

RELAZIONE BUILDWEEK



Progetto Infrastruttura Theta

FalconLock

Sommario

1.STRUTTURA DEL PROGETTO	3
2.INFRASTRUTTURA	4
3.SUBNETS.....	5
4.FIREWALL	6
4.1. Configurazione Porte GigabitEthernet.....	6
4.2. Creazione Alias	7
4.3. Aggiunta Regole pfSense.....	7
5.IDS/IPS	9
6.ANALISI DVWA.....	10
6.1. Enumerazione Porte Aperte.....	10
6.2. Analisi Metodi http.....	14
7.CONCLUSIONI	15
8.GLOSSARIO.....	15

1. STRUTTURA DEL PROGETTO

1.1. Obiettivi

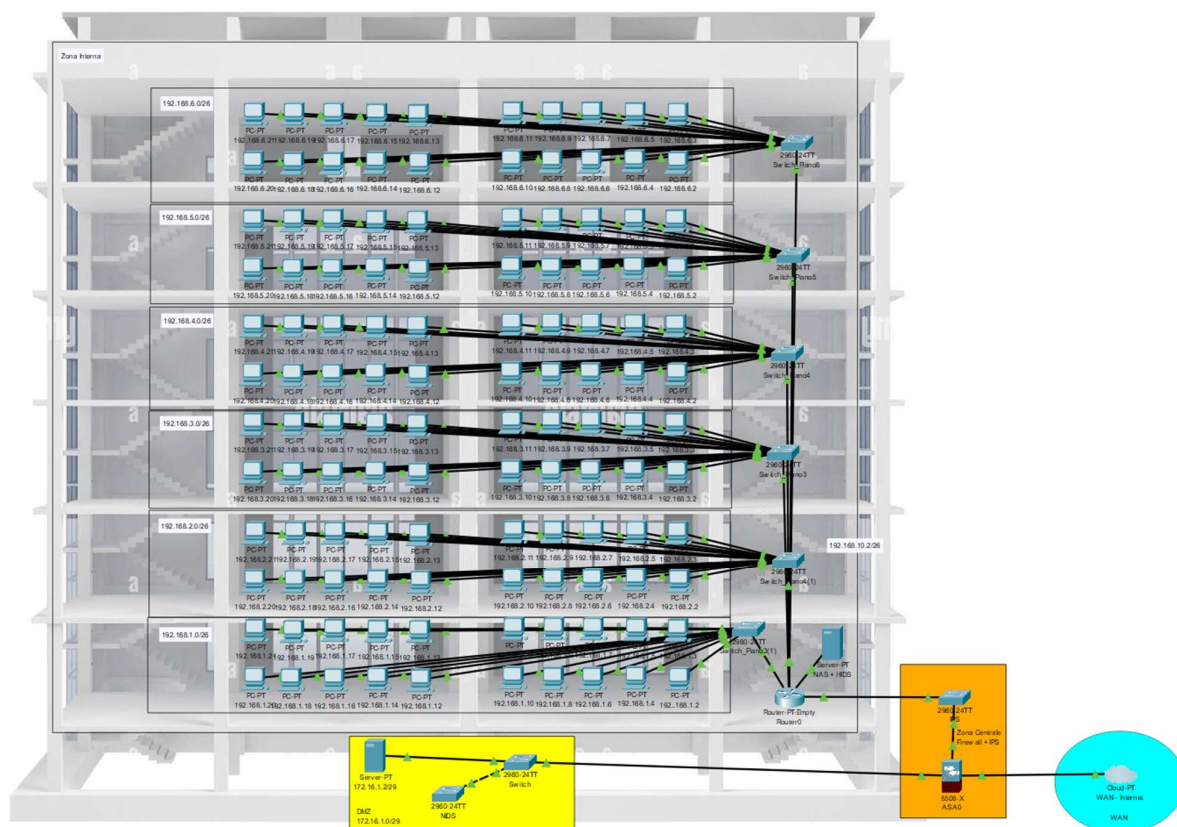
Il progetto si pone tre obiettivi principali:

- Progettazione dell'infrastruttura di rete per la società Theta composta da:
 - 6 piani di uffici per un totale di 120 Client
 - 1 NAS
 - 1 Web Server posizionato all'interno della DMZ
 - 1 Firewall
 - 3 IDS/IP
- Sviluppo Tools per l'analisi del Web Server
- Mitigazione vulnerabilità Web Server

1.2. Composizione Team

- Simeone Cristofaro - Team Leader
- Alfonso Pio Montalbano
- Andrea Pensierini
- Ernesto Mercurio
- Giuseppe Cevallos
- Matteo Garau
- Ritish Bantooa
- Sergio Musto

2.INFRASTRUTTURA



L'infrastruttura di rete della società Theta è stata divisa in quattro zone:

2.1. ZONA INTERNA: raggruppa gli uffici dell'azienda Theta che sono disposti su sei piani.

La topologia della zona è a stella estesa per semplicità di implementazione e facilità di una possibile futura espansione.

Ogni piano è composto da:

- 20 personal computer
- 1 switch 24 porte

Messi in collegamento da un centro stella costituito da un router con 8 porte GigabitEthernet.

Come sistema di archiviazione aziendale è stato predisposto un NAS accessibile da tutti i client della zona interna.

Nel NAS è in esecuzione un HIDS che invia messaggi di allert nel caso riscontrasse accessi/operazioni sui file non consuete.

2.2. DMZ: zona a cui è permesso l'accesso dall'esterno della rete aziendale. I dispositivi presenti non possono contattare la rete interna.

Composta da:

- Server Web: DVWA di Metasploitable.

2.3. ZONA ESTERNA: raffigurata per completezza ma non gestita dalla FalconLock. Rete pubblica che permette l'accesso alla WAN.

2.4. ZONA CENTRALE: Assolve i compiti di

- Collegamento tra le diverse zone che compongono l'infrastruttura
- Filtraggio del traffico tramite la presenza di un Firewall
- Monitoraggio del traffico mediante l'implementazione di:
 - NIDS all'interno della DMZ per ricevere avvisi in caso di attività che richiedano un approfondimento dal SOC.
 - IPS posto tra il firewall e la rete interna per intervenire prontamente in caso rilevamento di pattern riconosciuti come dannosi.

3.SUBNETS

Per dividere logicamente i piani degli uffici sono state create sei subnets.

Vista la presenza di computer fissi e di numero ben definito si è optato di assegnare staticamente ad ogni client un IP. Questa scelta permetterà al reparto IT, in caso di necessità, di connettersi da remoto in modo più agevole sapendo a quale IP corrisponde ogni macchina.

Le subnets sono le seguenti:

- Piano 1:
 - IP Network: 192.168.1.0
 - Subnetmask: 255.255.255.192
 - IP Gateway: 192.168.1.1
 - IP Broadcast: 192.168.1.63
 - N. Max Hosts: 61 + Gateway
- Piano 2:
 - IP Network: 192.168.2.0
 - Subnetmask: 255.255.255.192
 - IP Gateway: 192.168.2.1
 - IP Broadcast: 192.168.2.63
 - N. Max Hosts: 61 + Gateway
- Piano 3:
 - IP Network: 192.168.3.0
 - Subnetmask: 255.255.255.192
 - IP Gateway: 192.168.3.1
 - IP Broadcast: 192.168.3.63
 - N. Max Hosts: 61 + Gateway
- Piano 4:
 - IP Network: 192.168.4.0
 - Subnetmask: 255.255.255.192
 - IP Gateway: 192.168.4.1
 - IP Broadcast: 192.168.4.63
 - N. Max Hosts: 61 + Gateway
- Piano 5:
 - IP Network: 192.168.5.0
 - Subnetmask: 255.255.255.192
 - IP Gateway: 192.168.5.1
 - IP Broadcast: 192.168.5.63
 - N. Max Hosts: 61 + Gateway

