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

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

Scaletta del progetto

18 marzo 2024

- Overview del progetto
- Configurazione DVWA e Metasploit2
- Bozza su Packet Tracer
- Creazione di Vulnerability/Port Scanner
- Abilitazione metodi HTTP su porte necessarie

19 marzo 2024

- Finalizzazione schema Packet Tracer
- Esecuzione test bruteforce
- Sviluppo codice a scopo di bruteforce

20 marzo 2024

- Preventivo per aziende
- Penetration Testing
- Scrittura estensiva della documentazione e report di sicurezza

21 marzo 2024

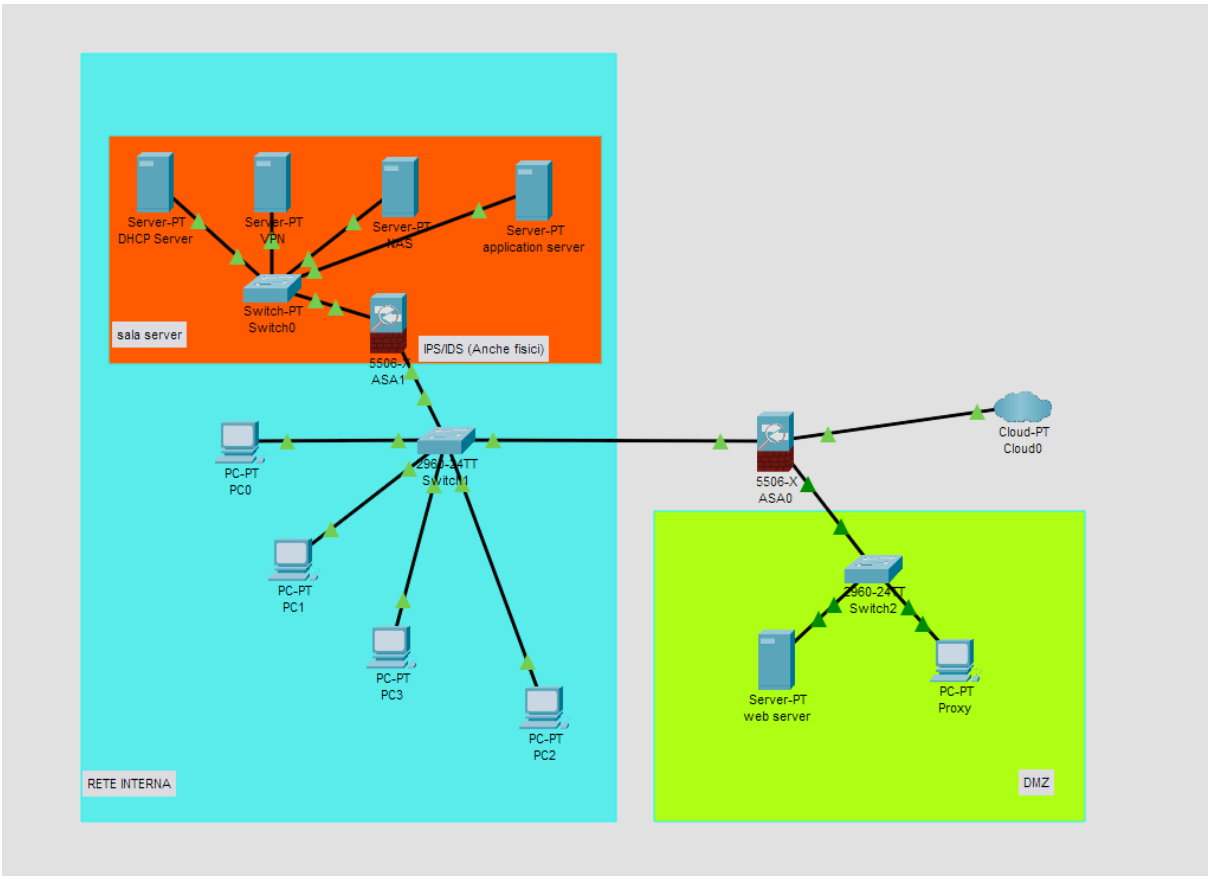
- Ottimizzazione degli applicativi

22 marzo 2024

- Revisione finale del progetto e presentazione

18 marzo 2024

Ci siamo approcciati al progetto abbozzando uno schema su Cisco Packet Tracer, tenendo conto di diversi punti chiave, quali: presenza di Web Server che si connette ad Internet e un Application Server isolato accessibile solamente da Intranet.
Prima di tutto, l'Application Server dovrebbe essere posto dentro una sala dedicata, con accesso limitato, solamente agli addetti autorizzati, fisicamente e virtualmente.
Per continuare, il Web Server andrà invece piazzato all'esterno della Intranet, in un'apposita DMZ (Demilitarized Zone). Qui, il traffico in entrata e uscita passa per un proxy, per garantire un ulteriore livello di sicurezza.



