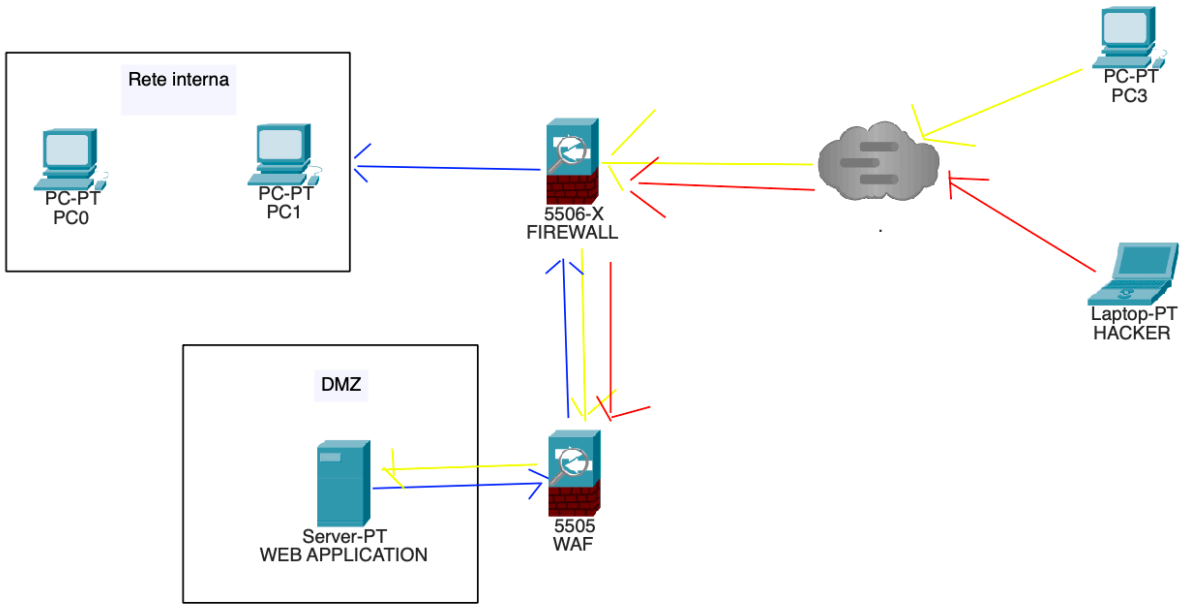
REPORT SETTIMANA 9

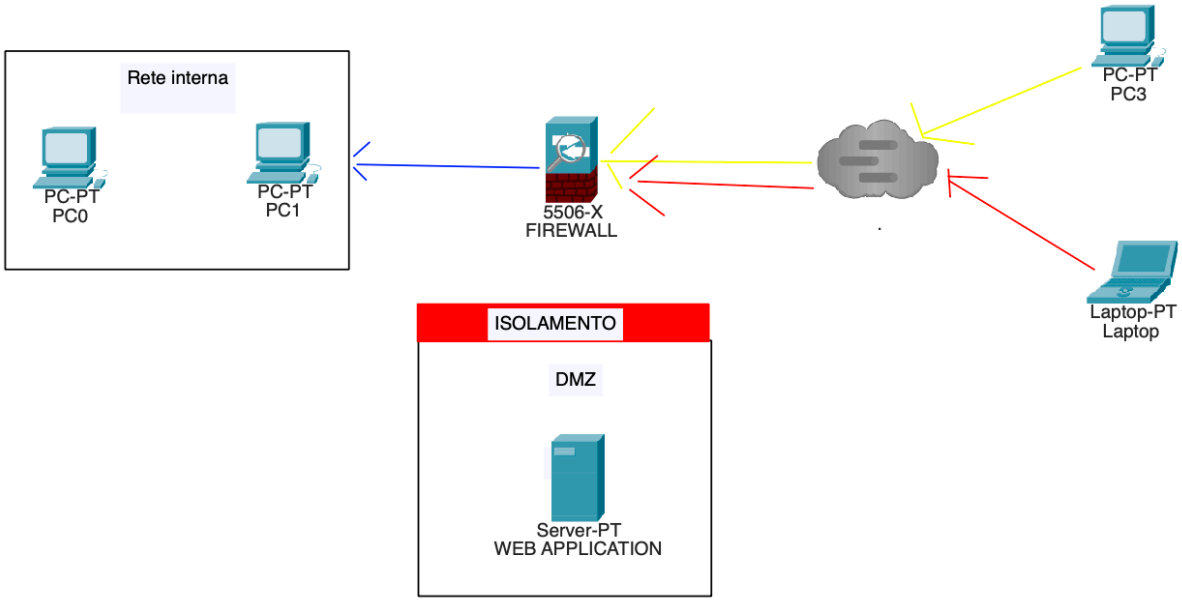
Esercizio 1: Azioni preventive



Nel primo esercizio veniva richiesto di implementare delle misure di sicurezza per impedire attacchi di tipo XSS e SQLi ad un e-commerce.
Come prima cosa ho inserito un Web Application Firewall, un tipo di