- Piano 6:
 - IP Network: 192.168.6.0
 - Subnetmask: 255.255.255.192
 - IP Gateway: 192.168.6.1
 - IP Broadcast: 192.168.6.63
 - N. Max Hosts: 61 + Gateway

All'interno del Router0 sono state caricate, mediante file di configurazione, le ACL per bloccare il traffico tra i piani dello stabile consentendo, allo stesso tempo, a tutte le subnets di collegarsi al NAS.

```

192.168.4.3
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
  
```

4. FIREWALL

A protezione dell'intera infrastruttura è stato predisposto un firewall NETGATE 1537 MAX pfSense+. Il software firewall in esecuzione al suo interno è la versione a pagamento di pfSense.

4.1. Configurazione Porte GigabitEthernet

- WAN: la configurazione della porta rispecchia i parametri forniti dall'ISP
- DMZ
 - IP: 172.16.1.1
 - Subnet Mask: 255.255.255.248 (CIDR /29)
- RETEINTERNA
 - IP: 172.16.1.9
 - Subnet Mask: 255.255.255.248 (CIDR/29)

4.2. Creazione Alias

Firewall / Aliases / Edit

Properties

Name
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description
A description may be entered here for administrative reference (not parsed).

Type

Network(s)

Hint Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

Network or FQDN					
<input type="text" value="192.168.1.0"/>	/	<input type="text" value="26"/>	<input type="text" value="Piano 1"/>		Delete
<input type="text" value="192.168.2.0"/>	/	<input type="text" value="26"/>	<input type="text" value="Piano 2"/>		Delete
<input type="text" value="192.168.3.0"/>	/	<input type="text" value="26"/>	<input type="text" value="Piano 3"/>		Delete
<input type="text" value="192.168.4.0"/>	/	<input type="text" value="26"/>	<input type="text" value="Piano 4"/>		Delete
<input type="text" value="192.168.5.0"/>	/	<input type="text" value="26"/>	<input type="text" value="Piano 5"/>		Delete
<input type="text" value="192.168.6.0"/>	/	<input type="text" value="26"/>	<input type="text" value="Piano 6"/>		Delete
<input type="text" value="192.168.10.0"/>	/	<input type="text" value="26"/>	<input type="text" value="NAS"/>		Delete

Per una gestione migliore delle regole si definisce un nome per indicare un gruppo di reti.

- Rete_Interna
 - 192.168.1.0/26 - Piano 1
 - 192.168.2.0/26 - Piano 2
 - 192.168.3.0/26 - Piano 3
 - 192.168.4.0/26 - Piano 4
 - 192.168.5.0/26 - Piano 5
 - 192.168.6.0/26 - Piano 6
 - 192.168.10.0/26 - NAS

4.3. Aggiunta Regole pfSense

Firewall / Rules / RETEINTERNA

Floating WAN DMZ RETEINTERNA

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗	0/0 B	IPv4 *	Uffici_Subnets	*	172.16.1.0/29	*	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 *	*	*	*	*	*	none		

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

- Rete Interna:
 - Regola1: Impedisce qualsiasi richiesta avanzata dalla zona interna verso la DMZ
 - Action: Block
 - Address Family: IPv4

- Protocol: Any
- Source Address or Alias: Uffici_Subnets
- Source Port: Any
- Destination: 172.16.1.0/29
- Destination Port: Any

- Regola2: permette ai client della rete interna di raggiungere internet
 - Action: Pass
 - Address Family: IPv4
 - Protocol: Any
 - Source: Any
 - Source Port: Any
 - Destination: Any
 - Destination Port: Any

Firewall / Rules / DMZ

Floating WAN **DMZ** RETEINTERNA

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	172.16.1.0/29	*	Uffici_Subnets	*	*	none			

