LAN AZIENDALE

Report sulla sicurezza

Breve analisi, ad uso interno, sullo stato di sicurezza della rete aziendale e delle modalità di monitoraggio

UFFICIO SERVIZI INFORMATICI

1. PREMESSA

Il perimetro della *LAN* aziendale deve essere posto in condizione di sicurezza massima, il che si traduce nel tenere la rete interna separata da *internet*, mediante l'utilizzo continuo di appositi *software* e *hardware* (*Firewall* e *IdS*) che rendano invisibili le risorse aziendali interne e, nel contempo, prevengano attacchi informatici dall'esterno.

2. PENETRATION TEST

L'attività di ***penetration test*** consiste nel verificare l'esistenza di eventuali "falle" e/o criticità esterne/interne della rete aziendale, che consentano a eventuali malintenzionati di mettere a rischio l'integrità dei dati.

2.1 FALLE E/O CRITICITÀ DALL'ESTERNO

Questa tipologia di eventi può essere originata dalla mancanza di aggiornamento di *software e\o hardware* dei sistemi di sicurezza, o anche dalla presenza di *bug* del software che rendano agevole la penetrazione dall'esterno nella *LAN* aziendale mediante appositi *virus* o *worm*.

2.2 FALLE E/O CRITICITÀ DALL'INTERNO

Questa tipologia di eventi può essere originata dalla mancanza di aggiornamento di *software e\o hardware* dei sistemi di sicurezza, o anche dalla presenza di *bug* del software, che rendono agevole l'inoculazione nella *LAN* aziendale, attraverso la posta elettronica, di *worm* e *virus ransomware.*

3. NETWORK AZIENDALE

Il *network* è strutturato con 2 *firewall*:

- esterno (Zyxell);
- interno (Forefront Tmg Microsoft).

La LAN interna è, in buona sostanza, "nascosta" dietro altre 2 reti, pertanto gli operatori interni, qualora navighino in *internet*, devono necessariamente passare attraverso un *proxy-server* che maschera gli indirizzi e di conseguenza blocca la trasmissione di eventuali *worm* verso l'esterno.

4. TIPOLOGIA E TEMPI DELL'INTERVENTO

L'attività di **penetration test** viene svolta almeno una volta al mese mediante l'utilizzo dei seguenti strumenti informatici[1]

- NMAP
- ZENMAP
- CAIN
- BACKBOX
- METASPLOIT
- KALI LINUX

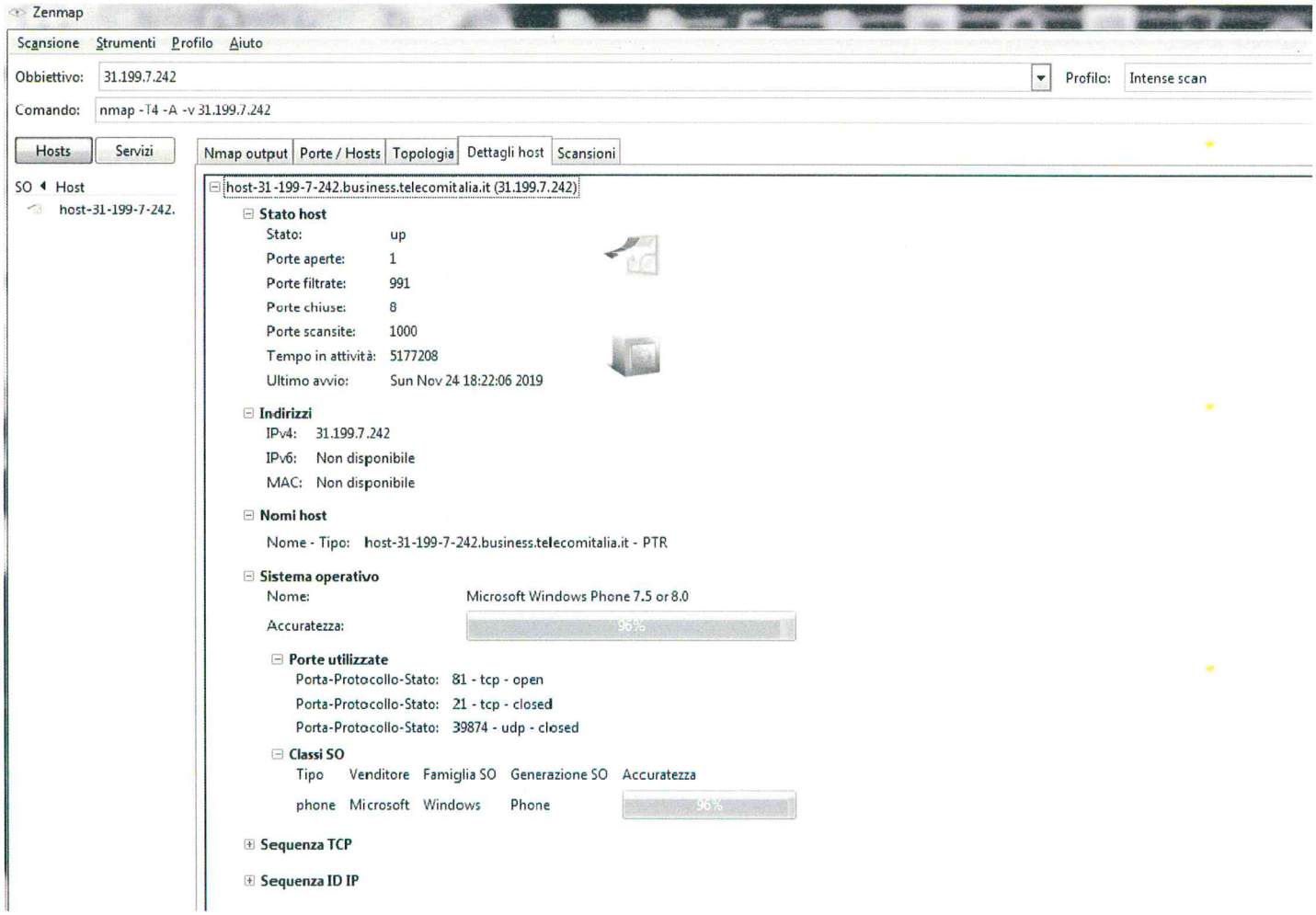
Nell'eventualità dall'analisi condotta emergano delle criticità, viene effettuato tempestivamente un intervento mediante l'applicazione di aggiornamenti e *patch* di sicurezza e/o eventuali modifiche delle *policy* di sicurezza aziendale.

