14/10/2025

Il Tuo Guardiano Digitale

CEO: Samuele Barba/ Tegege Fael/Lorenzo Mantoni/Cosimo Chincoli/ Antonio Gangale/ Emanuele Di Leva

CERBERUS S. P. A.

CERBERUS

CERBERUS è il partner strategico per la progettazione, implementazione e gestione di infrastrutture di rete aziendali e private.
Ispirato al leggendario custode a tre teste, la nostra missione si fonda su tre pilastri essenziali:

1. **Proteggere:** Difendiamo reti e dati con cybersecurity avanzata (firewall, IDS, VPN) da ogni minaccia interna ed esterna.
2. **Connettere:** Realizziamo architetture di rete resilienti per una connettività stabile, veloce e continua tra sedi, personale remoto e servizi cloud.
3. **Controllare:** Monitoriamo proattivamente le prestazioni per garantire massima efficienza operativa, stabilità e la rigorosa conformità agli standard.

Offriamo soluzioni integrate che uniscono infrastruttura robusta e sicurezza avanzata, agendo come il custode completo del tuo ecosistema IT.

RAPPORTO DETTAGLIATO PER THETA S.R.L

L'azienda Cerebrus è stata incaricata da Theta di progettare, la loro rete aziendale;

- Progettazione logica di una rete su 6 piani, con 120 host totali.
- Integrazione di componenti critici: Firewall perimetrale, Web Server (DVWA), NAS e sistemi IDS/IPS.
- Testing della sicurezza attraverso la scrittura di tool custom in Python.
- Esecuzione di attività: subnetting della rete e creazione di uno sniffer di pacchetti.

2. Progettazione dell'Infrastruttura di Rete

2.1 Schema Logico di Rete

È stato progettato il seguente schema a livelli:
1. Rete Interna:
   - Piani 1-6: Ogni piano è dotato di uno switch di layer 2 che collega 20 computer.
   - Uno switch centrale, collegato sia a tutti gli switch e al router, Progettato in modo da non interrompere le connessioni, in caso di guasto dello switch centrale.
   - Router
   - NAS: Collegato allo switch del Centrale per un accesso centralizzato e performante ai dati.

2. **Perimetro di Sicurezza (DMZ)**
   - Firewall Perimetrale: Posizionato tra il router interno e Internet. Definisce le regole di filtrazione del traffico.
   - Zona Demilitarizzata (DMZ): Collocata tra il firewall e Internet, ospita il Web Server (Metasploitable2 - DVWA)
   - Il firewall è configurato per inoltrare solo il traffico web (porte 80/443) verso questo server, isolandolo dalla rete interna.

2. Progettazione dell'Infrastruttura di Rete

2.1 Schema Logico di Rete

È stato progettato il seguente schema a livelli:

1. Rete Interna:
   - Piani 1-6: Ogni piano è dotato di uno switch di layer 2 che collega 20 computer.
   - Uno switch centrale, collegato sia a tutti gli switch e al router,
   - Router
   - **NAS**: Abbiamo scelto di collegarlo allo **switch centrale** per garantire **prestazioni migliori** e una **comunicazione più efficiente** tra le diverse VLAN.
     Questa posizione centrale assicura che tutti i dispositivi autorizzati possano accedere al NAS in modo rapido, indipendentemente dalla loro rete di appartenenza.
     - Inoltre, questa scelta facilita il **monitoraggio del traffico** verso il NAS, grazie alla centralizzazione del punto di accesso. In caso di malfunzionamenti o **interruzioni in una delle VLAN**, il collegamento al core switch consente al NAS di rimanere comunque **disponibile** per le altre reti, migliorando l'affidabilità complessiva dell'infrastruttura.
2. **Perimetro di Sicurezza (DMZ)**
   - **Firewall** Perimetrale: Posizionato tra il router interno e Internet. Definisce le regole di filtrazione del traffico.
   - Zona Demilitarizzata (DMZ): Collocata tra il firewall e Internet, ospita il Web Server (**Metasploitable2** - DVWA)
   - Il firewall è configurato per inoltrare solo il traffico web (porte 80/443) verso questo server, isolandolo dalla rete interna.

