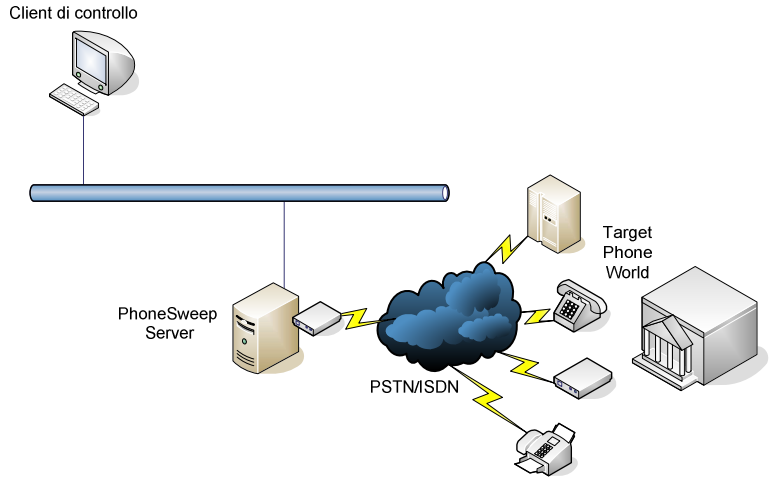
Modus Operandi

Fondamentalmente l'approccio utilizzato per effettuare un'analisi di tipo war dialing (o phone probe) è quello di chiamare tutti i numeri telefonici presenti in un determinato range e mettersi in ascolto per un certo periodo di tempo (40-50 secondi). A seconda della risposta dall'altro lato della linea si dovrà a questo punto riconoscere se l'interlocutore era un essere umano od un sistema automatico con il suo caratteristico handshake (modem, fax o pabx dialtone, ivr, vmbox).

Strumenti

Asterisk + iWAR (con gateway Patton)