[1] I software in questione sono quelli maggiormente utilizzati nel campo sella sicurezza informatica e nell'*ethical hacking.*

4.1 TEST *FIREWALL* DEL 23 GENNAIO 2020 – ESTERNO VS LAN

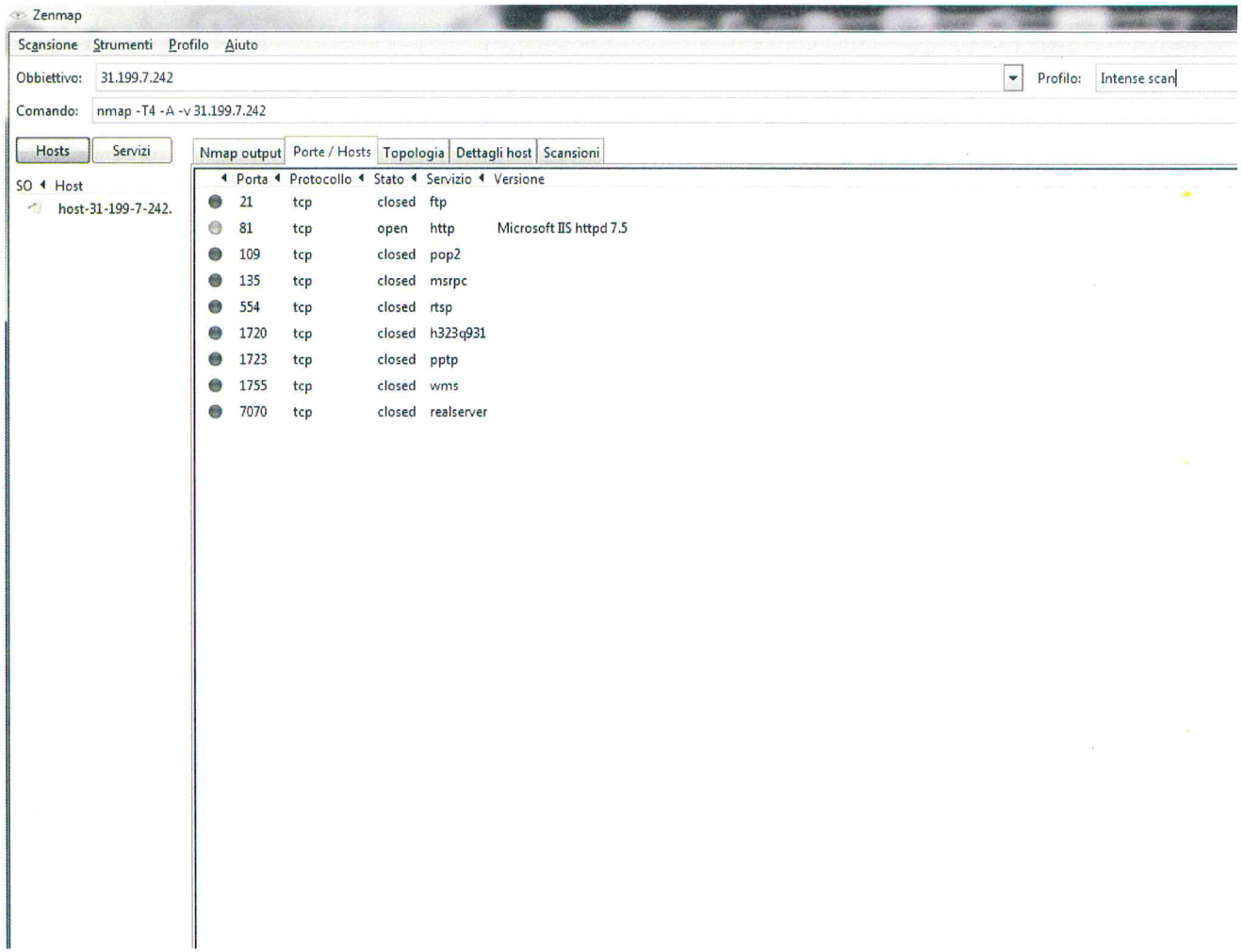
Di seguito si elencano brevemente i risultati dei recenti test eseguiti sulla rete Enpapi.

