UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

unimc

Studio sulla vulnerabilità della rete della Prefettura di Perugia

Stefano Franceschini

Dipartimento d'Ingegneria dell'Informazione
Università Politecnica delle Marche
S1127000@studenti.univpm.it

Sabato 11 ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Introduzione

Cybersecurity

- Confidenzialità
- Integrità
- Disponibilità
- Motivazioni e metodologia
- Dati sugli attacchi

Vulnerability assessment e Penetration Testing

- Definizioni
- Metodologia
- Tecniche e strategie
- Funzionamento del processo di VA

Quadro attuale della rete e degli applicativi delle Prefettura di Perugia

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Quadro attuale della rete e degli applicativi delle Prefettura di Perugia

- 2 reti lan con due indirizzi ip diversi con collegamento al Ministero dell'Interno tramite un server di routing
- Al ced del ministero tutte le operazioni sono filtrate da batterie di firewall
- Cloud dati su PSN (piano strategico nazionale) infrastruttura per la PA
- Navigazione internet con accesso tramite sistemi gestiti dal ced del Ministero (limitato)
- Procedure gestionali centralizzate e locali

Principi e metodologia applicata

Principi e metodologia applicata (VA)

- Analisi delle conoscenze di sicurezza del personale
- Controllato lo stato delle postazione con SCCM
- Identificate le vulnerabilità e Classificate
- Valutate le vulnerabilità
- Stabilito una periodicità dei controlli e delle procedure di mantenimento dello status raggiunto

Principi e metodologia applicata (PT)

- Raccolta delle informazioni
- Simulazione di un attacco sulla rete con software open
- Exploitation
- Valutazione delle vulnerabilità rilevate e definizione del possibile sfruttamento
- Frequenza bassa di rilevazioni e pianificazioni
- Report per ulteriori verifiche

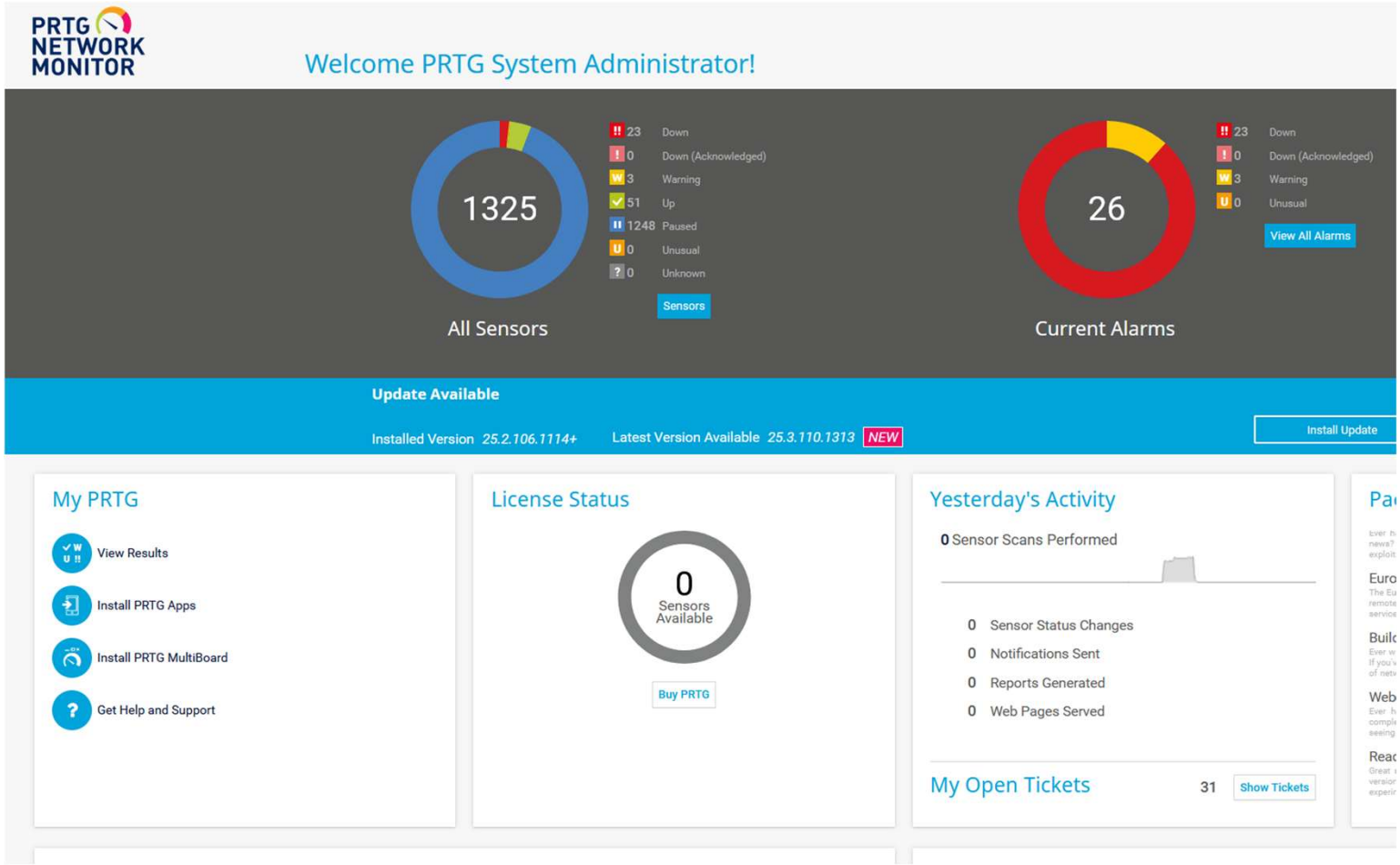
Valutazione dello stato di sicurezza della rete, della intranet e delle macchine virtuali