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

- DMZ:
 - Regola1: impedisce qualsiasi richiesta avanzata dalla DMZ verso la zona interna
 - Action: Block
 - Address Family: IPv4
 - Protocol: Any
 - Source: 172.16.1.0/29
 - Source Port: Any
 - Destination Address or Alias: Uffici_Subnets
 - Destination Port: Any

- WAN:

Firewall / Rules / WAN

Floating **WAN** DMZ RETEINTERNA

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✗ 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	*	*	Uffici_Subnets	*	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	172.16.1.2	443 (HTTPS)	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	172.16.1.2	80 (HTTP)	*	none			
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	*	*	172.16.1.0/29	*	*	none			

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

- Regola 1: impedisce qualsiasi richiesta proveniente da internet destinata alla rete interna
 - Action: Block
 - Address Family: IPv4
 - Protocol: Any
 - Source: Any
 - Source Port: Any
 - Destination Address or Alias: Uffici_Subnets
 - Destination Port: Any
- Regola 2 + Regola 3 + Regola 4: permette di raggiungere il server web nella DMZ solo sulla porta 80 o 443
 - Action: Pass
 - Address Family: IPv4
 - Protocol: TCP
 - Source: Any
 - Source Port: Any
 - Destination Address or Alias: 172.16.1.2
 - Destination Port: 80
- Action: Pass
- Address Family: IPv4
- Protocol: TCP
- Source: Any
- Source Port: Any
- Destination Address or Alias: 172.16.1.2
- Destination Port: 443
- Action: Block
- Address Family: IPv4
- Protocol: TCP
- Source: Any
- Source Port: Any
- Destination: 172.16.1.0/29
- Destination Port: Any

5.IDS/IPS

La scelta del posizionamento di IDS/IPS e di quali dei due componenti installare nella rete è dovuta a una decisione strategica rappresentata in questo modo:

IDS (Intrusion Detection System)

Questo sistema è utilizzabile in due modi:

- HIDS (Host-based Intrusion Detection System): Monitora un singolo dispositivo, analizzando log di sistema, modifiche ai file e attività sospette inviando Alert al SOC. Nel nostro caso il software è installato nel server NAS.
- NIDS (Network Intrusion Detection System): Analizza il traffico di rete per identificare attacchi come scansioni, exploit o malware inviando notifiche come l'HIDS. A differenza del precedente lo abbiamo installato all'interno della rete DMZ.

IPS (Intrusion Prevention System)

Per implementare la sicurezza delle reti interne abbiamo optato per l'utilizzo dell'IPS, un componente attivo per incrementare la sicurezza del sistema.

Il posizionamento dell'IPS, inline tra il firewall e la rete interna, è stato pensato in quanto capaci di bloccare immediatamente minacce identificate rivolte all'interno di Theta.

È consigliabile tenere in conto che questo sistema è soggetto alla segnalazione di falsi positivi.

Una delle differenze cruciali tra IDS e IPS è che quest'ultimo rallenta la rete dato che svolge dei processi aggiuntivi più complessi nell'invio dei dati.

6.ANALISI DVWA

Nella DMZ è presente il web server su cui si è andati a svolgere un'attenta analisi in quanto raggiungibile dall'esterno della rete.