Figura 1: NMAP – report accuratezza



In figura 1 è possibile leggere il livello di accuratezza *firewall* Zyxell pari al **96%** e la **chiusura di tutte le porte** del Firewall Zyxell da esterno

Figura 2: NMAP – dettaglio porte TCP



In figura 2 il *software* NMAP evidenzia il dettaglio delle porte TCP, da cui si può evincere che unicamente la TCP 81 (insieme con HTTPS 443), risulta correttamente in stato *"open"*, in quanto utilizzata per la gestione remota del *firewall.*

4.2 TEST *FIREWALL* DEL 23 GENNAIO 2020 – LAN VS ESTERNO

Il report che segue è copiato dall'OUTPUT del software NMAP che analizza le porte TCP dall'interno verso l'esterno. Dall'analisi condotta si evince che le porte dei protocolli principali TCP risultano "crittografate" (*STATE filtered*)

TEST FIREWALL 31.199.7.242

Starting Nmap 7.70 (https://nmap.org) at 2020-01-23 15:08 UTC

Nmap scan report for host242-7-static.199-31-b.business.telecomitalia.it (31.199.7.242)

Host is up (0.11s latency).

PORT STATE SERVICE

21/tcp filtered ftp

22/tcp filtered ssh

23/tcp filtered telnet

80/tcp filtered http

110/tcp filtered pop3

143/tcp filtered imap

443/tcp open https

3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.36 seconds

4.3 AREA RISERVATA

Il report che segue, ottenuto con il *software* ZENMAP, mostra il livello di sicurezza dell'area riservata:

Normalized URL:	http://areariservata.enpapi.it:80
Submission date:	Thu Jan 23 16:24:10 2020
Server IP address:	31.199.7.253
Country:	Italy
Malicious files:	0
Suspicious files:	0
Potentially Suspicious files:	0
Clean files:	0
External links detected:	32
Iframes scanned:	0
Blacklisted:	No

Dalla lettura della tabella in questione risulta l'assenza di *file* sospetti (valore 0 in corrispondenza delle "minacce") o potenzialmente infetti.

5. CONCLUSIONI

Dall'analisi dei risultati ottenuti è possibile dedurre che la sicurezza della rete aziendale è costantemente monitorata mediante il controllo attivo del traffico dati in entrata e in uscita.