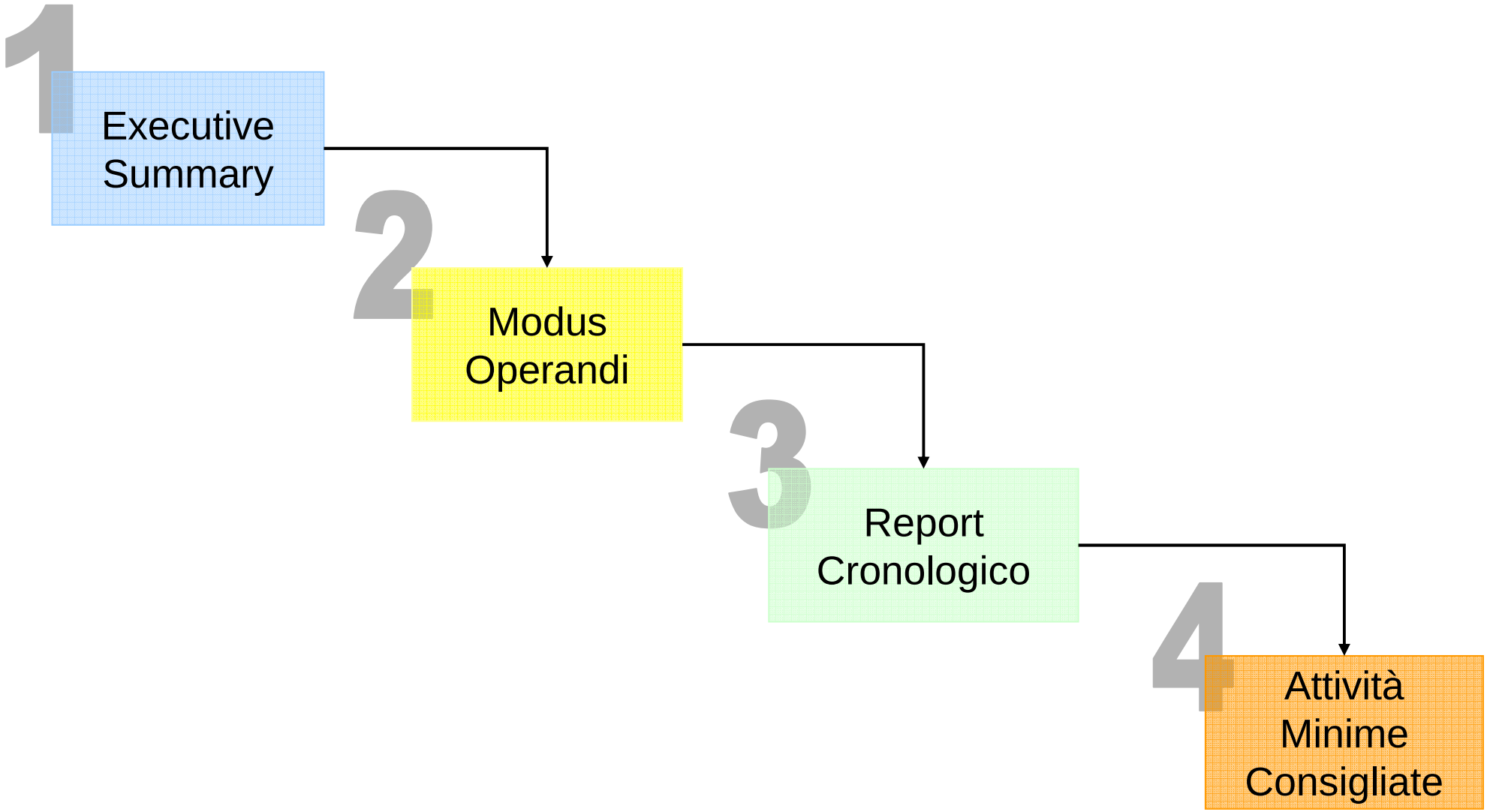


PhoneSweep

Report

Il risultato finale di un security probe è un documento tecnico dove sono evidenziate le problematiche riscontrate sia attraverso l'analisi 'a tavolino' con la parte tecnica del cliente e sia attraverso una fase di scansioni e attacchi simulati. Il documento dovrebbe sempre concludersi con i suggerimenti per l'assessment della situazione con un elenco di contromisure minime da applicare per sanare le problematiche evidenziate.

Macroblocchi del Report Tecnico finale



Scan (Modemlines)

Linea	Speed	Identificazione	Banner	Note
011-5550000	33.600 bps	ET Record Urmet	Nessuno	Non risponde a nessun comando inviato
011-5550000	33.600 bps	EMC2 controller (Linux)	Pino1 login:	Accetta tentativi di password guessing 3 volte e poi ti scollega. Non ci sono password banali.
011-5550000	2.400 bps	MD 110 Ericsson	Username ? >	Credenziali di default permettono l'accesso al sottosistema NIUX del centralino MD110 Ericsson Username: MDUSER Password: HELP
011-5550000	33.600 bps	MD 110 Ericsson	Username ? >	Credenziali di default permettono l'accesso al sottosistema NIUX del centralino MD110 Ericsson Username: MDUSER Password: HELP
011-5550000	9.600 bps	Modem Clientexx	Nessuno	
06-5550000	1.200 bps	MD 110 Ericsson Roma	Username ? >	Credenziali di default permettono l'accesso al sottosistema NIUX del centralino MD110 Ericsson Username: MDUSER Password: HELP
06-5550000	33.600 bps	Modem Log PABX Roma	Nessuno	
011-5550000	33.600 bps	EMC2 controller (Linux)	Pino2 login:	Accetta tentativi di password guessing 3 volte e poi ti scollega. Credenziali di default ti permettono però un completo accesso al sistema e da questo alla rete interna di ersel bypassando tutto il sistema di sicurezza perimetrale. Username: root Password: nasadmin Username: nasadmin Password: nasadmin
02-5550000	33.600 bps	Modem Log PABX Milano	Nessuno	

