Assessment perimetrale ed applicativo (light)

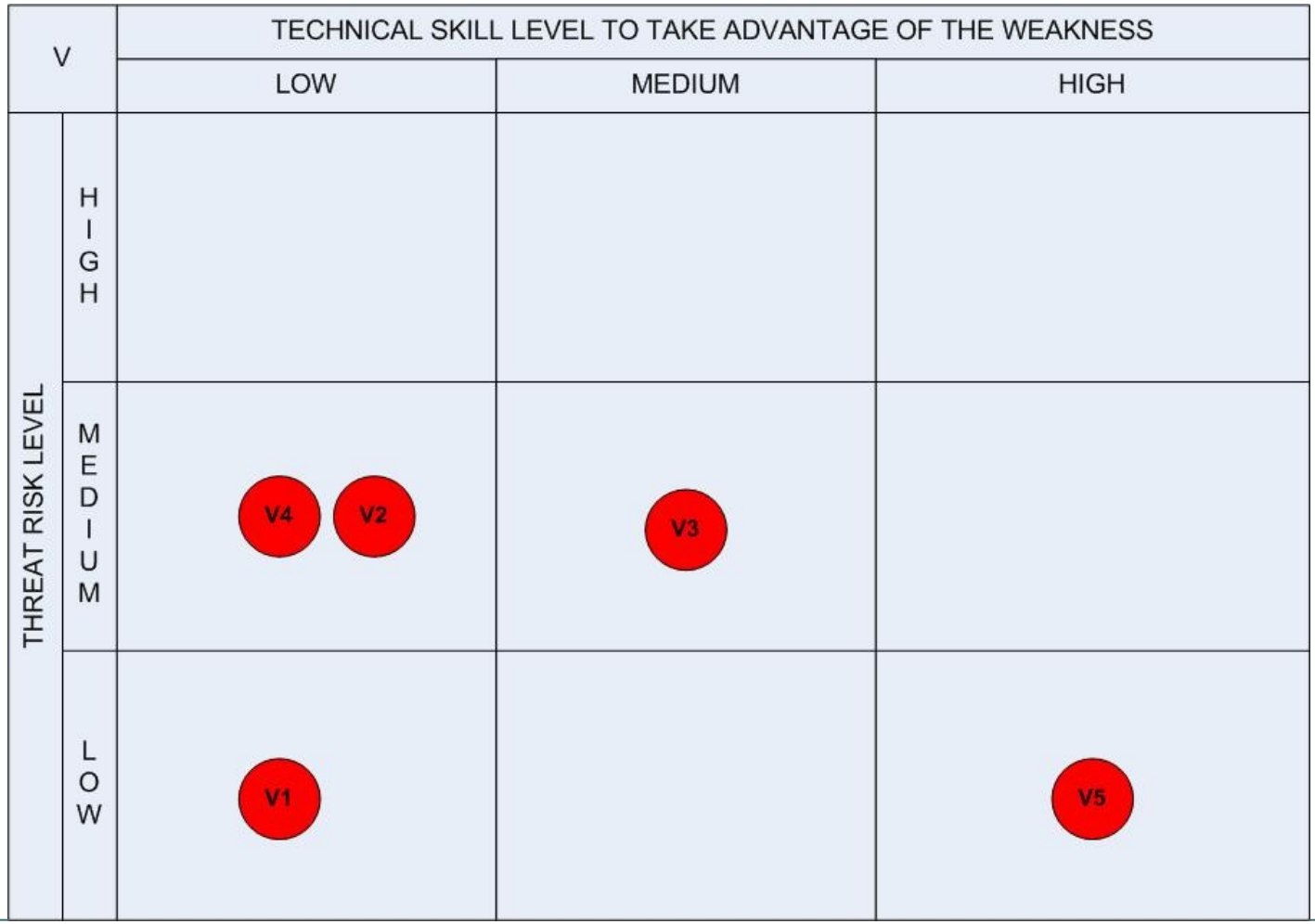
Studio della sicurezza del perimetro Internet ed applicazioni di

GM servizi

Attività svolte

- Esterna
  - Black-box
  - Sede Hacking Team

Classificazione vulnerabilità



Livello alto

- Nessuna vulnerabilità

Livello medio

- V2: DNS “open”
- V3: SQL injection
- V4: Source code disclosure

Livello basso

- V1: DNS zone transfer
- V5: Methodi HTTP Trace/track abilitati

Piano di fixing

N°	Tipo di vulnerabilità	Soluzione proposta
V1	DNS Zone Transfer	Modificare la configurazione del DNS per permettere le *zone transfer* solo ai DNS che effettivamente hanno necessità di tale operazione (ad es. i secondari)
V2	Open DNS	Modificare la configurazione del DNS server per limitare la risoluzione dei nomi Internet al più alle reti interne del Cliente.
V3	SQL Injection	Per eliminare la vulnerabilità è necessaria la riscrittura del codice di interfacciamento fra le pagine WEB e il database SQL. Come ulteriore soluzione è possibile l'inserimento di un *application firewall* a monte del *web server*. Le due soluzioni non sono mutuamente esclusive.
V4	Source Code Disclosure	Impostare correttamente i permessi di accesso ai file e rimuovere i file contenenti i sorgenti delle applicazioni non più utilizzate.
V5	Metodi TRACE e TRACK HTTP abilitati	Disabilitare i metodi TRACE e TRACK modificando i file di configurazione del Web Server

Action Plan

1. Fixing actions
2. Approfondire lo studio applicativo anche con code review
3. Firewall applicativo
4. Ottimizzazione dell'hardening
5. Sensibilizzazione programmatori o strumenti di check dei sorgenti