THETA PROJECT

BUILD WEEK 1
CS0424IT

SECURE
SENTINELS

Table Of Contents

NETWORK DESIGN

OBIETTIVI DI SICUREZZA

- Confidenzialità
- Integrità
- Disponibilità

DMZ (De-Militarized Zone)

Regione separata dal resto della rete interna per minimizzare il rischio di accesso non autorizzato.

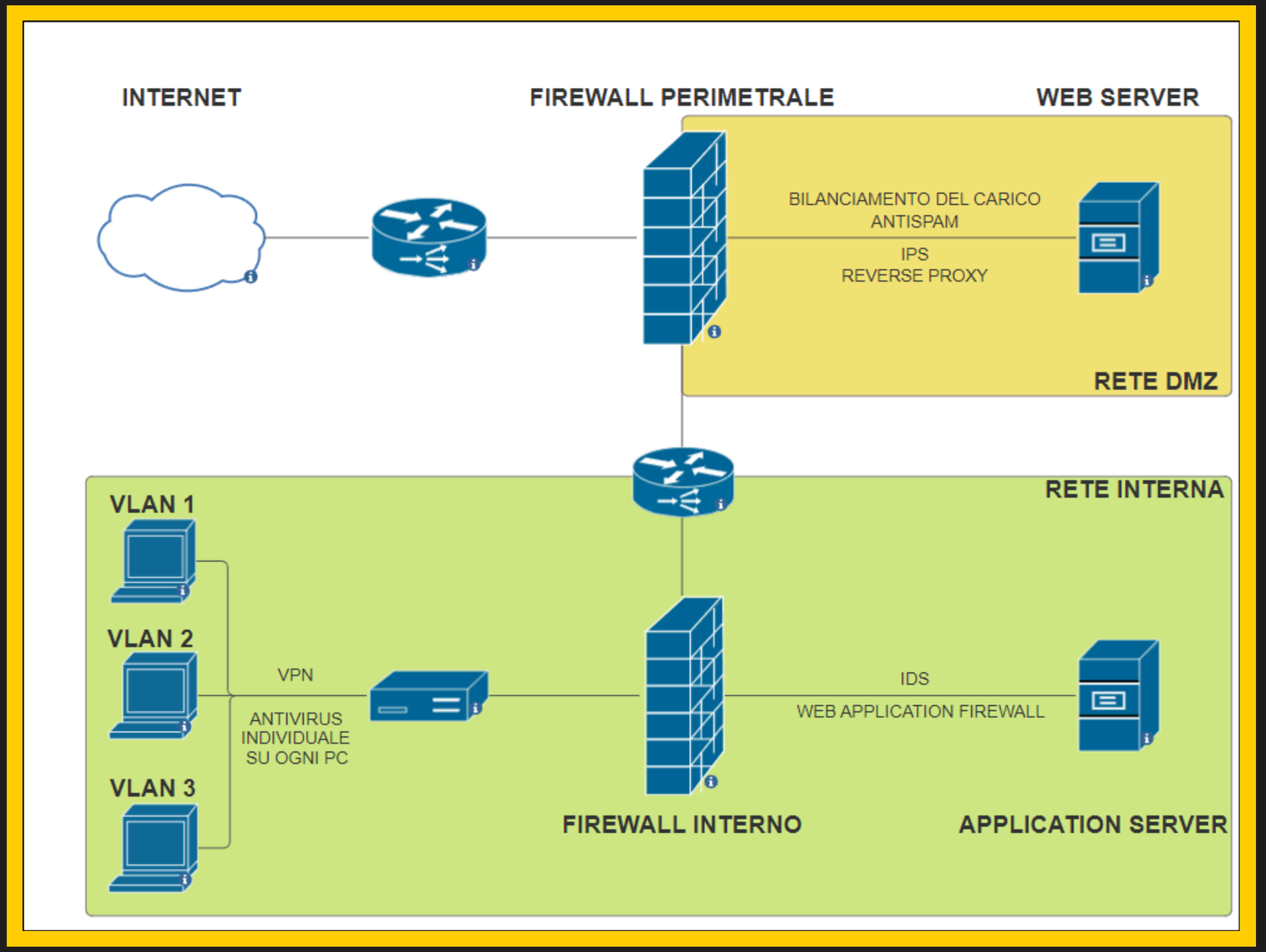
- **Web Server (WS)**: espone servizi su internet, accessibile al pubblico.
- **Firewall perimetrale** per permettere solo il traffico necessario (HTTP/HTTPS) verso il WS.
- **Web Application Firewall (WAF)** per proteggere contro-attacchi specifici alle applicazioni web (es. SQL Injection, XSS).
- **IPS** per rilevare e prevenire traffico malevolo.