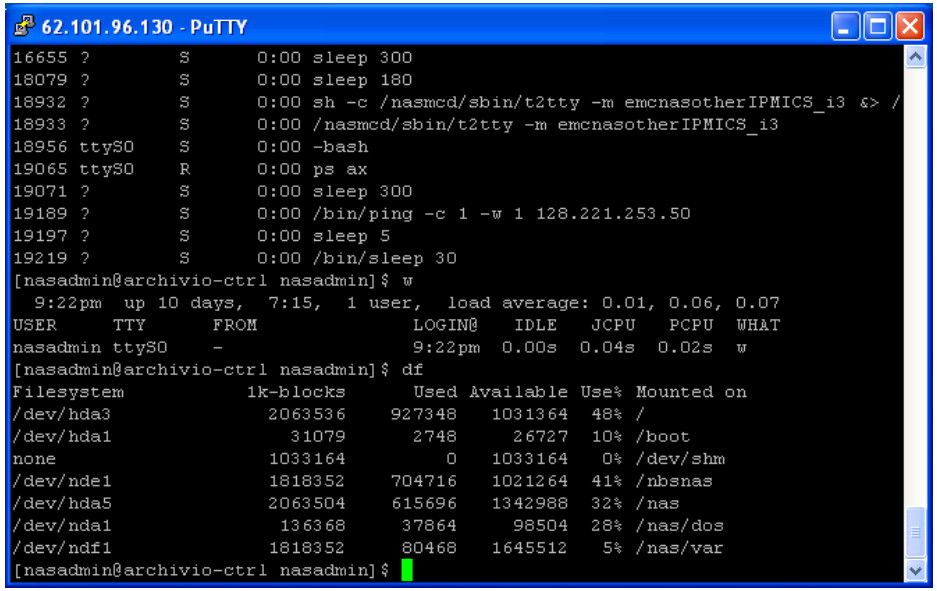
MD110 Ericsson

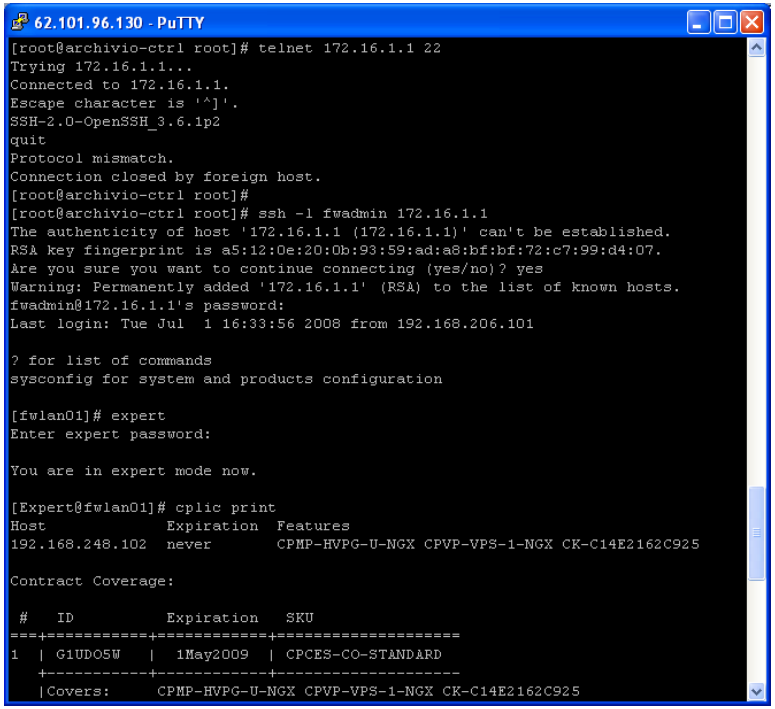
Per cui il PABX MD110 è accessibile via modem dall'esterno ed è accessibile ai numeri 011-5550111 (il PABX principale) e 011-5550222 (solo a 2400 bps, probabilmente un PABX secondario).
Tramite l'account di default MDUSER con password HELP si accede al sottosistema NIUX da cui è possibile effettuare ping e telnet verso la rete interna Cliente dall'IP 172.16.1.1 e riconfigurare alcuni paramteri del PABX (e scaricarne i LOG delle chiamate).

```
niux > help
bdsvi:        set NIU board to service mode
bdsve:         end service mode on NIU board
bdsvp:         print service mode status of NIU board
telstat:      Print Telnet and MML statistics
ping:         ping a remote host
netcnf:        Print and configure port IP parameters
help:         Command Info
h:           Command Info
quit:         quit niux shell
```

SAN

La SAN EMC2 al numero 011-5550333 presenta delle credenziali non banali e ti scollega dopo tre tentativi di password guessing. Invece la SAN EMC2 al numero 011-5550444 (sancl002) permette l'accesso direttamente alla rete interna di Cliente su IP 172.16.1.2 con credenziali di default nasadmin/nasadmin e root/nasadmin.