6.1. Enumerazione Porte Aperte

Il tool sviluppato ha effettuato una scansione dandoci immediato riscontro delle porte aperte e del servizio ad esse collegata.

```
Enter the IP address to scan (default: 192.168.100.110):
Enter the port range to scan (default: 1-1024): 1-65365
Scanning host 192.168.100.110 from port 1 to port 65365
>>> Port 21 File Transfer [Control] - OPEN
>>> Port 22 SSH Remote Login Protocol - OPEN
>>> Port 23 Telnet - OPEN
>>> Port 25 Simple Mail Transfer - OPEN
>>> Port 53 Domain Name Server - OPEN
>>> Port 80 World Wide Web HTTP - OPEN
>>> Port 111 SUN Remote Procedure Call - OPEN
>>> Port 139 NETBIOS Session Service - OPEN
>>> Port 445 Microsoft-DS - OPEN
>>> Port 512 Remote process execution - OPEN
>>> Port 513 Remote Login - OPEN
>>> Port 514 Remote Shell - OPEN
>>> Port 1099 RMI Registry - OPEN
>>> Port 1524 dtspcd / ingres - OPEN
>>> Port 2049 Network File System - Sun Microsystems - OPEN
>>> Port 2121 CCProxy FTP / SCIENTIA-SSDB - OPEN
>>> Port 3306 MySQL - OPEN
>>> Port 5432 postgres database server - OPEN
>>> Port 5900 VNC Virtual Network Computing - OPEN
>>> Port 6000 X-Windows / W32.LoveGate.ak virus - OPEN
>>> Port 6667 IRC - OPEN
>>> Port 8009 Apache JServ Protocol - OPEN
```

WELL KNOWN PORTS

File Transfer (FTP) 21

La porta in questione consente la condivisione, upload e download tra il client e il server. Seppur semplice nelle sue funzionalità il protocollo è sprovvisto di crittografia i dati sono suscettibili a sniffing e attacchi MITM.

Un'alternativa più sicura sarebbe FTPS che ha le stesse funzionalità ma è affidabile nella crittazione di dati sensibili.

SSH Remote Login Protocol 22

SSH è un protocollo di rete crittografato utilizzato per operazioni sicure su reti non sicure.

Permette anche di accedere in remoto a un dispositivo e di trasferire file tra di essi.

Mantere aggiornato il software SSH e implementare sistemi di autenticazione forti usando le giuste configurazioni eviterà molti degli attacchi informatici possibili.

Si consiglia anche di monitorare gli accessi del log per eventuali intrusioni.

TELNET 23

Telnet fa sì che ci sia una comunicazione bidirezionale tra due macchine su rete TCP/IP, permette anche di accedere in remoto su un computer e di eseguire comandi come se si fosse collegati localmente.

Non ha nessuna crittografia rendendolo vulnerabile a intercettazione e MITM, per questa ragione se necessarie le funzioni elencate soprastanti si consiglia di chiudere la porta e passare a SSH.

Simple Mail Transfer 25 (SMTP)

SMTP è un protocollo standard per l'invio di email attraverso le reti IP dal client al server di posta notificando eventuali errori nel processo.

Per evitare problemi di spam e abusi è necessario prevenire l'accesso non autorizzato usando meccanismi di autenticazione forte.

Per impedire sniffing e MITM bisogna crittografare le comunicazioni usando SSL/TLS.

Domain Name Server 53 (DNS)

Essenziale per la risoluzione dei nomi di dominio va comunque configurata e calibrata correttamente usando firewall e autenticazioni per impedire eventuali attacchi.

Nonostante le utilità, il DNS non è necessario al dispositivo del web server creando vulnerabilità facilmente evitabili.

World Wide Web HTTP 80

Il protocollo in questione ha molte vulnerabilità ed è fortemente consigliato il passaggio ad HTTP over SSL/TLS (HTTPS) sulla porta 443 per garantire sicurezza, autenticazione e integrità.

SUN Remote Procedure Call 111

Remote Procedure Call consente di invocare una determinata funzione sul web server in remoto da un altro dispositivo.

Lasciare la porta aperta crea delle vulnerabilità ampiamente conosciute.

Vista l'esposizione ad internet del Web Server è necessario terminare il servizio.

NETBIOS Session Service 139

NetBIOS è solitamente usato su windows per condividere file e stampanti in rete locale.

Essendo un protocollo datato ha varie vulnerabilità, come esporre i pc in comunicazione tra di loro e rendendo le sessioni vulnerabili a spoofing.

Se la sua funzione rimane necessaria all'azienda si consiglia di usare TCP/IP o DNS che risultano simili ma con sistemi di sicurezza più robusti.