6. ALLEGATO 1: LOG COMPLETO NMAP

```
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-23 16:27 ora solare Europa occidental

NSE: Loaded 148 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 16:27

Completed NSE at 16:27, 0.00s elapsed

Initiating NSE at 16:27

Completed NSE at 16:27, 0.00s elapsed

Initiating Parallel DNS resolution of 1 host. at 16:27

Completed Parallel DNS resolution of 1 host. at 16:27, 0.00s elapsed

Initiating SYN Stealth Scan at 16:27

Scanning host-31-199-7-242.business.telecomitalia.it (31.199.7.242) [1000 ports]

Discovered open port 81/tcp on 31.199.7.242

Completed SYN Stealth Scan at 16:28, 32.95s elapsed (1000 total ports)

Initiating Service scan at 16:28

Scanning 1 service on host-31-199-7-242.business.telecomitalia.it (31.199.7.242)

Completed Service scan at 16:28, 6.02s elapsed (1 service on 1 host)

Initiating OS detection (try #1) against host-31-199-7-242.business.telecomitalia.it (31

Retrying OS detection (try #2) against host-31-199-7-242.business.telecomitalia.it (31.1

Retrying OS detection (try #3) against host-31-199-7-242.business.telecomitalia.it (31.1

Retrying OS detection (try #4) against host-31-199-7-242.business.telecomitalia.it (31.1

Retrying OS detection (try #5) against host-31-199-7-242.business.telecomitalia.it (31.1

Initiating Traceroute at 16:28
```

Completed Traceroute at 16:28, 1.02s elapsed

Initiating Parallel DNS resolution of 3 hosts. at 16:28

Completed Parallel DNS resolution of 3 hosts. at 16:28, 0.02s elapsed

NSE: Script scanning 31.199.7.242.

Initiating NSE at 16:28

Completed NSE at 16:28, 0.10s elapsed

Initiating NSE at 16:28

Completed NSE at 16:28, 0.00s elapsed

Nmap scan report for host-31-199-7-242.business.telecomitalia.it (31.199.7.242)

Host is up (0.21s latency).

Not shown: 991 filtered ports

PORT STATE SERVICE VERSION

21/tcp closed ftp

81/tcp open http Microsoft IIS httpd 7.5

| http-methods:

| Supported Methods: OPTIONS TRACE GET HEAD POST

|_ Potentially risky methods: TRACE

|_http-server-header: Microsoft-IIS/7.5

|_http-title: IIS7

109/tcp closed pop2

135/tcp closed msrpc

554/tcp closed rtsp

1720/tcp closed h323q931

1723/tcp closed pptp

1755/tcp closed wms

7070/tcp closed realserver

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org

TCP/IP fingerprint:

OS:SCAN(V=7.70%E=4%D=1/23%OT=81%CT=21%CU=39874%PV=N%DS=3%DC=T%G=Y%TM=5E29BB

OS:B6%P=i686-pc-windows-windows)SEQ(SP=101%GCD=1%ISR=109%TI=I%TS=7)OPS(O1=M

OS:5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST11%O5=M5B4NW8ST11%

OS:O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%

OS:DF=Y%T=7E%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=7E%S=O%A=S+%F=AS%RD=

OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=82%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)

OS:T5(R=N)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=41%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%

OS:RUCK=7AF2%RUD=G)IE(R=N)

Uptime guess: 59.921 days (since Sun Nov 24 18:22:06 2019)

Network Distance: 3 hops

TCP Sequence Prediction: Difficulty=261 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 1723/tcp)

HOP RTT ADDRESS

1 53.00 ms 192.168.50.1

2 0.00 ms 192.168.50.254

3 1.00 ms host-31-199-7-242.business.telecomitalia.it (31.199.7.242)

NSE: Script Post-scanning.

Initiating NSE at 16:28

Completed NSE at 16:28, 0.00s elapsed

Initiating NSE at 16:28

Completed NSE at 16:28, 0.00s elapsed

Read data files from: C:\Program Files (x86)\Nmap

OS and Service detection performed. Please report any incorrect results at https://nmap.

Nmap done: 1 IP address (1 host up) scanned in 65.33 seconds

Raw packets sent: 2188 (102.634KB) | Rcvd: 146 (12.930KB)

Starting Nmap 7.70 (https://nmap.org) at 2020-01-24 12:30 ora solare Europa occidentale

NSE: Loaded 148 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 12:30

Completed NSE at 12:30, 0.00s elapsed

Initiating NSE at 12:30

Completed NSE at 12:30, 0.00s elapsed

Initiating Ping Scan at 12:30

Scanning 31.199.7.242 [4 ports]

Completed Ping Scan at 12:30, 0.34s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 12:30

Completed Parallel DNS resolution of 1 host. at 12:30, 0.08s elapsed

Initiating SYN Stealth Scan at 12:30

Scanning host242-7-static.199-31-b.business.telecomitalia.it (31.199.7.242) [1000 ports]