Oggi abbiamo anche scritto un Port Scanner che utilizzeremo nei Penetration Test del 20 marzo. Sarà in futuro disponibile alla verifica nelle nostre repository.

```python
import socket

target = input("inserisci indirizzo IP da scansire:")
portrange = input("inserisci il port range da scansire (di default scansiona tutte le porte):")



if (portrange == ""):
    lowport = 0
    highport = 65535
else:
    lowport = int(portrange.split('-')[0])
    highport = int(portrange.split('-')[1])



print("scan host", target, "dalla porta", lowport, "alla porta", highport)

porte_aperte = []

for port in range(lowport, highport + 1):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(0.00000001)
    status = s.connect_ex((target, port))
    if status == 0:
        print(" ***  PORTA" , port, " APERTA ***")
        porte_aperte.append(port)
    else:
        print('- PORTA', port,  " CHIUSA")
    s.close()

if porte_aperte:
    print("\nRiepilogo porte aperte: ", porte_aperte)
else:
    print("\nnessuna porta aperta trovata")
```

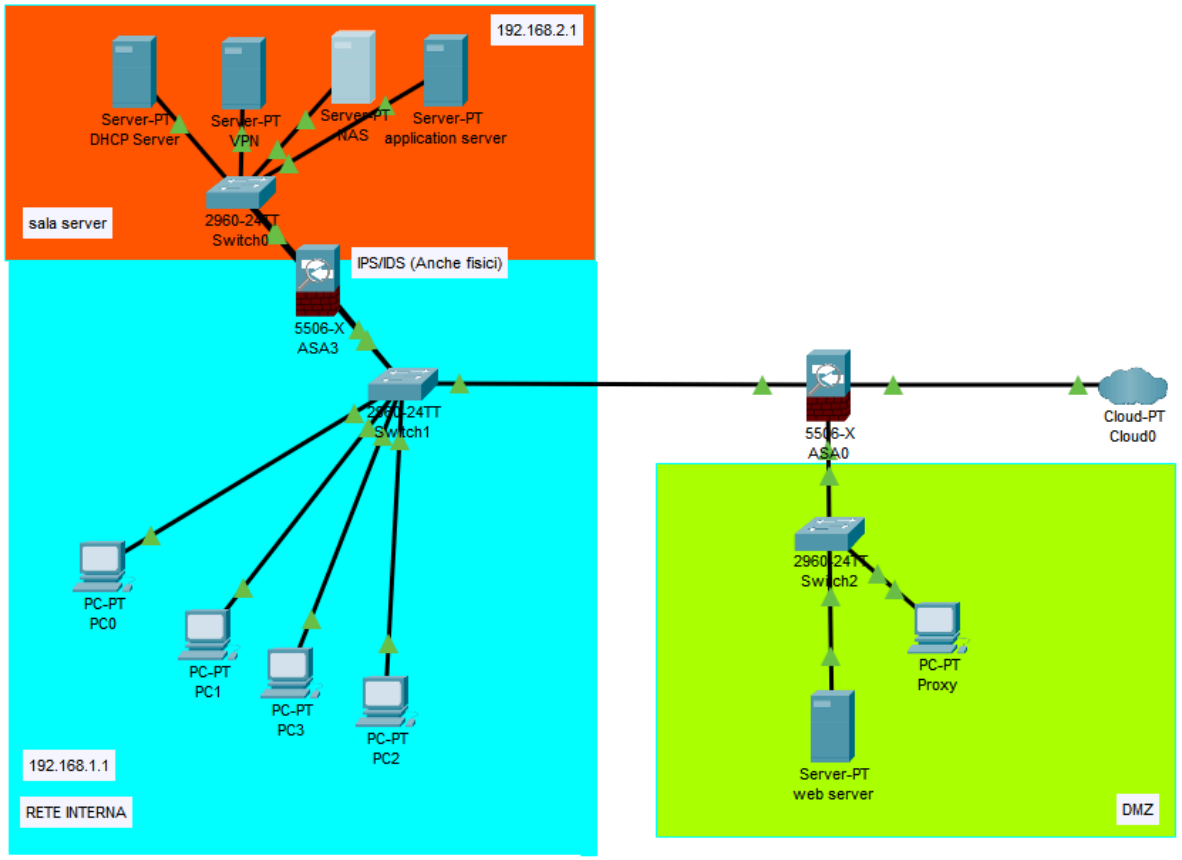
Potrà essere implementato anche questo tool compilato oggi, a scopo di verifica dei metodi HTTP abilitati.

```python
import http.client

host = input("Inserire Host/IP del sistema target: ")
port = input("Inserire la porta del sistema target (default: 80): ")
path = input("Inserire path da controllare (default /): ").strip()

if (port == ""):
        port = 80
else:
        port = int(port)

if (path == ""):
        path = "/"

try:
        connection = http.client.HTTPConnection(host, port)
        connection.request("OPTIONS", path)
        response = connection.getresponse()
        print("Lo status e' : ", response.status)
        if response.status in (301,302,303,307,308):
                redirect = response.getheader("Location")
                print(f"Reindirizzamento ({response.status}) a: {redirect}")
        else:
                methods_enabled = response.getheader("allow")
                print("I metodi abilitati sono: ", methods_enabled)
        connection.close()
except ConnectionRefusedError:
        print("Connessione Fallita")
```