firewall che può aiutare a rilevare e bloccare gli attacchi XSS e SQL injection creando una barriera tra l'e-commerce e potenziali malintenzionati.
Altre contromisure da adottare sono:

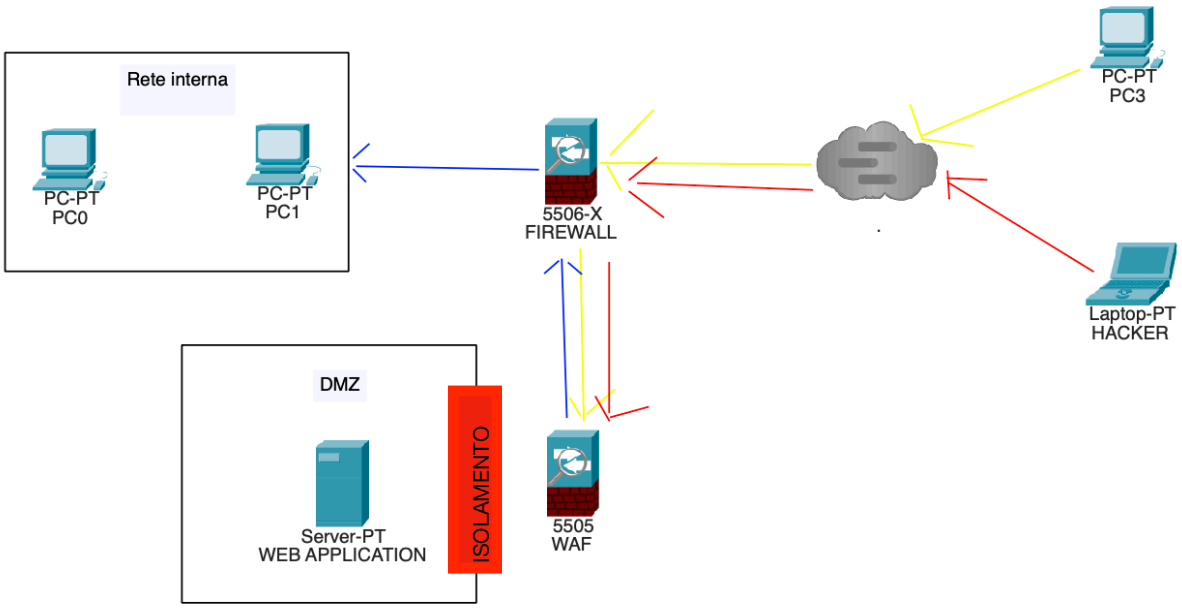
- Validazione e sanitizzazione dei dati in input
- Escape dei caratteri speciali
- Limitazione dei privilegi del database