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

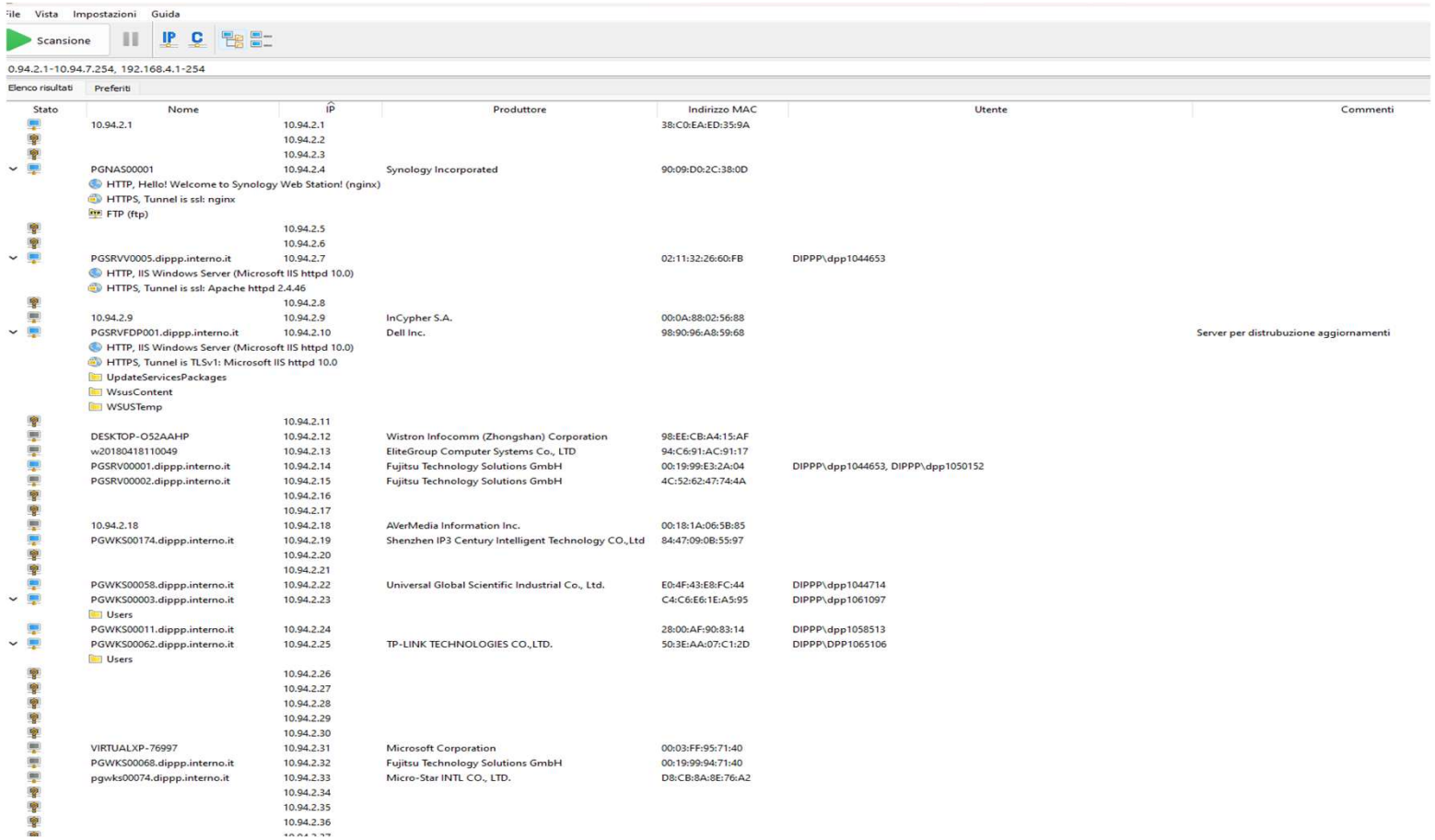
Processo iniziale di VA

- Scansione rete utilizzando
- Lansweeper
- PRTG Network monitor
- Advanced IP scanner
- Ulteriore indagine ed analisi con SCCM
- Nmap e Owasp zap
- Bonifica delle postazioni e standardizzazione