Nei prossimi giorni, prepareremo il tool per eseguire test di tipo Bruteforce sul sito, a scopo di rafforzare la sicurezza e informare i dipendenti su pratiche di sicurezza base.
Il codice è ancora in lavorazione e manca di commenti e della dovuta documentazione, che verrà scritta nei giorni a seguire, per essere quindi revisionata, il giorno prima della consegna.

19 marzo 2024

Considerando le necessità dell'azienda e calcolando il rischio, il team ha notato la necessità della pianificazione di un preventivo. Questo verrà stilato insieme al report finale nei prossimi giorni.
Oggi abbiamo potuto confermare la progettazione su Cisco Packet Tracer, effettuando le ultime modifiche per rendere la presentazione più pulita, e aumentando l'utilità del DHCP.



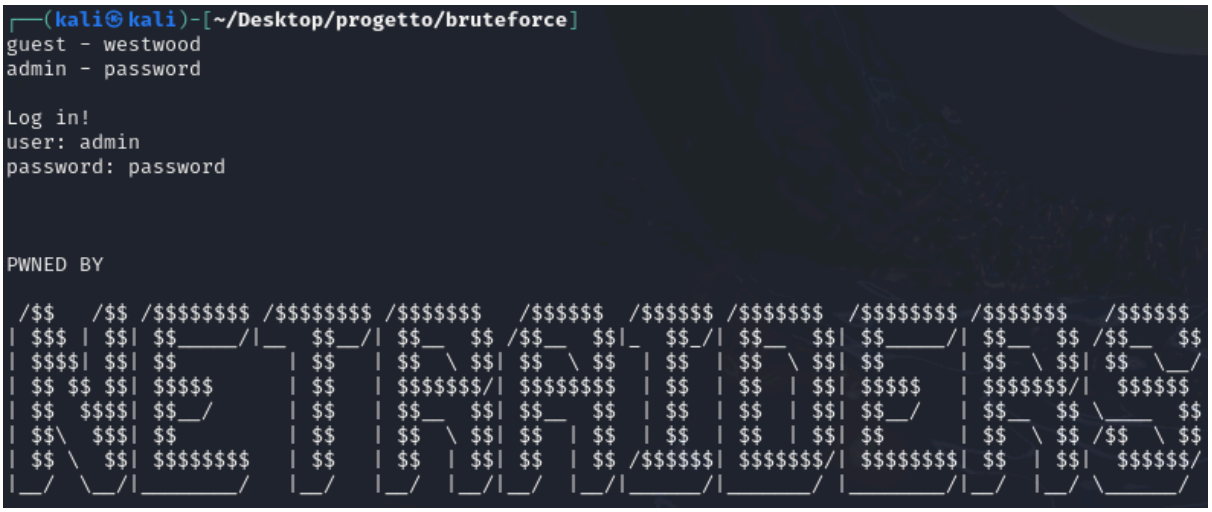
Lo script di bruteforce che stavamo preparando ha dato esiti positivi, dopo diversi bug fixes e ottimizzazioni. Sia il phpMyAdmin che il DVWA/Vulnerabilities sono stati penetrati impostando la complessità della sicurezza sia a Low, che ad High, tramite diversi exploit, consultabili direttamente sul codice .py.
Segue una breve dimostrazione dell'effetto del codice.