3. **Sistemi di Monitoraggio**

IDS/IPS: Tre sensori sono stati posizionati strategicamente:

- Collegati tra le 3 reti in modo da proteggere eventuali attacchi,
  Con questo metodo preveniamo anche il tentato attacco di altre vlan tramite un exploit
  (es. DHCP spoofing, ARP poisoning, vulnerabilità Layer 2)

Rete Interna Aziendale: 192.168.0.0/17

- PC/P1: **"192.168.10.1/24"**
- PC/P2: **"192.168.20.1/24"**
- PC/P3: **"192.168.30.1/24"**
- PC/P4: **"192.168.40.1/24"**
- PC/P5: **"192.168.50.1/24"**
- PC/P6: **"192.168.60.1/24"**

Virtualizzazione/Simulazione PKT

Introduzione e Contesto Progettuale

Questa relazione descrive la configurazione firewall **pfSense** implementata nell'ambito di una simulazione **Packet Tracer**, commissionata per proteggere l'infrastruttura di rete aziendale. Il firewall è stato posizionato strategicamente per separare la rete interna dalle connessioni Internet, garantendo sicurezza senza compromettere la funzionalità dei servizi. In questa virtualizzazione l'indirizzo IP **192.168.50.10** rappresenta i pc utilizzati nel modello. Il firewall proteggerà OPT1 che corrisponde al server rappresentato nel progetto.

Obiettivi della Configurazione

Protezione dalla Rete ESTERNA (OPT1)

- Blocco attacchi **brute-force** su servizi esposti
- Limitazione accessi non autorizzati dalla rete pubblica
- Protezione servizi critici dall'esposizione indiscriminata

Gestione Accessi dalla Rete INTERNA (192.168.50.0/24)

- Accesso privilegiato per amministrazione
- Comunicazioni controllate verso l'esterno
- Separazione logica tra reti interne ed esterne

Analisi Dettagliata delle Regole Implementate

1. Regola DNS - Permesso Condizionato

Motivazione: Consente la risoluzione **DNS** verso server esterni, essenziale per il funzionamento di applicazioni e servizi che necessitano di risoluzione nomi.

2. Accesso SSH Amministrativo - Controllo Rigido

Motivazione: Permette esclusivamente ai pc autorizzati di stabilire connessioni SSH verso l'esterno. Previene accessi **SSH** non autorizzati dalla rete interna.

3. Redirect HTTP a HTTPS - Security Enforcement

Strategia: Redirect automatico a **HTTPS** per forzare comunicazioni cifrate e proteggere dati sensibili in transito. Regola essenziale per fare in modo che tutti i dati, possano viaggiare in maniera sicura diminuendo drasticamente la fuga di dati sensibili. Migliora l'esperienza utente facendo in modo che il processo di passaggio alla porta più sicura avvenga automaticamente.

4. Accesso HTTPS Pubblico - Servizi Web

Motivazione: Si ricollega alla regola tre aprendo una porta che favorisce la crittografia dei dati e garantendo la **privacy** e la sicurezza di essi.
Una procedura ormai standardizzata per la maggioranza dei servizi web.

5. Blocco Servizi ad Alto Rischio

Analisi Rischio:

• SSH/Telnet (22-23): Vettori comuni per brute-force
• RPC (135): Storicamente vulnerabile a **exploit**
• SMB (445): Target frequente per ransomware
• RDP (3389): Attacchi **brute-force**

Queste sono tra le porte più "**famose**" per essere vulnerabili perché non garantiscono la crittografia dei dati e non hanno sistemi di sicurezza. Sono spesso tra le prime che vengono prese di mira quando avviene un attacco **hacker**, è di estrema importanza chiuderle perché si rischierebbe una fuga di dati oltre che un grande danno d'immagine per l'azienda verso i propri clienti.