Processo iniziale di VA



Processo iniziale di VA



File Vista Impostazioni Guida

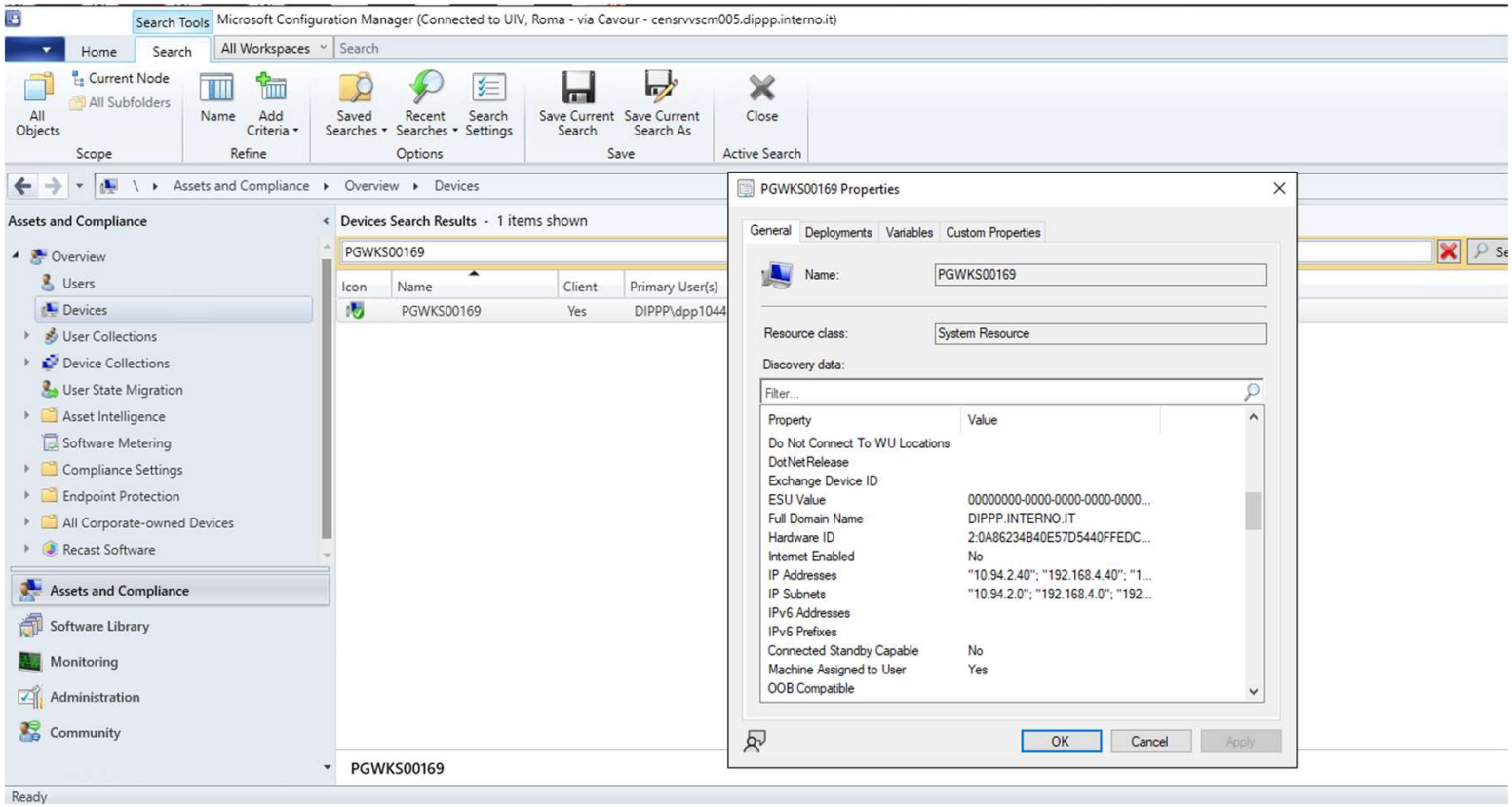
Scansione

0.94.2.1-10.94.7.254, 192.168.4.1-254

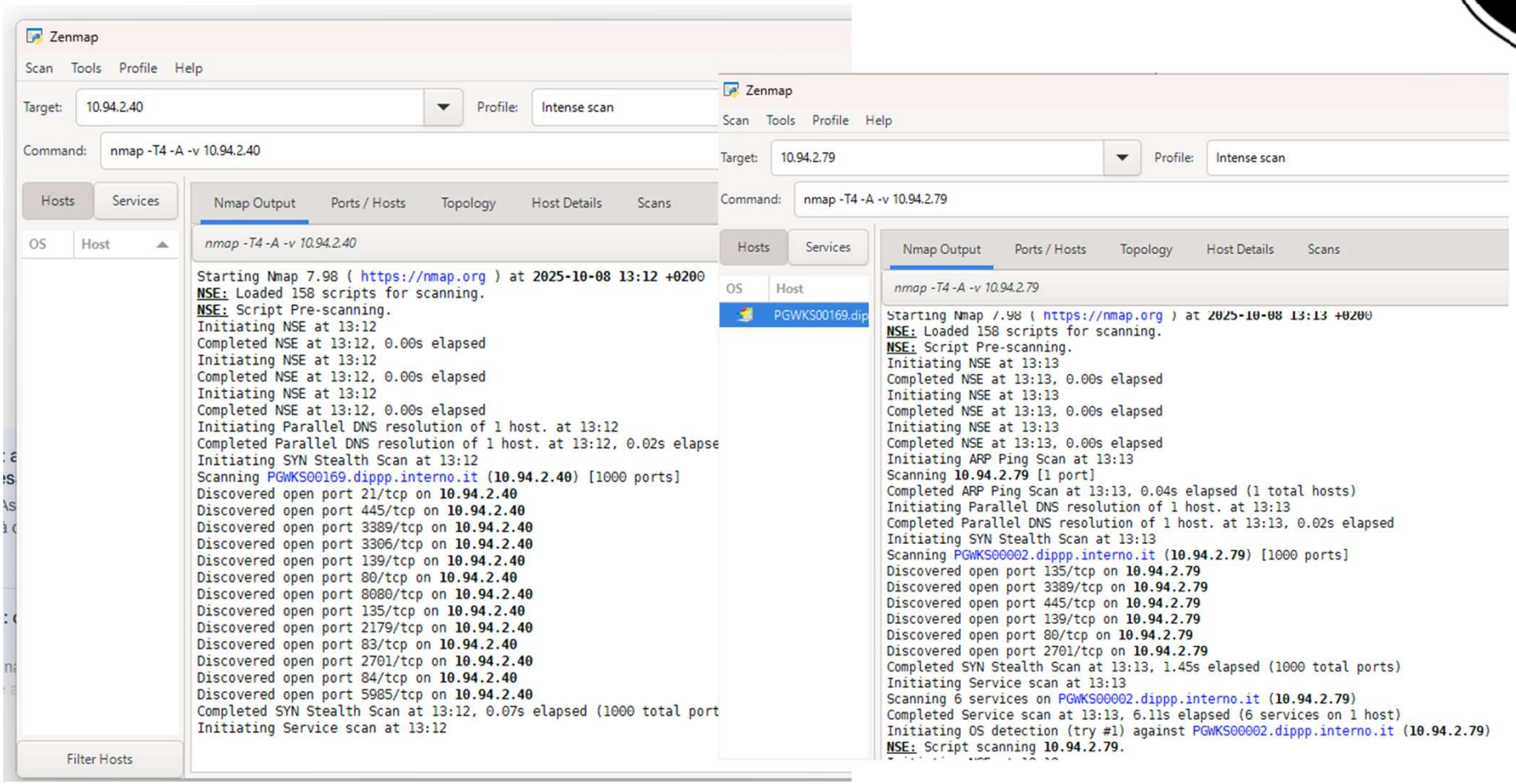
Elenco risultati | Preferiti

Stato	Nome	IP	Produttore	Indirizzo MAC	Utente	Commenti
	10.94.2.1	10.94.2.1		38:C0:EA:ED:35:9A		
		10.94.2.2				
		10.94.2.3				
	PGNAS00001	10.94.2.4	Synology Incorporated	90:09:D0:2C:38:0D		
	HTTP, Hello! Welcome to Synology Web Station! (nginx)					
	HTTPS, Tunnel is ssl: nginx					
	FTP (ftp)					
		10.94.2.5				
		10.94.2.6				
	PGSRVV0005.dippp.interno.it	10.94.2.7		02:11:32:26:60:FB	DIPPP\dpp1044653	
	HTTP, IIS Windows Server (Microsoft IIS httpd 10.0)					
	HTTPS, Tunnel is ssl: Apache httpd 2.4.46					
		10.94.2.8				
	10.94.2.9	10.94.2.9	InCypher S.A.	00:0A:88:02:56:88		
