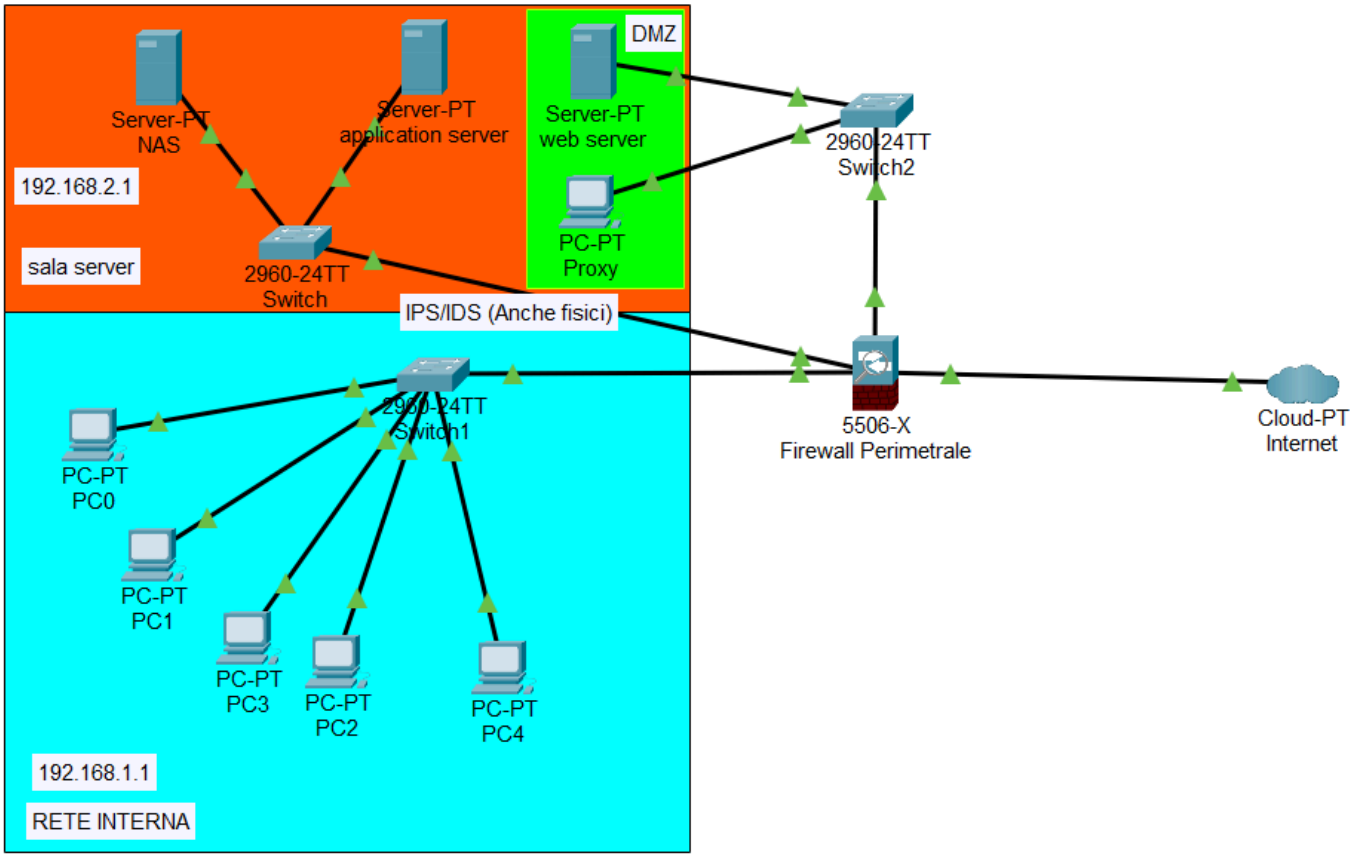
# S4, Build Week 1 - Progetto // NetRaiders - Marzo 2024

Partecipanti:
**Matteo Leoni**, Rosario Giaimo, Claudio Maida,
Gianmarco Mazzoni, Lorenzo Moro, Stefano Di Prospero.