6. Limitazione Protocollo ICMP

Motivazione: Riduce la visibilità di rete attraverso scanner automatici limitando il "ping"

- Nessun mapping della rete da parte di estranei
- Protezione da attacchi di saturazione (come attacchi **DDoS)**
- Maggiore **privacy** della struttura interna

7. Accesso Privilegiato Completo

Amministrazione: Concede accesso completo ai pc autorizzati

8. Blocco Reti Private Non Autorizzato

Motivazione: Si ricollega alla regola 7 bloccando tutti gli indirizzi IP non autorizzati nella rete interna.
Previene il rischio di attacchi interni e accessi non autorizzati.

DISTRIBUZIONE SOFTWARE E PC

1° PIANO - WLAN 10

Dipartimento: Segreteria e Assistenza Clienti

- 20 PC - Preventivo: $5.000
- Software: Suite Office, CRM clienti, telefono VoIP
- Specifiche: Configurazione base per attività amministrative

2° PIANO - WLAN 20

Dipartimento: Produzione e Logistica

- 20 PC - Preventivo: $10.000
- Software: ERP produzione, gestione magazzino, tracciamento ordini
- Specifiche: Workstation robuste per gestione operativa

3° PIANO - WLAN 30

Dipartimento: Sicurezza Informatica e Developer

- 20 PC - Preventivo: $24.000
- Software: IDE sviluppo, tool sicurezza, monitoraggio rete, testing
- Specifiche: High-performance per sviluppo e sicurezza

4° PIANO - WLAN 40

Dipartimento: Reparto Grafico

- 20 PC - Preventivo: $26.000
- Schede Grafiche: NVIDIA RTX 3080 (20 unità × $400 = $8.000)
- Software: Suite Adobe Creative Cloud, AutoCAD, rendering 3D
- Specifiche: Workstation grafiche professionali

5° PIANO - WLAN 50

Dipartimento: Marketing

- 20 PC - Preventivo: $15.000
- Software: Analytics, social media management, graphic design base
- Specifiche: Configurazione media per attività marketing

6° PIANO - WLAN 60

- Dipartimento: Dirigenza
- 20 PC - Preventivo: $30.000
- Software: Business intelligence, dashboard direzionali, videoconferenza
- Specifiche: Workstation premium per decision-making
- Pc Mac

Distinte base (BOM)

Switch

- 6× switch accesso 24 porte 1G con 2× uplink SFP+ 10G → €650 cad. = €3.900
- 1× switch core 24p 10G (mix SFP+/RJ-45, stacking pronto) → €3.000

Edge / sicurezza

- 1× Router WAN/edge (rack) → €1.200
- 1× Firewall dedicato (classe “ASA” mid-range, HA non incluso) → €2.500
- 2× IDS/IPS dedicati (inline/span) → €1.500 cad. = €3.000

Server & storage

- 2× server rack (CPU moderna, 32–64 GB, RAID, 2× PSU) → €2.000 cad. = €4.000
- 1× NAS 16 TB RAW (RAID, 2× NIC) → €1.200

Racks & energia

- 1× rack 42U chiuso + accessori → €800
- Patch panel Cat6A: 12×24p → €50 cad. = €600
- Cable management, guide, mensole → €300
- 2× PDU → €200
- 2× UPS 2 kVA (rack) → €700 cad. = €1.400

Backbone fibra & transceiver

- SFP+ 10G: 12 pz → €80 cad. = €960
- BHS OM4/OS2 (trunk/patch, bretelle, cassettini) → €1.200

Rame orizzontale

- Cavo Cat6A LSZH: ~4.200 m (120 prese × media 35 m) → €0,35/m = €1.470
- 120× keystone RJ45 + placche + box → €5 cad. = €600
- Patch cord armadio (120) + lato utente (120) → €3 cad. = €720
- Etichette + certificazione basic → €200

SUB-TOTALE HARDWARE/MATERIALI: €27.350

Manodopera

Cabling & posa (2 tecnici)

- 120 tratte rame (posa, crimpature, test), dorsali fibra, rack & ordine: ~186 h
- Tariffa media tecnico: €70/h → €26400

Ingegneria di rete

- Design L2/L3 (VLAN, STP/RSTP, routing), sicurezza (ACL, NAT, rules FW/IDS), QoS, logging, backup config, collaudo, documentazione: 56 h
- Tariffa network engineer: €150/h → €8400