Discovered open port 443/tcp on 31.199.7.242

Discovered open port 80/tcp on 31.199.7.242

Completed SYN Stealth Scan at 12:30, 12.04s elapsed (1000 total ports)

Initiating Service scan at 12:30

Scanning 2 services on host242-7-static.199-31-b.business.telecomitalia.it (31.199.7.242)

Completed Service scan at 12:33, 152.80s elapsed (2 services on 1 host)

Initiating OS detection (try #1) against host242-7-static.199-31-b.business.telecomitalia.Retrying OS detection (try #2) against host242-7-static.199-31-b.business.telecomitalia.Initiating Traceroute at 12:33

Completed Traceroute at 12:33, 3.12s elapsed

Initiating Parallel DNS resolution of 12 hosts. at 12:33

Completed Parallel DNS resolution of 12 hosts. at 12:33, 0.07s elapsed

NSE: Script scanning 31.199.7.242.

Initiating NSE at 12:33

Completed NSE at 12:34, 73.80s elapsed

Initiating NSE at 12:34

Completed NSE at 12:34, 3.13s elapsed

Nmap scan report for host242-7-static.199-31-b.business.telecomitalia.it (31.199.7.242)

Host is up (0.055s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http?

443/tcp open ssl/http ZyXEL ZyWALL http config

|_http-favicon: Unknown favicon MD5: 9FBBFD393A734A290AFE46EA03CE7FF6

| http-methods:

|_ Supported Methods: GET HEAD POST OPTIONS

|_http-server-header: <empty>

|_http-title: ZyWALL USG 300

|_http-trane-info: Problem with XML parsing of /evox/about

| ssl-cert: Subject: commonName=usg300_B0B2DCC44A53

| Subject Alternative Name: email:usg300_B0B2DCC44A53

| Issuer: commonName=usg300_B0B2DCC44A53

| Public Key type: rsa

| Public Key bits: 1024

| Signature Algorithm: sha1WithRSAEncryption

| Not valid before: 2012-09-21T00:00:18

| Not valid after: 2032-09-16T00:00:18

| MD5: 557e e456 437c ae99 83b5 02cf bea1 4020

|_SHA-1: 9568 80a7 0860 8238 027f a1cb 1c77 f184 5871 cba1

|_ssl-date: 2020-01-24T11:33:38+00:00; 0s from scanner time.

| sslv2:

| SSLv2 supported

|_ ciphers: none

Warning: OSScan results may be unreliable because we could not find at least 1 open and Device type: general purpose|firewall|storage-misc

Running (JUST GUESSING): Linux 2.6.X|3.X (90%), WatchGuard Fireware 11.X (89%), Synology OS CPE: cpe:/o:linux:linux_kernel:2.6.39 cpe:/o:linux:linux_kernel:3.10 cpe:/o:watchguard:Aggressive OS guesses: Linux 2.6.39 (90%), Linux 2.6.32 (89%), Linux 3.10 (89%), WatchGuard No exact OS matches for host (test conditions non-ideal).

Uptime guess: 3.385 days (since Tue Jan 21 03:19:54 2020)

Network Distance: 18 hops

TCP Sequence Prediction: Difficulty=261 (Good luck!)

IP ID Sequence Generation: All zeros

Service Info: Device: security-misc

TRACEROUTE (using port 443/tcp)

HOP RTT ADDRESS

1 5.00 ms 192.168.43.1

2 ...

3 46.00 ms 10.128.76.77

4 50.00 ms 10.128.76.14

5 54.00 ms 10.128.76.236

6 58.00 ms 10.128.76.1

7 60.00 ms 10.176.18.122

8 46.00 ms 83.224.40.197

9 55.00 ms 83.224.40.217

10 59.00 ms 83.224.40.230

11 54.00 ms 83.224.46.141

12 ... 16

17 50.00 ms host-31-199-56-110.business.telecomitalia.it (31.199.56.110)

18 47.00 ms host242-7-static.199-31-b.business.telecomitalia.it (31.199.7.242)

NSE: Script Post-scanning.

Initiating NSE at 12:34

Completed NSE at 12:34, 0.00s elapsed

Initiating NSE at 12:34

Completed NSE at 12:34, 0.01s elapsed

Read data files from: D:\Nmap

OS and Service detection performed. Please report any incorrect results at https://nmap.Nmap done: 1 IP address (1 host up) scanned in 267.04 seconds

Raw packets sent: 2135 (99.156KB) | Rcvd: 82 (4.612KB.