Link Utili:
**Repository** / I titoli nella Pagina 2 sono cliccabili per verificare il *source code*!

## Schema di rete

Lo schema che vogliamo proporre all'azienda è il seguente, e comprende diversi punti chiave.
La **Sala Server** conterrà tutti gli elementi di rete che devono essere mantenuti al sicuro, quali *Server NAS*, *Application Server* e lo *Switch* a cui connettiamo il **firewall**, quest'ultimo piazzato sul perimetro, ma non all'interno. Questa sala dovrà essere quindi protetta con dispositivi di sicurezza high-end, quali una **porta blindata e un modulo di accesso biometrico** in grado di leggere le impronte digitali, consentendo l'accesso solamente al personale autorizzato. Sempre **all'interno della Sala**, sarà situata la **Demilitarized Zone**, contenente *proxy* e *Web Server*, sempre interfacciate con uno *Switch*, piazzato sul perimetro.
L'unico modo per comunicare con gli elementi nella Sala Server, *virtualmente* e non fisicamente, sarà tramite i PC collegati alla **Intranet**, grazie al firewall prima menzionato. Si è pensato anche di implementare del **software IPS/IDS** all'Application Server, per ridurre la possibilità di accessi nello stesso da parte di malintenzionati.
Ogni accesso sarà regolato anche da **MFA (Multi-Factor Authentication)**, a scelta tra numero di telefono o dispositivo fisico secondario, o dato biometrico.
Per concludere, il firewall sarà la prima e più importante **barriera d'accesso ad Internet**.



# Penetration Testing

I test effettuati sull'hardware dell'azienda sono stati effettuati con del software creato appositamente *Ad-Hoc*.

## Port Scanner

Il software importa il modulo per interagire con i socket. All'avvio richiede all'utilizzatore un indirizzo e un range di porte. Se in quest'ultimo campo, non viene inserito nulla, il controllo verrà effettuato su tutto il range disponibile (da **0** a **65535**). Dispone anche di controllo di errori di inserimento.
Dopo l'input dell'Utente, viene stampato lo stato della scansione della porta corrente, passando subito dopo a quella successiva. Ogni porta che viene indicata come aperta, viene quindi inserita in una lista temporanea per facilitare la visualizzazione una volta terminata la scansione.
Per concludere, se sono state trovate porte aperte, viene stampato un resoconto, includendo l'host scansionato, per assistere l'Utente nella creazione di report di scansioni multiple. Se invece non vengono trovate porte aperte, viene stampata il messaggio di avviso che indica che nessuna porta è stata trovata.