Project management

- Coordinamento, SAL, handover: 12 h × 150 → €1800

SUB-TOTALE MANODOPERA: €13.350

Extra, imprevisti e formazione

- Trasferte/piccoli consumabili: €1.000
- Breve formazione/hand-over (2–3 h + manuali PDF): €1.000
- Contingency 10% su materiali manodopera: €4.070

Totali

- Materiali: €27.350 + IVA 22%
- Manodopera: €36.627 + IVA 22%
- TOTALE PER LA RETE: €85.000 + IVA 22%
- PC: € 85.800 + IVA 22%
- TRASPORTO €5000 + IVA 22%
- LICENZE SOFTWARE: 30.000 primo anno
- TOTALE FINALE: €230.000 IVA inclusa.

Cronoprogramma

Sopralluogo & esecutivo (0.5–1 gg)
Racks, posa cavi rame/fibra, patch panel (5–6 gg, 2 tecnici)
Montaggio apparati & cablaggio armadi (1 gg)
Configurazione rete & sicurezza (2–3 gg)
Collaudo, documentazione, formazione (0.5–1 gg)

Premesse e Vincoli Progettuali

- Impianto elettrico e locali tecnici già pronti (messa a terra, climatizzazione, canaline agibili).
- Niente Wi-Fi/AP (non presenti nel disegno).
- Nessuna ridondanza in HA (firewall singolo, core singolo).
- Cat6A per l'orizzontale, 10G fiber uplink (dorsale) tra access e core.
- 24 porte per piano bastano (20 client + margine); se vuoi margine forte, passiamo a 48p.
- Percorsi cavi "normali" (senza lavori edili).
- Server: specifiche standard; se servono VM/servizi critici, possiamo dimensionare

Sicurezza e Conformità (+15–30%):

- NAC/802.1X: Controllo degli Accessi alla Rete e autenticazione port-based.
- Syslog/SIEM: Gestione dei log e sistema di gestione delle informazioni e degli eventi di sicurezza.
- Segmentazione Zero-Trust: Architettura di rete che applica il principio "mai fidarsi, verificare sempre".
- Hardening Avanzato: Rafforzamento della sicurezza di sistemi e applicazioni tramite configurazioni specifiche.
- Runbook: Documentazione procedurale per la risposta a eventi o per operazioni standardizzate.

Script per la verifica dei verbi http

Questo script è uno scanner di verbi **HTTP**, uno strumento di base per l'analisi della sicurezza di un server web, il suo obiettivo è scoprire quali metodi **HTTP** (come **GET**, **POST**, **PUT**, **DELETE**) sono permessi su una specifica risorsa (**URL**).

Analisi:

La funzione di test "test_http_verb" per ogni verbo **HTTP** che le viene passato: usa la libreria requests per inviare una richiesta **HTTP** al server con il metodo specificato, controlla la risposta analizzando il codice di stato restituito dal server e identifica il pericolo, inoltre segnala un'allerta se il server risponde con "**200 OK**" (operazione riuscita) ad una richiesta **PUT** o **DELETE**, indicando una grave vulnerabilità.

Il ciclo principale **if __name__==’__main__’** gestisce l'interazione con l'utente e orchestra i test:

Chiede il target: domanda all'utente l'IP/dominio del server e il percorso della risorsa da testare.

Esegue i test in serie: avvia un ciclo for che scorre la lista dei verbi **[‘GET’, ‘POST’, ‘PUT’, ‘DELETE’].**

Chiama la funzione: per ogni verbo chiama la funzione test_http_verb per eseguire il test effettivo.

Funzione e scopo

Lo scopo non è solo vedere quali metodi funzionano, ma identificare una configurazione debole e potenzialmente pericolosa:

PUT: permette di caricare o sostituire un file sul server.

DELETE: permette di cancellare un file sul server.

Se il server accettasse queste richieste da chiunque, un malintenzionato potrebbe modificare o cancellare il contenuto del sito web.

