Esercizio M3

REPORT ESERCIZIO DI FINE MODULO

Rilevamento, analisi e correzione delle vulnerabilità

Elenco delle vulnerabilità critiche riscontrate		
Nome vulnerabilità	**CVE**	**Tipo | categoria**
NFS Exported Share Information Disclosure	CVE-1999-0170, CVE-1999-0211, CVE-1999-0554	Remote | RPC
Bind Shell Backdoor Detection	*N/A*	Remote | Backdoor
VNC Server 'password'	*N/A*	Remote | Shell remotely

Descrizione delle vulnerabilità

NFS Exported Share Information Disclosure: Questa vulnerabilità è causata da una scorretta implementazione del protocollo NFS e consentirebbe ad un utente malintenzionato di leggere e scrivere file sull'host, essa può essere sfruttata per ottenere informazioni sensibili, come nomi utente, password e dati aziendali, esse possono essere utilizzate per ulteriori attacchi o per compromettere l'integrità del sistema.

Bind Shell Backdoor Detection: Consente la creazione di una backdoor **senza autenticazione**, questo permette di collegarsi tramite i una porta remota ed inviare comandi alla shell.

VNC Server 'password' Password: Essa è causata da un inadeguato livello di sicurezza che non richiedere l'accesso tramite un sistema di autenticazione sicuro, ma semplicemente autenticandosi usando "password", essa è molto pericolosa poiché può essere sfruttata per prendere il controllo del sistema.

Correzione delle vulnerabilità

NFS Exported Share Information Disclosure: Questa vulnerabilità è stata risolta restringendo la possibilità di usare il servizio ai soli host e indirizzi autorizzati, impostando le configurazioni `/etc/hosts.allow` e `/hosts.deny`.

Bind Shell Backdoor Detection: La vulnerabilità in questione è stata corretta attivando il firewall e impostarlo in modo che blocchi la porta *1524*, essa poteva essere sfruttata per la vulnerabilità di sicurezza in questione.

VNC Server 'password' Password: La vulnerabilità in questione era causata da un inefficiente richiesta di autenticazione, per correggere tale vulnerabilità è stato necessario impostare un obbligo di autenticazione per usare il servizio in questione tramite l'inserimento di due password sicure e separate: una per l'utilizzo del servizio in modo completo e l'atra per autenticarsi come *viewer*.

Report finale

Vulnerabilità	Gravità | CVSS	Stato
NFS Exported Share Information Disclosure	Critical | 10.0	Risolto
Bind Shell Backdoor Detection	Critical | 9.8	Risolto
VNC Server 'password' Password	Critical | 10.0	Risolto

Consigli di sicurezza futuri

Punti per una migliore sicurezza

1. Aggiornare periodicamente i sistemi con le più recenti patch di sicurezza
2. Impostare password sicure, cambiarle periodicamente e conservarle in modo sicuro (es. gestore di password)
3. Effettuare periodicamente scansioni di sicurezza e di ricerca delle vulnerabilità