## Metodi HTTP

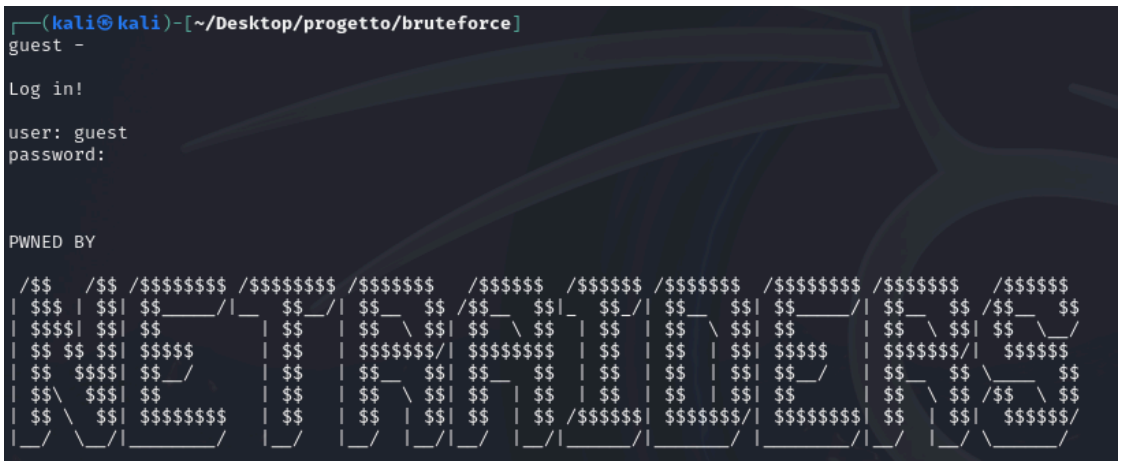
Come nel programma precedente, vengono richiesti host, porta e path in input dall'Utente, se non viene inserito nulla, verrà impostata la porta **80** (a cui si appoggiano i servizi HTTP). Questi valori vengono inseriti in una stringa, che sarà il target con cui interagiremo.
Con questo programma, possiamo verificare lo status dell'indirizzo IP, che avviene tramite una richiesta in '**OPTIONS**', che a seconda della risposta possiamo capire se la pagina esiste, se causa reindirizzamenti, o se ci sono errori lato host. Gli output sono i seguenti:
**Status 200** = La pagina esiste
**Status 301, 302, 303, 307, 308** = La pagina reindirizza
**Status 40X** = La pagina da un errore
In quest'ultimo caso, viene stampato il tipo di errore riscontrato.
Invece, se viene mostrato lo **Status 200**, vengono stampati i metodi HTTP abilitati.

## Bruteforce

Vengono importati i moduli **sys** e **requests**.
Il software legge da un file una serie di username e password più usati durante il processo di autenticazione. Tramite un ciclo **for**, che verrà interrotto il momento in cui viene trovata una combinazione efficace, effettua una serie di tentativi di login sulla pagina di accesso. Questa pagina è indicata all'interno del codice, infatti, sono state create più versioni, il cui funzionamento è pressoché identico, con la differenza del target a cui viene effettuato l'attacco. Durante l'attacco, viene visualizzata la combinazione di credenziali che sta venendo utilizzata come tentativo, che per migliorare l'User Experience e ridurre il clutter visivo, viene sostituito dalla combinazione di credenziali successiva. Una volta trovata una combinazione efficace, si chiude il ciclo e viene stampata in output, fermando il processo e lasciando il tempo all'Utente di leggere il risultato. Subito dopo, i file utilizzati prima, vengono chiusi.

## Falle di sicurezza rilevate

Riguardo al bruteforce di phpMyAdmin, dopo aver constatato che username e password fossero guest - *null (un campo vuoto)*, siamo entrati e abbiamo visto che l'Utente guest ha gli stessi privilegi dell'utente root, ciò significa che un qualsiasi ospite, nonostante fosse sprovvisto di password, avrebbe potuto effettuare modifiche nel database, come aggiungere, modificare, rimuovere utenti e liste, persino togliere privilegi al root.
Tutto ciò è inammissibile, ed è una grave falla di sicurezza.




| | User | Host | Password | Global privileges [1] | Grant | |
|---|---|---|---|---|---|---|
| ☐ | Any | % | -- | USAGE | No | |
| ☐ | debian-sys-maint | | No | SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, RELOAD, SHUTDOWN, PROCESS, FILE, REFERENCES, INDEX, ALTER, SHOW DATABASES, SUPER, CREATE TEMPORARY TABLES, LOCK TABLES, REPLICATION SLAVE, REPLICATION CLIENT, EXECUTE | Yes | |
| ☐ | guest | % | No | ALL PRIVILEGES | Yes | |
| ☐ | root | % | No | ALL PRIVILEGES | Yes | |

L'amministratore di sistema inoltre, non ha avuto la decenza di cambiare la password di default, tenendo in bella vista nella schermata di login, dentro un flavor text, le credenziali per accedere come Admin.