Bruteforce su phpMyAdmin:

```
┌──(kali㉿kali)-[~/Desktop/progetto/bruteforce]
guest -

Log in!

user: guest
password:



PWNED BY

 /$$   /$$ /$$$$$$$$ /$$$$$$$$ /$$$$$$$   /$$$$$$  /$$$$$$ /$$$$$$$  /$$$$$$$$ /$$$$$$$   /$$$$$$
| $$$ | $$| $$_____/|__  $$__/| $$__  $$ /$$__  $$|_  $$_/| $$__  $$| $$_____/| $$__  $$ /$$__  $$
| $$$$| $$| $$         | $$   | $$  \ $$| $$  \ $$  | $$  | $$  \ $$| $$      | $$  \ $$| $$  \__/
| $$ $$ $$| $$$$$      | $$   | $$$$$$$/| $$$$$$$$  | $$  | $$  | $$| $$$$$   | $$$$$$$/|  $$$$$$
| $$  $$$$| $$__/      | $$   | $$__  $$| $$__  $$  | $$  | $$  | $$| $$__/   | $$__  $$ \____  $$
| $$\  $$$| $$         | $$   | $$  \ $$| $$  | $$  | $$  | $$  | $$| $$      | $$  \ $$ /$$  \ $$
| $$ \  $$| $$$$$$$$   | $$   | $$  | $$| $$  | $$ /$$$$$$| $$$$$$$/| $$$$$$$$| $$  | $$|  $$$$$$/
|__/  \__/|________/   |__/   |__/  |__/|__/  |__/|______/|_______/ |________/|__/  |__/ \______/
```

Bruteforce su DVWA:

Bruteforce su DVWA_Vulnerabilities:



Come si può vedere, il software creato funziona con successo.
Per i prossimi giorni, abbiamo in programma di espandere gli script, implementando dei commenti, per rendere più leggibile il codice, in modo che sia consultabile prima dell'esecuzione. Il preventivo avrà come focus l'acquisto di materiale per la sicurezza dell'azienda, includendo anche delle slide a scopo informativo, per rafforzare la comprensione delle basi di sicurezza degli Utenti base, non addetti al settore IT.

20 marzo 2024

Oltre ad abbozzare le prime righe di documentazione, 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 inserita 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.

Riguardo invece la documentazione del programma, il team si è dedicato all'espansione del codice in modo da avere una UX invasiva al minimo, ma informando l'Utente sul processo in esecuzione, quale bruteforce in corso (vengono mostrate le credenziali utilizzate durante l'attacco) e descrizione delle porte accessibili. Segue una tabella delle porte trovate aperte. Le porte evidenziate, risultano libere e non fanno riferimento a porte well-known.

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	

Abbiamo inoltre proseguito nella scrittura dei commenti per facilitare la navigazione e la leggibilità del codice sorgente utilizzato nei pentest.

```
34
35          #nel riepilogo porte, abbiamo inserito anche la destinazione della porta. se non è una well-known port, stampa solo il numero
    della porta.
36              stringa_porte = f"{port} ( {socket.getservbyport(port)} )"
37          except:
38              stringa_porte = f"{port}"
39
40              #ogni porta aperta, va ad aggiornare il file porte_aperte
41          porte_aperte.append(stringa_porte)
42      else:
43
44          #se lo status non è 0, la porta è chiusa con relativo messaggio
45          print('- PORTA', port,  " CHIUSA")
46
47          #chiusura socket
48      s.close()
```

Di seguito, lasciamo una versione quasi finale del preventivo per l'azienda.

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			
Servizio VPN, ***piano annuale***, num. 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