	PGSRVFDP001.dippp.interno.it	10.94.2.10	Dell Inc.	98:90:96:A8:59:68		Server per distrubuzione aggiornamenti
	HTTP, IIS Windows Server (Microsoft IIS httpd 10.0)					
	HTTPS, Tunnel is TLSv1: Microsoft IIS httpd 10.0					
	UpdateServicesPackages					
	WsusContent					
	WSUSTemp					
		10.94.2.11				
	DESKTOP-O52AAHP	10.94.2.12	Wistron Infocomm (Zhongshan) Corporation	98:EE:CB:A4:15:AF		
	w20180418110049	10.94.2.13	EliteGroup Computer Systems Co., LTD	94:C6:91:AC:91:17		
	PGSRV00001.dippp.interno.it	10.94.2.14	Fujitsu Technology Solutions GmbH	00:19:99:E3:2A:04	DIPPP\dpp1044653, DIPPP\dpp1050152	
	PGSRV00002.dippp.interno.it	10.94.2.15	Fujitsu Technology Solutions GmbH	4C:52:62:47:74:4A		
		10.94.2.16				
		10.94.2.17				
	10.94.2.18	10.94.2.18	AVerMedia Information Inc.	00:18:1A:06:5B:85		
	PGWKS00174.dippp.interno.it	10.94.2.19	Shenzhen IP3 Century Intelligent Technology CO.,Ltd	84:47:09:0B:55:97		