Conclusioni

Lo script automatizza il processo di invio di diverse richieste **HTTP** e **URL** per verificare se metodi potenzialmente dannosi come **PUT** e **DELETE** sono stati lasciati aperti per errore.

Introduzione Sniffer

Lo script, “SnifferLogin.py” è progettata con uno scopo molto più specifico: intercettare e analizzare il traffico HTTP non crittografato alla ricerca di potenziali credenziali di accesso.

Analisi

sniff (filter=**’tcp** port 80’), questo potente filtro da istruzioni a **scapy** di catturare soltanto i pacchetti che viaggiano sul protocollo TCP e utilizzano la porta 80, standard universale HTTP.
La funzione di **callback**, verifica che il pacchetto contenga un livello **raw**, questo livello rappresenta i dati grezzi dell’applicazione, ovvero il contenuto effettivo della comunicazione (in questo caso i dati di una richiesta HTTP).
Successivamente estrae i dati grezzi (che sono in formato bit) e tenta di decodificarli in una stringa di testo “UTF-8”, **errors=’ignore’** previene gli errori nel caso in cui i dati non siano testo valido.
Lo script definisce una lista di keywords (come ‘user’, ‘pass’, ‘password’, etc.) solitamente usate nei moduli di login e controlla se una qualsiasi di queste parole chiave è presente nel payload, se viene trovata una corrispondenza, lo script segnala la scoperta e stampa l’intero payload, che potrebbe contenere le credenziali in chiaro.

Funzionamento e scopo

Questo sniffer evoluto non è più solo uno strumento di monitoraggio, ma un vero e proprio strumento di analisi della sicurezza, il cui scopo è dimostrare in modo pratico e allarmante i pericoli della trasmissione di informazioni sensibili su connessioni **HTTP** non crittografate.
Qualsiasi dato inviato tramite un modulo di login su un sito web “**http**://” può essere intercettato da uno strumento come questo, esponendo nomi utente e password in chiaro a chiunque si trovi sulla stessa rete locale (ad esempio una rete wi-fi pubblica).

Conclusioni

Questo script serve quindi come un potente promemoria dell’importanza fondamentale del protocollo **HTTPS**, che cripta i dati tra il browser e il **server**, rendendo questo tipo di sniffing completamente inefficace e proteggendo la privacy e la sicurezza degli utenti.

Il gruppo **CERBERUS** ha consegnato con successo un progetto completo per theta, che include:

1. Una progettazione di rete dettagliata e sicura, scalabile e con una chiara strategia di indirizzamento.
2. La simulazione e il testing dell'infrastruttura attraverso tool personalizzati in Python, che hanno dimostrato capacità proattive di analisi e sicurezza.
3. L'identificazione di punti di forza (configurazione corretta dei verbi **HTTP** su phpMyAdmin) e debolezze critiche (numerosi servizi obsoleti ed esposti sul web server).

Raccomandazioni Principali per theta
-Hardening del Server: Disabilitare immediatamente i servizi non essenziali (Telnet, FTP anonimo) sulla macchina pubblica.
-Patching e Aggiornamento: Mantenere tutti i software (specialmente WordPress, phpMyAdmin) aggiornati all'ultima versione per mitigare vulnerabilità note.
-Regole Firewall Strette: Implementare regole sul firewall perimetrale che consentano solo il traffico strettamente necessario verso la DMZ (es. solo porta 80/443).
-Monitoraggio Continuo: Utilizzare gli IDS/IPS e tool di sniffing per un monitoraggio continuo e proattivo della rete.

Il gruppo CERBERUS si dichiara a disposizione per eventuali fasi successive di implementazione o auditing.

CEO: **SAMUELE BARBA**

Firma, *SamueleBarba*

Il Team **CERBERUS S. P. A.**

CISO (Responsabile Sicurezza Informatica) **Tegege Fael**

CTO (Direttore Tecnico) **Lorenzo Mantoni**

COO (Direttore Operativo) **Cosimo Chincoli**

CFO (Direttore Finanziario) **Antonio Gangale**

Responsabile Vendite & Marketing **Emanuele Di Leva**