RETE INTERNA

La rete interna ospita l'AS e altre risorse interne, protetta da ulteriori livelli di sicurezza.

- **Application Server (AS) + Firewall/IDS**:
  - applicativo di e-commerce, accessibile solo da indirizzi IP interni.
  - VPN per l'accesso remoto degli impiegati, con autenticazione a due fattori (2FA).
  - segmentazione della rete per isolare l'AS da altre aree della rete interna.

NETWORK DESIGN



Virtual lab

Metasploitable2

In conformità con le direttive, non sono stati eseguiti test invasivi nell'ambiente operativo principale.

Le componenti sono state replicate nei nostri laboratori di prova, consentendo di eseguire controlli in modo sicuro, separati dall'ambiente di produzione.

Metasploitable2: web server svolto da un'istanza della macchina che ospita un servizio web sulla porta 80.

HTTP VERBS

Identificazione delle vulnerabilità

Uno scan dei servizi può individuare servizi non necessari o non autorizzati che potrebbero essere sfruttati da hacker per infiltrarsi nel sistema, rivelando potenziali punti deboli.

Valutazione della configurazione di sicurezza

Gli amministratori possono valutare se la configurazione dei servizi è sicura, identificando password deboli o servizi non aggiornati che potrebbero essere vulnerabili agli attacchi.

Rilevamento di intrusioni

Lo scan dei servizi aiuta a individuare attività sospette o intrusioni, segnalando servizi non autorizzati o comportamenti anomali che potrebbero indicare una compromissione del sistema.

Gestione del rischio

Conoscere i servizi attivi consente agli amministratori di valutare meglio il rischio associato al sistema e di prendere misure adeguate per mitigare tali rischi, come chiudere o limitare l'accesso a determinati servizi per ridurre la superficie di attacco.

HTTP VERBS

Identificati i seguenti metodi abilitati sulla porta 80:

- OPTIONS
- GET
- HEAD
- POST
- PUT
- DELETE
- TRACE
- PATCH

Metodi disabilitati:

- CONNECT

```
1  Inizio nuova sessione
2  E' stato creato il file di log
3  2024-06-19 00:39:53,077 - INFO - Inizio scansione metodi HTTP su 192.168.50.101:80/
4  2024-06-19 00:39:53,114 - INFO - Metodo OPTIONS all'indirizzo 192.168.50.101:80/ - Enabled
5  2024-06-19 00:39:53,145 - INFO - Metodo GET all'indirizzo 192.168.50.101:80/ - Enabled
6  2024-06-19 00:39:53,174 - INFO - Metodo HEAD all'indirizzo 192.168.50.101:80/ - Enabled
7  2024-06-19 00:39:53,204 - INFO - Metodo POST all'indirizzo 192.168.50.101:80/ - Enabled
8  2024-06-19 00:39:53,234 - INFO - Metodo PUT all'indirizzo 192.168.50.101:80/ - Enabled
9  2024-06-19 00:39:53,263 - INFO - Metodo DELETE all'indirizzo 192.168.50.101:80/ - Enabled
10 2024-06-19 00:39:53,266 - INFO - Metodo TRACE all'indirizzo 192.168.50.101:80/ - Enabled
11 2024-06-19 00:39:53,267 - INFO - Metodo CONNECT all'indirizzo 192.168.50.101:80/ - Disabled
12 2024-06-19 00:39:53,295 - INFO - Metodo PATCH all'indirizzo 192.168.50.101:80/ - Enabled
13 2024-06-19 00:39:53,295 - INFO - Scansione terminata
14 2024-06-19 00:39:53,295 - INFO - OPTIONS: Enabled
15 2024-06-19 00:39:53,295 - INFO - GET: Enabled
16 2024-06-19 00:39:53,296 - INFO - HEAD: Enabled
17 2024-06-19 00:39:53,296 - INFO - POST: Enabled
18 2024-06-19 00:39:53,296 - INFO - PUT: Enabled
19 2024-06-19 00:39:53,296 - INFO - DELETE: Enabled
20 2024-06-19 00:39:53,296 - INFO - TRACE: Enabled
21 2024-06-19 00:39:53,296 - INFO - CONNECT: Disabled
22 2024-06-19 00:39:53,296 - INFO - PATCH: Enabled
```

PORT SCANNING

Il port scanning è un processo che identifica le porte aperte e chiuse su un sistema o una rete.