		10.94.2.20				
		10.94.2.21				
	PGWKS00058.dippp.interno.it	10.94.2.22	Universal Global Scientific Industrial Co., Ltd.	E0:4F:43:E8:FC:44	DIPPP\dpp1044714	
	PGWKS00003.dippp.interno.it	10.94.2.23		C4:C6:E6:1E:A5:95	DIPPP\dpp1061097	
	Users					
	PGWKS00011.dippp.interno.it	10.94.2.24		28:00:AF:90:83:14	DIPPP\dpp1058513	
	PGWKS00062.dippp.interno.it	10.94.2.25	TP-LINK TECHNOLOGIES CO.,LTD.	50:3E:AA:07:C1:2D	DIPPP\DPP1065106	
	Users					
		10.94.2.26				
		10.94.2.27				
		10.94.2.28				
		10.94.2.29				
		10.94.2.30				
	VIRTUALXP-76997	10.94.2.31	Microsoft Corporation	00:03:FF:95:71:40		
	PGWKS00068.dippp.interno.it	10.94.2.32	Fujitsu Technology Solutions GmbH	00:19:99:94:71:40		
	pgwks00074.dippp.interno.it	10.94.2.33	Micro-Star INTL CO., LTD.	D8:CB:8A:8E:76:A2		
		10.94.2.34				
		10.94.2.35				
		10.94.2.36				