Hint: default username is 'admin' with password 'password'

Particolare attenzione va posta nel Bruteforce all'interno della pagina DVWA.
Dopo numerosi tentativi, ci siamo accorti che il **`PHPSESSID`** è effettivamente il cookie utilizzato per l'accesso precedente, e che senza questo token casuale (che in questo caso, non viene rigenerato), non sarebbe stato possibile effettuare altri tentativi di Bruteforce, in quanto qualsiasi risposta, avrebbe reindirizzato al login del DVWA. Attraverso uno script, creato appositamente per il bruteforce precedente, si riesce a copiare questo cookie, in un file .txt per poi riutilizzarlo nella penetrazione all'interno del DVWA. Ci siamo anche accorti che se avessimo implementato nello script il livello di security del cookie, impostandolo su **`low`**, avremmo aggirato senza problemi tutte le misure di sicurezza aggiuntive (in questo caso, avrebbero solamente rallentato il processo di check della coppia di credenziali).

```
Accept-Language: en-US,en;q=0.9
Cookie: security=high; PHPSESSID=212047b7ad6a24607f1a9807588527ed
Connection: close
```

# Report dei test

Analizziamo i punti chiave che sono sorti durante i nostri test di sicurezza informatica.

- *Porte vulnerabili e inutilizzate*
- *Credenziali deboli*
- *Assenza di Autenticazione a Fattori Multipli*

Troviamo delle soluzioni efficaci.

- E' consigliata la **chiusura delle porte non utilizzate** più vulnerabili, segue una lista dettagliata che potete consultare, di ciò che è stato trovato aperto, tra porte non well-known, e ciò che andrebbe chiuso ai fini di diminuire la possibilità di accessi non consentiti.

| | |
|---|---|
| **21** | FTP Control |
| **22** | SSH |
| **23** | Telnet |
| **25** | SMTP |
| **53** | DNS |
| **80** | HTTP |
| **111** | SUN Remote Procedure Calls |
| **139** | NetBIOS |
| **445 / TCP** | Microsoft-DS |
| **445 / UDP** | Microsoft-DS File sharing |
| **512 / TCP** | Rexec (Remote Process Execution) |
| **512 / UDP** | Comsat |
| **513 / TCP** | rlogin |
| **513 / UDP** | Who |
| **514 / TCP** | rsh / Remote Shell |
| **1099** | RMI Registry |
| **1524** | ingreslock |
| **2049** | nfs |
| **2121** | iprop |
| **3306** | mySQL |
| **3632** | distcc |
| **5432** | postgresql |
| **5900** | |
| **6000** | x11 |

| | |
|---|---|
| **6667** | irccs-u |
| **8009** | |
| **8180** | |
| **8787** | |
| **33733** | |
| **37758** | |
| **52633** | |
| **60906** | |

- **Cambio della password periodico**, ogni 3 mesi, con password completamente diversa dalla precedente, un semplice aumento di numero, non è abbastanza efficace, e il sistema dovrebbe rifiutare in modo categorico, combinazioni semplici e frequentemente utilizzate come **`qwerty`**, **`password`**, **`12345678`**, e così via.
- Rimanendo sullo stesso argomento, obbligo di **password con almeno 8 caratteri**, una lettera maiuscola e minuscola, numero e un carattere speciale (es: '**`!#@`**'). Questo renderebbe la password di difficile individuazione a dei malintenzionati in possesso di programmi capaci di eseguire bruteforce.
- L'uso di **connessioni sicure** e criptate, che si appoggiano quindi su **HTTPS**.
- L'introduzione della **MFA (Multi-Factor Authentication)** limiterebbe l'accesso ai soli dipendenti, dando all'Utente la possibilità di scegliere tra l'aggiunta di un numero di telefono a cui inviare un SMS contenente un ulteriore codice per accedere, o un dispositivo fisico secondario come un badge o una chiavetta, o un dato biometrico, come un'impronta digitale, o anche grazie ad un'**app dedicata di autenticazione**, con lo scopo di impedire l'intrusione di malintenzionati ai vostri servizi.
- Un **corso di Sicurezza Informatica** (almeno livello base) per tutti i dipendenti dell'azienda, in modo da istruire coloro che usano i PC, sui rischi che si possono incontrare in rete..
- **Modifica dei parametri di sicurezza** all'interno del sito, per renderlo effettivamente più sicuro e difficile da penetrare. In questo caso, la **sicurezza di DVWA** andrebbe impostata su **`high`**.