Strumento cruciale per valutare la sicurezza e individuare vulnerabilità:

- identificare i servizi in esecuzione;
- valutare della sicurezza del sistema;
- rilevare possibili intrusioni;
- migliorare la configurazione di rete.

Lo scanning delle porte è stato effettuato usando uno script ad hoc sviluppato dal nostro team.

PORT SCANNING

```
UDP Port 7 (echo): OPEN or FILTERED
UDP Port 9 (discard): OPEN or FILTERED
UDP Port 13 (daytime): OPEN or FILTERED
UDP Port 19 (chargen): OPEN or FILTERED
UDP Port 21 (fsp): OPEN or FILTERED
UDP Port 37 (time): OPEN or FILTERED
UDP Port 49 (tacacs): OPEN or FILTERED
UDP Port 53 (domain): OPEN or FILTERED
UDP Port 67 (bootps): OPEN or FILTERED
UDP Port 68 (bootpc): OPEN or FILTERED
UDP Port 69 (tftp): OPEN or FILTERED
UDP Port 88 (kerberos): OPEN or FILTERED
UDP Port 111 (sunrpc): OPEN or FILTERED
UDP Port 123 (ntp): OPEN or FILTERED
UDP Port 137 (netbios-ns): OPEN or FILTERED
UDP Port 138 (netbios-dgm): OPEN or FILTERED
UDP Port 161 (snmp): OPEN or FILTERED
UDP Port 162 (snmp-trap): OPEN or FILTERED
UDP Port 163 (cmip-man): OPEN or FILTERED
UDP Port 164 (cmip-agent): OPEN or FILTERED
UDP Port 177 (xdmcp): OPEN or FILTERED
```

```
TCP Port 21 (ftp): OPEN
TCP Port 22 (ssh): OPEN
TCP Port 23 (telnet): OPEN
TCP Port 25 (smtp): OPEN
TCP Port 53 (domain): OPEN
TCP Port 80 (http): OPEN
TCP Port 111 (sunrpc): OPEN
TCP Port 139 (netbios-ssn): OPEN
TCP Port 445 (microsoft-ds): OPEN
TCP Port 512 (exec): OPEN
TCP Port 513 (login): OPEN
TCP Port 514 (shell): OPEN
TCP Port 1099 (rmiregistry): OPEN
TCP Port 1524 (ingreslock): OPEN
TCP Port 2049 (nfs): OPEN
TCP Port 2121 (iprop): OPEN
TCP Port 3306 (mysql): OPEN
TCP Port 3632 (distcc): OPEN
TCP Port 5432 (postgresql): OPEN
TCP Port 5900 (Unknown): OPEN
TCP Port 6000 (x11): OPEN
TCP Port 6667 (ircd): OPEN
TCP Port 6697 (ircs-u): OPEN
TCP Port 8009 (Unknown): OPEN
TCP Port 8180 (Unknown): OPEN
TCP Port 8787 (Unknown): OPEN
TCP Port 52118 (Unknown): OPEN
TCP Port 57915 (Unknown): OPEN
TCP Port 58359 (Unknown): OPEN
TCP Port 60778 (Unknown): OPEN
```

BRUTE FORCE ATTACK

Il Brute Force può essere utilizzato per compromettere la sicurezza di sistemi informatici, reti, account online e altro ancora.

- Tecnica utilizzata per tentare di ottenere accesso a un sistema o a un account tramite il tentativo ripetuto e sistematico di tutte le possibili combinazioni di username/password o altre credenziali di accesso.

- Questo metodo si basa sull'idea che, con sufficiente tempo e risorse a disposizione, è possibile violare la sicurezza di un sistema tramite il tentativo di tutte le combinazioni possibili finché non si trova quella corretta.