Esercizio 3



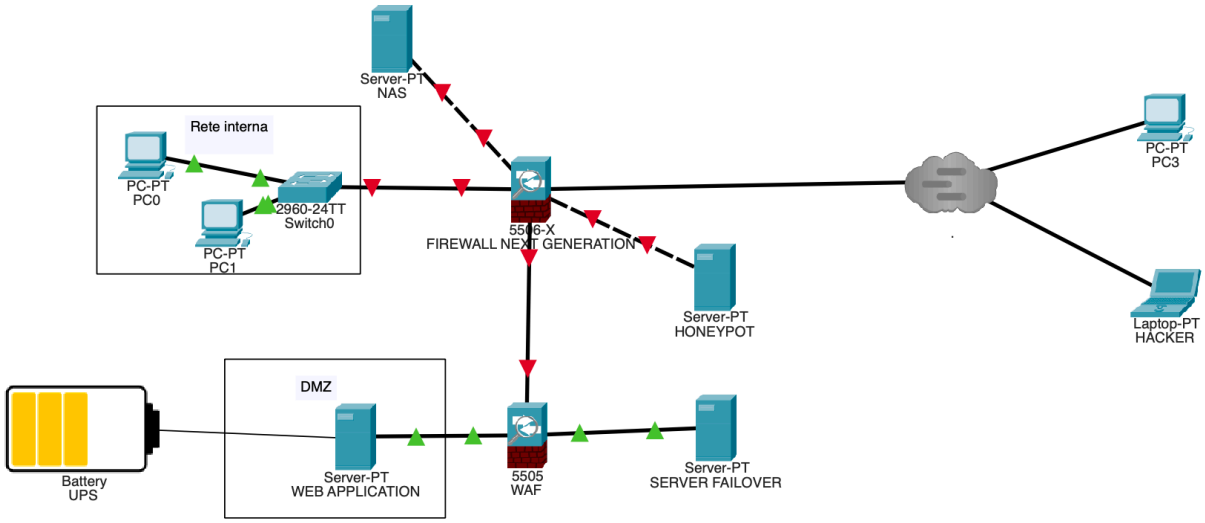
Nel terzo esercizio veniva richiesto di attuare delle risposte ad un attacco malware all'e-commerce.
La prima azione da intraprendere è l'isolamento del sistema compromesso, sia dalla rete interna per evitare il propagarsi del malware nella rete aziendale, sia da internet per evitare la divulgazione di informazioni sensibile attraverso la rete.
Dopodiché bisogna analizzare il malware, rimuoverlo completamente, controllare gli altri sistemi, ripristinare il sistema compromesso e i backup e verificare i danni subiti.

Esercizio 4



Nel quarto esercizio veniva chiesto di unire i due disegni dei punti 1 e 3.

Esercizio 5



Nel quinto punto veniva richiesto di implementare misure di sicurezza aggiuntive per rendere maggiormente sicura l'infrastruttura.
Per rendere l'infrastruttura sicura bisognerebbe effettuare le seguenti modifiche:

- Firewall di nuova generazione con IDS integrato per controllare eventuali utenti malevoli.
- Honeypot per attirare eventuali attacchi e studiarli.
- Server Failover, un server configurato per entrare in funzione nel caso il server principale su cui gira l'e-commerce non sia raggiungibile.
- UPS per fare in modo che il l'e-commerce sia raggiungibile anche in caso di mancanza di corrente.
- NAS per programmare ed effettuare backup nel modo più efficiente possibile.

Esercizio 2

Nell’esercizio 2 veniva richiesto di analizzare il contenuto di due link.
Dopo aver inserito i link su Virus Total e aver visto che erano link reindirizzanti a “any.run” li ho aperti e analizzati uno alla volta.

Link 1:

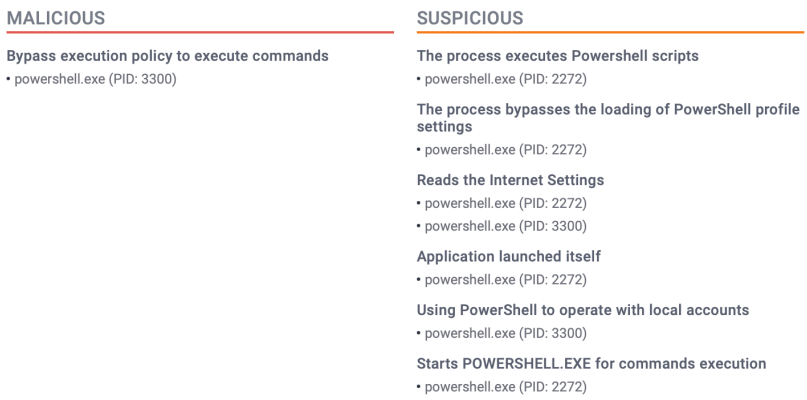
Il primo link riportava ad una pagina any.run che mostrava il funzionamento del seguente codice:

```
if (!([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole] "Administrator")) {
Start-Process powershell.exe "-NoProfile -ExecutionPolicy Bypass -File `"$PSCommandPath`"" -Verb RunAs; exit }
Write-Host ""
Write-Host "Change DNS Server Settings for Wi-Fi"
Write-Host ""
Write-Host "Enter your Choice: "
Write-Host "1. AdGuard DNS"
Write-Host "2. AdGuard Family Protection DNS"
Write-Host "3. Reset DNS to default"
Write-Host "0. Exit"
Write-Host ""
$Input = Read-Host -Prompt 'Input your choice'
Write-Host ""
if($Input -eq 1){
   Set-DnsClientServerAddress -InterfaceAlias Wi-Fi -ServerAddresses "94.140.14.14","94.140.15.15"
   write-host("AdGuard DNS enabled.")
   Start-Sleep -s 1
}elseif($Input -eq 2){
   Set-DnsClientServerAddress -InterfaceAlias wi-fi -ServerAddresses "94.140.14.15","94.140.15.16"
   write-host("AdGuard Family DNS enabled.")
   Start-Sleep -s 1
}elseif($Input -eq 3){
   Set-DnsClientServerAddress -InterfaceAlias wi-fi -ResetServerAddresses
   write-host("DNS Reset")
   Start-Sleep -s 1
}elseif($Input -eq 0){
   Break
}else {
   write-host("Wrong Input")
   Start-Sleep -s 1
   Break
}
```

Come possiamo notare il codice inizialmente controlla i privilegi dell’utente e nel caso non possieda i privilegi di amministratore avvia una PowerShell con privilegi di amministratore.
Dopodiché chiede all’utente di scegliere tra quattro possibili azioni:

- e l'utente inserisce "1", vengono impostati gli indirizzi del server DNS su "94.140.14.14" e "94.140.15.15" per l'interfaccia Wi-Fi.
- Se l'utente inserisce "2", vengono impostati gli indirizzi del server DNS su "94.140.14.15" e "94.140.15.16" per l'interfaccia Wi-Fi.
- Se l'utente inserisce "3", vengono ripristinati gli indirizzi del server DNS predefiniti per l'interfaccia Wi-Fi.
- Se l'utente inserisce "0", lo script viene interrotto.
- Se l'utente inserisce qualsiasi altra scelta, viene visualizzato un messaggio di errore.

Questo codice è scritto per modificare le impostazioni del server DNS per l'interfaccia Wi-Fi sulla macchina in cui viene eseguito, consentendo all'utente di selezionare tra diverse opzioni di server DNS e dal report testuale di any.run possiamo vedere per quale motivo questo script è da considerare malevolo.



Link 2:

Il secondo link riportava ad una pagina any.run che mostrava il funzionamento di un malware di tipo REMCOS, un malware di tipo RAT (Remote Administration Tool) che viene utilizzato per il controllo remoto non autorizzato della macchina vittima. Il nome "REMCOS" deriva proprio dalla sua funzionalità principale di fornire funzionalità di amministrazione remota.
Come possiamo notare dal report testuale di any.run questo malware impatta maggiormente il sistema vittima rispetto al semplice script di prima:

MALICIOUS

Application was dropped or rewritten from another process
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Starts Visual C# compiler
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

Uses Task Scheduler to run other applications
- cmd.exe (PID: 3604)
- cmd.exe (PID: 3200)
- cmd.exe (PID: 2628)
- cmd.exe (PID: 2960)

Remcos is detected
- csc.exe (PID: 3824)

REMCOS detected by memory dumps
- csc.exe (PID: 3824)

SUSPICIOUS

The process creates files with name similar to system file names
- WinRAR.exe (PID: 1944)

Drops a system driver (possible attempt to evade defenses)
- WinRAR.exe (PID: 1944)
- procexp.exe (PID: 3476)

Reads settings of System Certificates
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Reads security settings of Internet Explorer
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Reads the Internet Settings
- Autoruns.exe (PID: 4056)
- csc.exe (PID: 3824)

Connects to unusual port
- csc.exe (PID: 3824)

Starts CMD.EXE for commands execution
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

Writes files like Keylogger logs
- csc.exe (PID: 3824)

Checks Windows Trust Settings
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Executable content was dropped or overwritten
- procexp.exe (PID: 3476)

E attiva un numero maggiore di processi:

Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
138	74	7	1