Microsoft-DS 445

La porta in questione è una delle più vulnerabili essendo spesso soggetto di attacchi informatici, il protocollo è pensato unicamente per la condivisione di file e stampanti tramite pc con diversi OS senza imporre nessun sistema di sicurezza.

Per farne uso è cruciale implementare autenticazioni forti, crittografie, controllo degli accessi e isolare la rete.

Per evitare molte problematiche è preferibile chiudere la porta.

Remote process execution 512

Come altri protocolli permette di eseguire comandi da remoto sul server, utile per amministratori e sviluppatori per gestire il Web Server dell'azienda.

Nonostante ciò comporta delle problematiche di sicurezza come un'autenticazione debole e una mancanza di cifratura, l'alternativa migliore è usare SSH.

Remote Login 513

Il servizio Remote Login permette l'accesso in remoto al server usando una connessione TCP così da poter eseguire comandi e accedere i file da altri dispositivi esterni.

Per queste stesse ragioni va strettamente monitorata e configurata per impedire qualsiasi abuso, ha anche gravi problemi come una mancanza di cifratura e di autenticazione forte.

Come la precedente è meglio passare a SSH che mantiene le stesse funzioni.

REMOTE SHELL 514

Permette a utenti esterni di eseguire comandi sulla macchina del server in remoto senza la necessità di autorizzazioni, trasmettendo i comandi in chiaro.

Implementare sistemi di autenticazione e criptazione è essenziale per mantenere l'integrità del server anche come riconfigurare correttamente il firewall.

REGISTERED PORTSRMI REGISTRY 1099

Questa funzione di Java permette di registrare in una sorta di rubrica tutti i dispositivi collegati in remoto facilitandone la connessione.

Non essendo provvisto di metodo di autenticazione e crittografia chiunque può modificare i registri creando connessioni non sicure o collegamenti Man-In-The-Middle.

Altri rischi sono di andare incontro ad attacchi DOS (Denial of service) e RCE (Remote code execution).

Configurare il registro con autenticazione e criptazioni delle connessioni può evitare molte di queste problematiche.

INGRES /DTSPCD 1524

Ingres permette la gestione e archiviazione dei dati nel database del server, bisogna assicurarsi che sia aggiornato per evitare vulnerabilità nel server.

Il DTSPCD comporta dei rischi nella manipolazione dei dati e la porta è consigliato chiuderla per evitare che attaccanti esterni possano accedere sul server con privilegi Root e mantenendosi collegati con una backdoor

NETWORK FILE SYSTEM 2049:

Permette la condivisione efficiente dei file sulla rete di un server.

Per rendere sicura questa funzione bisogna implementare un servizio di autenticazione o limitare con il firewall l'accesso ad utenti esterni non riconosciuti.

Non avendo le funzioni capaci di criptare i dati si consiglia di implementarne per evitare vulnerabilità come SNIFFING e MITM. Consigliato l'uso di SSH.

CCProxy FTP / SCIENTIA-SSDB 2121

CCProxy è un software che permette la gestione di dati attraverso il protocollo FTP e all'uso del servizio di SCIENTIA-SSDB.

La porta se lasciata aperta mette in rischio il server all'esecuzione di codice da remoto.

Se necessaria è d'obbligo FTPS invece di FTP avendo delle funzionalità molto più sicure per gli standard di oggi.

Numerose Backdoor utilizzano questa porta per avviare un server FTP insicuro.

MySQL 3306

Questo sistema permette la gestione dei database ed è utile per il supporto di applicazioni web dinamiche.

Per evitare accessi non autorizzati si consiglia di configurare il firewall consentendo l'accesso solo agli IP di rete fidati della rete interna.

Implementare un sistema di autenticazione a due fattori e mantenere aggiornato il software sono cruciali per mantenere la sicurezza del server.