Definizione gradi di rischio

2 DEFINIZIONE DEI GRADI DI RISCHIO

Prima definisco i livelli di rischio secondo un range da 0 a 9 :

Livelli di rischio per Probabilità ed Impatto	
0 – 2	**Low**
3 – 5	**Medium**
6 – 9	**High**

Medio sui valori dati alle Minacce ed alle Vulnerabilità (che mi danno insieme la **Probabilità** dell'evento) :

Minacce					Vulnerabilità			
Skill level inverso	Motivazione	Opportunità	Dimensione		Facilità di scoperta	Facilità da sfruttare	Diffusione	Tracciabilità
0-9	0-9	0-9	0-9		0-9	0-9	0-9	0-9
Probabilità complessiva = 0.0 (media)								

Skill level : livello tecnico dell'attaccante per sfruttare tale vulnerabilità (0=alto, 9=basso)
Motivazione : quanto può essere motivato l'attaccante (0=nessuna ricompensa, 9=grande ricompensa)
Opportunità : quali risorse ed opportunità sono necessarie per trovare la falla (0=pieno accesso al sistema, 9=accesso anonimo)
Dimensione : quanto può essere grande il gruppo di attaccanti (0=sviluppatori interni,9=chiunque su internet)
Facilità di scoperta : quanto è facile scoprire tale vulnerabilità (0=difficile, 9=facile)
Facilità da sfruttare : quanto è semplice sfruttare tale vulnerabilità (0=difficile, 9=facile)
Diffusione : quanto è diffusa e conosciuta tale vulnerabilità (0=poco, 9=molto)
Tracciabilità : quanto è invisibile questo tipo di attacco (0=facilmente individuabile,9=difficilmente individuabile)

Medio sui valori dati agli Impatti Tecnici e di Business (che mi danno insieme l'**Impatto** dell'evento) :

Impatti Tecnici					Impatti di Business			
Perdita di riservatezza	Perdita di integrità	Perdità di disponibilità	Perdità di tracciabilità		Danno economico	Danno di immagine	Non compliance	Violazione Privacy
0-9	0-9	0-9	0-9		0-9	0-9	0-9	0-9
Impatto complessivo = 0.0 (media)								

Perdita di riservatezza : quanti dati riservati e/o sensibili espongo (0=informazioni pubbliche,9=informazioni segrete)
Perdita di integrità : possono essere modificati i dati (0=minimamente,9=completamente)
Perdita di disponibilità : interruzione di servizio e quanto il servizio è critico (0=poco,9=molto)
Perdita di tracciabilità : è possibile sapere chi ha avuto accesso al dato o ne perdo le tracce (0=log completi,9=anonimo)
Danno economico : quanto è grave il danno economico venisse sfruttata questa vulnerabilità (0=basso,9=alto)
Danno di immagine : quanto è grave il danno di immagine (0=basso, 9=alto)
Non compliance : questa vulnerabilità quanto mi rende non compliance alle mie policy aziendali (0=poco,9=molto)
Violazione privacy : vi è violazione del dlgs 196/03 e della pricavy di utenti (0=nessuna,9=totale)

Rischio complessivo :

Rischio complessivo				
Impatto	**HIGH**	Medium	High	**Critical**
	MEDIUM	Low	Medium	High
	LOW	Information	Low	Medium
		LOW	**MEDIUM**	**HIGH**
	Probabilità			