Processo iniziale di VA



Processo iniziale di VA



Prova di riduzione del rischio

Scansione delle vulnerabilità

- Inventario dei dispositivi
  scansionati 6 server
  2 NAS
  2 Server virtuali
  140 Personal Computer (postazioni)
  1 intranet wordpress e procedure su nas
- Controllo del database delle vulnerabilità
- Creazione di un elenco delle vulnerabilità
- Valutazione della conformità dei dispositivi

Scansione delle vulnerabilità

- Controllo database delle vulnerabilità

  Common Vulnerability an Exposure (CVE)

  National Vulnerability Database (NVD)

  Exploit Database

  O-Day Today

Scansione delle vulnerabilità

- Elenco delle vulnerabilità

  - Software obsoleto
    (patch sicurezza assenti – configurazioni errate)
  - Firewall con impostazioni sbagliate
  - Problemi alle credenziali di accesso
  - Backdoor software rilevato
  - Scarso monitoraggio

Scansione delle vulnerabilità

- Valutazione della conformità dei dispositivi
  - Certificazione del cablaggio
  - Controllo dei dispositive attivi (switch – hub)
  - Ulteriore esecuzione di test VA e PT

Prova di penetrazione (Test)

Prova di penetrazione (Test)

- Scansione delle porte
  - Utilizzando strumenti di port scanning sono state individuate molte porte aperte
  - Controllate e rilevate falle sulle configurazioni
  - Password facilmente individuabili e ripetitive
  - Politiche di sicurezza assenti o errate

Prova di penetrazione (Test)

- Sniffer

  analizzato il traffico di dati della rete,in alcuni casi risulta criptato quindi con meno informazioni recuperabili.

- Generatori di pacchetti

  utilizzando tali strumenti si è simulato il traffico di dati di rete, in questo modo, si è imitato il traffico di dati reale.

- Password cracking

  con la violazione delle password si è tentato di rubare password che si sono verificate insicure.

Identificazione delle vulnerabilità

Credenziali deboli o crackabili

- Molte persone non riescono a creare password forti e uniche per ciascuno dei loro account.
- Ricorrendo a cattive abitudini in materia di password, come il riutilizzo delle stesse password su più account e la creazione di password deboli e facili da ricordare.
- I cybercriminali sfruttano le credenziali di accesso deboli e lanciano attacchi informatici come gli attacchi di brute force che mirano a rubare queste.

Configurazioni errate

- Le configurazioni errate del sistema avvengono quando le risorse di rete hanno impostazioni vulnerabili o controlli di sicurezza disparati.
- I sistemi che richiedono la configurazione manuale possono presentare errori e lacune se configurati in modo improprio.
- I cybercriminali cercano queste configurazioni errate per sfruttare e ottenere l'accesso non autorizzato.

Software obsoleto

- I cybercriminali cercano eventuali bug o falle all'interno del software, sfruttando queste falle per ottenere l'accesso non autorizzato e rubare eventuali dati sensibili.
- L'aggiornamento regolare del software corregge la maggior parte delle falle o dei bug, in particolare le vulnerabilità note.
- Utilizzando un software obsoleto, si è suscettibili alle minacce informatiche e al furto dei dati.
- es. 7zip vulnerabile scoperto da poco

Accessi non autorizzati

- Sono stati riscontrati alcuni dipendenti con l'accesso privilegiato alle risorse necessarie per svolgere il loro lavoro.
- Sono stati forniti accidentalmente ad alcuni dipendenti accessi e autorizzazioni maggiori, (accesso come amministratori della macchina), subito sanificate.
- Questo può creare rischi per la sicurezza se un dipendente abusa di queste autorizzazioni o il suo account viene compromesso da un malintenzionato.

Report e conclusioni

Report e conclusioni

- Dopo aver svolto test di VA e PT siamo coscienti dei problemi che possono verificarsi all'interno della rete
- Predisposizione di un piano di rimedio e azioni correttive necessarie
- Monitoraggio costante
- Corsi di sensibilizzazione per il personale
- Le debolezze della rete devono diventare punti di forza anche se molti rischi sono evitati perché qualsiasi operazione è filtrata dalle rete centrale del Ministero dell'Interno

Ringraziamenti

- Grazie per l’attenzione