POSTGRES DATABASE SERVER (PostgreSQL) 5432

Utile per stabilire connessioni tra il client e il server capace di inviare query SQL al server per eseguire operazioni CRUD.

Limitare l'accesso con l'uso di firewall e autenticazioni sicure può limitare l'area di attacco del server.

Aggiornare e configurare il software sono elementi cruciali per mantenerne la sicurezza.

VNC Virtual Network Computing 5900

La porta in questione è associata ad un servizio di Graphical Remote Desktop.

Come le precedenti, seguire gli stessi passaggi di configurazione per il software e il firewall limitando gli IP a quelli aziendali.

L'implementazione di un sistema di autenticazione per l'uso in remoto è necessaria per evitare che esterni sfruttino le funzioni del VNC.

X-Windows / W32.LoveGate.ak virus 6000

Porta utilizzata da diversi trojan quali: LoveGate, The Thing, Aladino, NetBus, APStrojan.

Necessaria una scansione approfondita del Web Server.

IRC (Internet Relay Chat) 6667

Permette la discussione attraverso una chat tra i dispositivi client e il server.

Spesso trojan e backdoors sfruttano la porta per mantenere l'accesso al server, ormai in declino questo protocollo è preferibile evitarlo per non andare incontro a svariate exploit.

Disabilitare il servizio e usare un sistema di comunicazione in tempo reale alternativo.

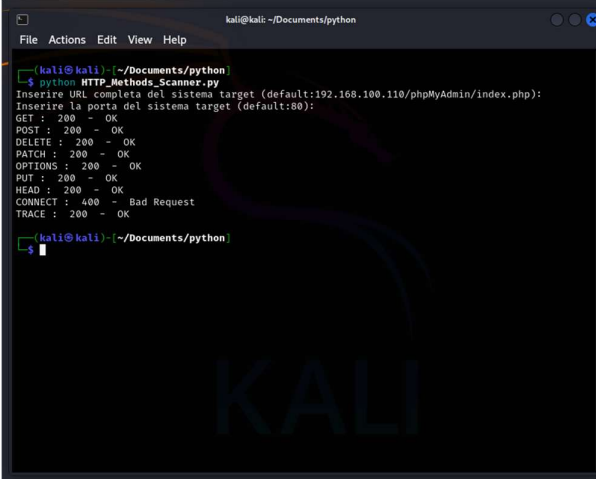
Apache JServ Protocol 8009

L'ultima porta aperta nella lista è usata per le comunicazioni tra Apache e l'applicazione del server in maniera efficiente alleggerendo il traffico di rete.

Versions datate di AJP espongono a vulnerabilità note. Si consiglia l'aggiornamento all'ultima versione disponibile.

6.2. Analisi Metodi http

La seconda parte dell'analisi si è concentrata sull'analisi dei metodi accettati dal Web Server e sui codici di stato restituiti.



```
kali@kali: ~/Documents/python
File Actions Edit View Help
(kali@kali)~/Documents/python
$ python HTTP_Methods_Scanner.py
Inserire URL completa del sistema target (default:192.168.100.110/phpMyAdmin/index.php):
Inserire la porta del sistema target (default:80):
GET : 200 - OK
POST : 200 - OK
DELETE : 200 - OK
PATCH : 200 - OK
OPTIONS : 200 - OK
PUT : 200 - OK
HEAD : 200 - OK
CONNECT : 400 - Bad Request
TRACE : 200 - OK
(kali@kali)~/Documents/python
$
```

Analisi risposte:

- GET: 200 - OK => Risposta corretta
- POST: 200 - OK => Risposta non corretta. Dovrebbe restituire 400 - Bad Request in quanto non sono stati forniti dati da processare
- DELETE: 200 - OK => Risposta non corretta. Il server non esegue la DELETE della risorsa. Dovrebbe restituire 401 - Unauthorized in quanto è stata inviata una richiesta per una cancellazione di una risorsa senza fornire nessun metodo di autenticazione.
- PATCH: 200 - OK => Risposta non corretta. Il server non esegue la PATCH. Dovrebbe restituire 401 - Unauthorized in quanto è stata inviata una richiesta per una modifica di una risorsa senza fornire nessun metodo di autenticazione.
- OPTION: 200 - OK => Risposta corretta. A seguito di ulteriori analisi si riscontra che il server non invia in risposta i metodi ammessi.
- PUT: 200 - OK => Risposta non corretta. Il server non esegue la PUT. Dovrebbe restituire 401 - Unauthorized in quanto è stata inviata una richiesta per un inserimento di una nuova risorsa senza fornire nessun metodo di autenticazione.
- HEAD: 200 - OK => Risposta corretta
- CONNECT: 400 - Bad Request => Risposta corretta.
- TRACE: 200 - OK => Risposta corretta.

Mitigazione:

- Implementare una corretta gestione delle richieste dapprima settando adeguatamente i file di configurazione del servizio web impostando i metodi ammessi.
- Se non fosse possibile accedere alla configurazione del server gestire le richieste tramite funzioni nel codice della pagina web.

7.CONCLUSIONI

La corretta progettazione di una rete è un passo fondamentale per garantire un adeguato livello di sicurezza. Ogni parte di questo processo, sia hardware nella scelta e posizionamento dei componenti, sia software nella loro corretta configurazione, svolge un ruolo di primaria importanza.

Si è visto come:

- la scelta e il posizionamento di strumenti quali IPS, HIDS e NIDS sia strategico per garantire il massimo livello di QoS, senza interruzioni dei servizi offerti per rilevamenti errati ma con gli asset aziendali sotto costante supervisione.
- La configurazione del Firewall protegge le zone sensibili aziendali impedendo accessi indesiderati e potenziali minacce.
- La ricerca e identificazione delle vulnerabilità sui sistemi applicativi sia indispensabile affinché, tutto quello fatto in precedenza, non venga vanificato da una cattiva configurazione.

Nello specifico il Web Server, esposto all'accesso da internet, presenta un elevato numero di vulnerabilità che potrebbero sicuramente minare la sicurezza dell'azienda Theta nonostante gli accorgimenti messi in campo nella progettazione della rete.

8.GLOSSARIO

- **DMZ - Demilitarized Zone**
sottorete fisica o logica che contiene ed espone dei servizi ad una rete esterna non ritenuta sicura, come ad esempio Internet. Lo scopo di una DMZ è di proteggere la rete LAN di un'organizzazione.
- **IDS - Intrusion Detection System**
dispositivo software o hardware utilizzato per identificare accessi non autorizzati ai computer o alle reti locali.
- **IPS - Intrusion Prevention System**
componenti software attivi sviluppati per incrementare la sicurezza informatica di un sistema informatico, individuando, registrando le informazioni relative e tentando di segnalare e bloccare le attività dannose.
- **WAN - Wide Area Network**
rete di telecomunicazioni che si estende su una grande area geografica con lo scopo di mettere in comunicazione altre reti di computer. La più grande rete WAN mai realizzata, a cui si fa riferimento, è Internet.
- **DHCP - Dynamic Host Configuration Protocol**
protocollo di rete che permette ai dispositivi di una rete locale di ricevere automaticamente la configurazione IP.
- **NAS - Network Attached Storage**
dispositivo di archiviazione di rete che permette di salvare, condividere e accedere ai file da più dispositivi connessi.

- DVWA - Damn Vulnerable Web Application
applicazione web intenzionalmente vulnerabile, progettata per testare e migliorare le competenze in cybersecurity e penetration testing.
- FIREWALL
componente hardware e/o software di difesa perimetrale di una rete che può anche svolgere funzioni di collegamento tra due o più segmenti di rete.
- SOC (Security Operations Center)
centro operativo dedicato alla sicurezza informatica dove un team di esperti monitora, rileva, analizza e risponde alle minacce alla sicurezza informatica di un'organizzazione.