Per mitigare e proteggersi da questo tipo di attacco si consiglia:

- l'implementazione di politiche di sicurezza robuste;
- l'uso di password complesse;
- l'implementazione di misure di protezione, come la limitazione dei tentativi di accesso.

BRUTE FORCE ATTACK

Damn Vulnerable web application (DVWA)

Applicativo Web con diverse possibili impostazioni di sicurezza:

LOW SECURITY

L'unica richiesta all'utente durante il login è l'inserimento delle correte credenziali. Il server confronta i campi di interesse immessi dall'utente, come username e password, con i dati salvati nel proprio database, e, se i dati sono corretti, permetterà l'accesso.

MEDIUM SECURITY

Differenza rispetto al livello precedente: la **SANITISE**. Quando si accettano input dagli utenti, è essenziale applicare la sanitizzazione per evitare che questi possano essere utilizzati per compromettere la sicurezza del sistema.

HIGH SECURITY

Aggiunta importante del livello è lo **SLEEP**, periodo di tempo che il server attende prima di inviare la risposta al client nel caso in cui la prova di accesso abbia esito negativo.

BRUTE FORCE ATTACK

Damn Vulnerable web application (DVWA)

```
Livello di sicurezza: login
Tempo impiegato: 221.58 secondi
Username: 1337, Password: charley
Username: smithy, Password: password
Username: admin, Password: password
Username: gordonb, Password: abc123
Username: pablo, Password: letmein
```

```
Livello di sicurezza: low
Tempo impiegato: 123.70 secondi
Username: 1337, Password: charley
Username: smithy, Password: password
Username: admin, Password: password
Username: gordonb, Password: abc123
Username: pablo, Password: letmein

Livello di sicurezza: medium
Tempo impiegato: 127.35 secondi
Username: 1337, Password: charley
Username: smithy, Password: password
Username: admin, Password: password
Username: gordonb, Password: abc123
Username: pablo, Password: letmein

Livello di sicurezza: high
Tempo impiegato: 4446.39 secondi
Username: 1337, Password: charley
Username: smithy, Password: password
Username: admin, Password: password
Username: gordonb, Password: abc123
Username: pablo, Password: letmein
```

BRUTE FORCE ATTACK

phpMyAdmin

Fondamentale differenza rispetto a DVWA: il **CSRF TOKEN**.

Richiesta

Necessaria aggiunta di un'altra variabile non mostrata in chiaro, il token, a cui viene assegnato un codice alfanumerico casuale generato dal server ad ogni richiesta HTTP di accesso dell’utente.

Risposta

Il server verifica che il token CSRF inviato corrisponda a quello memorizzato per l’utente e per la sessione in corso. Se il token non è corretto o è assente, il server rifiuterà la richiesta.

```
1 Tempo impiegato: 463.89 secondi
2 Username: debian-sys-maint, Password:
3 Username: user, Password: pass
4 Username: guest, Password:
```

BEST PRACTICES

Il modello proposto garantisce una separazione chiara tra le componenti esposte al pubblico e quelle interne, con vari livelli di sicurezza per mitigare i rischi.
L'implementazione di dispositivi di sicurezza avanzati e la segmentazione della rete assicurano una protezione robusta delle infrastrutture critiche della compagnia Theta.

Prestare attenzione

a servizi web (social network, cloud, e-mail, spazio web, ecc.) offerti da terze parti;

Utilizzare password

complesse/differenti per ogni account, in aggiunta a servizi di autenticazione a due fattori (2FA);

Nominare un referente

responsabile per il coordinamento delle attività di gestione e protezione delle informazioni e dei sistemi informatici;

Dotare ogni dispositivo

di software di protezione (antivirus, antimalware, ecc.) regolarmente aggiornato;

Provvedere alla formazione

e sensibilizzazione del personale riguardo i rischi di sicurezza informatica;

Eseguire periodicamente

backup delle informazioni e dei dati critici per l’azienda, conservarli in modo sicuro, verificandone periodicamente l'integrità.

Our Team

Simone La Porta

Team Leader

Nicolò Callegaro

Simone Esposito

Grazia Coco

Gianluca Sansone

Alejandro Cristino

Alessio Forli