Rischio complessivo = Probabilità * Impatto

VA TABLE

Rischio Complessivo	Descrizione	Ipotesi Soluzione
[High Risk] RV = 36.4	**Problematica rilevata: Modem in ingresso al numero 011-5550111 con password di default di sistema SAN EMC2 Pino1** Il server di gestione di una SAN EMC2 denominato 'Pino1' è chiamabile via modem telefonico dalla rete pubblica al numero 011-5550111 e permette l'accesso direttamente alla rete interna di Cliente su IP 172.16.1.1 con credenziali di default nasadmin/nasadmin e root/nasadmin. Da tale macchina si salta completamente tutta l'infrastruttura perimetrale di sicurezza posta di fronte ai collegamenti Internet e VPN MPLS con le sedi remote e i partner e si accede direttamente a tutta la rete interna, compresi i firewall, l'as/400 e altri sistemi critici.	Utilizzare una password complessa conforme alla policy generale sulle password o disabilitare in ingresso tale modem.

Minacce					**Vulnerabilità**			
Skill level inverso	Motivazione	Opportunità	Dimensione		Facilità di scoperta	Facilità da sfruttare	Diffusione	Tracciabilità
4	7	4	8		3	6	3	7
Probabilità complessiva = 5.2								
Impatti Tecnici					**Impatti di Business**			
Perdita di riservatezza	Perdita di integrità	Perdita di disponibilità	Perdita di tracciabilità		Danno economico	Danno di immagine	Non compliance	Violazione Privacy
8	8	8	7		8	4	8	5
Impatto complessivo = 7								

VA TABLE

[Medium Risk] RV = 26.1	**Problematica rilevata: Modem in ingresso al numero 011-5550222 e 011-5550333 (2400 bps) con password di default del PABX MD110 Ericsson** Il PABX MD110 Ericcson risponde a chiamate via modem dalla rete telefonica pubblica ai numeri 011-5550222 e 011-5550333 (quest'ultimo solo a 2400 bps) esponendo il suo sistema operativo di gestione NIUX (uno unix ridotto) con autenticazione data dalle credenziali di default del sistema (mduser/help). A questo punto è possibile effettuare ping e telnet verso la rete interna Cliente dall'IP 172.16.1.2 e riconfigurare alcuni paramteri del PABX (e scaricarne i LOG delle chiamate).	Utilizzare una password complessa conforme alla policy generale sulle password o disabilitare in ingresso tali modem.

Minacce					**Vulnerabilità**			
Skill level inverso	Motivazione	Opportunità	Dimensione		Facilità di scoperta	Facilità da sfruttare	Diffusione	Tracciabilità
2	7	4	8		3	3	3	6
Probabilità complessiva = 4.5								
Impatti Tecnici					**Impatti di Business**			
Perdita di riservatezza	Perdita di integrità	Perdità di disponibilità	Perdità di tracciabilità		Danno economico	Danno di immagine	Non compliance	Violazione Privacy
7	3	6	6		6	4	7	8
Impatto complessivo = 5.8								

VA TABLE

[Medium Risk] RV = 30.1	**Problematica rilevata: Mancanza del Log Accouting sul PABX MD110 per le chiamate in ingresso al sistema** Sul PABX MD110 non sono configurati i Log Accounting delle chiamate in ingresso, ma solo quelli delle chiamate in uscita. I Log in ingresso sono indispensabili per poter valutare fatti illeciti e per verificare accessi anomali via modem a sistemi interni (ad esempio monitorando i numeri dell'MD110 e delle SAN EMC2 come orari e frequenza di accesso via modem) o per diverse altre situazioni critiche.	Abilitare il Log Accounting anche per le chiamate entranti.

Minacce					**Vulnerabilità**			
Skill level inverso	Motivazione	Opportunità	Dimensione		Facilità di scoperta	Facilità da sfruttare	Diffusione	Tracciabilità
5	7	4	8		5	5	5	8
Probabilità complessiva = 5.8								
Impatti Tecnici					**Impatti di Business**			
Perdita di riservatezza	Perdita di integrità	Perdità di disponibilità	Perdità di tracciabilità		Danno economico	Danno di immagine	Non compliance	Violazione Privacy
5	7	2	8		7	4	7	2
Impatto complessivo = 5.2								