# Preventivo

Basandosi sulla progettazione della rete su Cisco Packet Tracer, abbiamo pianificato un piano per i costi generali del progetto, prioritizzando la sicurezza dei servizi di rete dell'azienda. Segue quindi una descrizione dei prodotti da noi scelti:
*Cisco ASA 5506-K9*: Questo firewall è disegnato per essere utilizzato in aziende di piccole dimensioni, il fattore forma lo rende ideale per essere inserito in armadi già presenti e con pochi slot liberi. 8 porte Gigabit Ethernet sono sufficienti per gestire il traffico dell'azienda. Come indicato anche nel preventivo, questo device è coperto dalla nostra assistenza.
Essendo il nostro focus principale, la Sala Server dovrà essere protetta da molteplici layer di sicurezza, fisici e virtuali, per questo nel preventivo è stata aggiunta una somma per l'assunzione di tecnici addetti all'installazione di una porta blindata, protetta da un modulo di accesso biometrico, che scansiona l'impronta digitale, facendo accedere solamente i dipendenti autorizzati.
Dopo il nostro sopralluogo, abbiamo constatato che i PC sono già collegati ad Internet, ma sarà necessario commissionare a degli elettricisti un ulteriore lavoro per fare in modo che sia tutto connesso, senza creare ingombro in termini di spazi. Verranno usati cavi di tipo CAT7, per risparmiare sui costi di deployment, e perché tipologie di grado superiore non funzionerebbero al massimo potenziale con l'hardware scelto. Si consiglia comunque di utilizzare un doppio switch da 24 porte, invece che uno singolo da 48, per rinforzare la business continuity e avere un flusso dati più stabile e affidabile.

Preventivo NetRaiders per Theta

| | Quantità / ore | Costo unitario | Costo totale |
|---|---|---|---|
| Requisiti | | | |
| Firewall ( **Cisco** ASA 5506-K9 ) | | € 1.500,00 | € 1.500,00 |
| PC Desktop a scopo di proxy | | € 1.200,00 | € 1.200,00 |
| Cablaggio Ethernet CAT7, misurato in metri | 1000 | € 1,50 | € 1.500,00 |
| Modulo accesso biometrico ( fingerprint ) per Sala Server | | € 500,00 | € 500,00 |
| Porta blindata per Sala Server | | € 4.000,00 | € 4.000,00 |
| Manodopera, comprende IVA | | | |
| Sopralluogo e progettazione, pentest, architettura di rete | 230 | € 50,00 | € 11.500,00 |
| Configurazione Firewall | 12 | € 50,00 | € 600,00 |
| Installazione accesso biometrico e porta blindata | 4 | € 50,00 | € 200,00 |
| Manodopera operai per installazioni | 16 | € 50,00 | € 800,00 |
| Prezzo totale del preventivo | | | ~~€ 21.800,00~~ **€ 21.500,00** |
| include assistenza ordinaria post-vendita Annuale, 2 anni | | | Gratuita |

| | | | |
|---|---|---|---|
| Eventuali optional | | | |
| Corso sicurezza informatica anti-phishing per N° dipendenti | 30 | € 100,00 | € 3.000,00 |
| Servizio VPN, ***piano annuale***, N° dipendenti | 30 | € 240,00 | € 7.200,00 |
| Configurazione VPN | 8 | € 50,00 | € 400,00 |
| Assistenza straordinaria Giornaliero, Feriale, in loco, dalle 8 alle 20 | | € 100,00 | € 100,00 |
| Assistenza straordinaria, festiva/notturna Giornaliero, Festivo, in loco, dalle 8 alle 20 | | € 200,00 | € 200,00 |