Relazione Tecnica

Network Assessment

Pippo
Caserta

Sommario

1 I VOSTRI INTERLOCUTORI

Nome	Funzione	Dettagli

2 PREMESSA

Con l'aumento delle notizie riportate dai media sulla diffusione di programmi software dannosi tramite Internet, le minacce esterne hanno assunto un'importanza sempre maggiore nelle strategie di protezione delle risorse di rete delle organizzazioni. Tuttavia, alcune delle minacce più pericolose per l'infrastruttura di un'organizzazione sono costituite dagli attacchi provenienti dalla rete interna.
Gli attacchi interni che potrebbero causare potenzialmente i danni maggiori sono quelli risultanti dalle attività di persone a cui sono assegnati i privilegi più alti, ad esempio gli amministratori di rete, o di una non adeguata configurazione dei sistemi di rete che consentono l'accesso ad informazioni pubbliche che non devono essere accedute.
Per le organizzazioni che hanno l'obbligo di rispettare determinati vincoli normativi, il monitoraggio della rete è un fattore essenziale. Con l'aumentare dei requisiti normativi richiesti da numerose istituzioni a livello mondiale, le organizzazioni hanno la necessità di effettuare un monitoraggio delle reti interne, controllare il possibile accesso alle risorse nonché individuare gli utenti che si connettono e si disconnettono dalla rete.
In alcuni casi, è anche possibile che le aziende siano obbligate a mantenere in archivio i dati relativi alla protezione per un determinato periodo di tempo.

Il test è stato effettuato senza creare rallentamenti sulle performance di rete, anzi avendo finalmente una concreta possibilità di verificarle e di poterle migliorare e ottimizzare, identificando ad esempio i punti critici di consumo di banda, i protocolli più utilizzati (Broadcast-Multicast-Unicast), la topologia della rete e punti di criticità della stessa.

3 TOPOLOGIA DELLA RETE

3.1 Mappatura della rete

3.1.1 Indirizzamento Lan/Wan

La rete Lan è un unico dominio di broadcast e utilizza la seguente classe di indirizzamento:

- Lan Pippo 172.16.100.0/23
- Lan Marcianise 192.168.8.0/24

Ulteriori reti rilevate:

- DMZ Pippo 172.16.102.0
- Management Pippo 10.0.0.0

La rete geografica ha assegnati i seguenti IP Pubblici:

- Wan Pippo 85.43.190.192 - 85.43.190.207

Gli IP Pubblici sono registrati a nome di:

- netname: PIPPOSRL
- descr: PIPPO SRL
- person: Andrea Savio
- address: O.L.M. Officina Lavorazione Meccaniche
- address: Via Torino, 171
- address: I- 12048 Sommariva del Bosco
- address: Italy

3.1.2 Domain

Di seguito i domini rilevati:

- CANONWORK
- MATRIX_HOME
- PIPPO
- MULTINVEST
- MUTLINVEST
- SEWP
- WORKGROUP

I device appartenenti ai vari domini sono riportati nel file: nbinv.xls

3.2 Elenco apparati attivi SNMP

Il sistema ha rilevato i seguenti apparati di rete:

Mac	Ip	SysName	Description
000A04C759C0	172.16.100.247	swced5	3Com SuperStack 3
000E6A2B78C0	172.16.100.246	swced9	3Com SuperStack 3
000FCB921040	172.16.100.245	swced8	3Com SuperStack 3
000FCBEBE060	172.16.100.242	swced3	3Com SuperStack 3
000FCBEBF820	172.16.100.241	swced2	3Com SuperStack 3
000FCBF30FA0	172.16.100.240	swced1	3Com SuperStack 3
000FCBF330E0	172.16.100.243	swced4	3Com SuperStack 3
00147C5E6A80	172.16.100.239	swced10	3Com SuperStack 3
00157746A7E0	172.16.101.128	swmvest 1	ATI 8000S
00157746A8C0	172.16.101.129	swmvest2	ATI 8000S
00157746C4E0	172.16.101.131	swmvest 4	ATI 8000S
00157746E8E0	172.16.101.130	swmvest 3	ATI 8000S
0015774B81A0	172.16.100.233	SWCED6	ATI 8000S
0015774B8440	172.16.100.238	swced7	ATI 8000S
00260A176400	172.16.100.83	multimag1	Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE6, RELEASE SOFTWARE (fc1)
00260AD89F00	172.16.100.84	multimag2	Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE6, RELEASE SOFTWARE (fc1)
3CDF1E1CA700	172.16.100.86	swced13	Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE6, RELEASE SOFTWARE (fc1)
D0574C05E400	172.16.100.248	swmag1	Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE6, RELEASE SOFTWARE (fc1)
D0574C4A6800	172.16.100.249	swmag2	Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE6, RELEASE SOFTWARE (fc1)
F4ACC16E8200	172.16.100.85	swced12	Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE6, RELEASE SOFTWARE (fc1)
0025B4619280	172.16.100.80	multicore4	Cisco IOS Software, C3560E Software (C3560E-UNIVERSAL-M), Version 12.2(35)SE5, RELEASE SOFTWARE (fc1)
00260B5F0D80	172.16.100.79	multicore3	Cisco IOS Software, C3560E Software (C3560E-UNIVERSAL-M), Version 12.2(35)SE5, RELEASE SOFTWARE (fc1)
00260B8EEE80	172.16.100.77	multicore1	Cisco IOS Software, C3560E Software (C3560E-UNIVERSAL-M), Version 12.2(35)SE5, RELEASE SOFTWARE (fc1)
00260BE9E680	172.16.100.78	multicore2	Cisco IOS Software, C3560E Software (C3560E-

			UNIVERSAL-M), Version 12.2(35)SE5, RELEASE SOFTWARE (fc1)
0025B4164B00	172.16.100.81	multinvfarm	Cisco IOS Software, C3750 Software (C3750-IPBASE-M), Version 12.2(35)SE5, RELEASE SOFTWARE (fc1)
0025B42E5480	172.16.100.82	multifarm	Cisco IOS Software, C3750 Software (C3750-IPBASE-M), Version 12.2(35)SE5, RELEASE SOFTWARE (fc1)
00104004E175	172.16.101.99		Intermec Technologies AP
00104004E179	172.16.101.90		Intermec Technologies AP
00104004E17A	172.16.101.110		Intermec Technologies AP
00104004E17B	172.16.101.91		Intermec Technologies AP
00104004E17C	172.16.101.92		Intermec Technologies AP
00104004E17E	172.16.101.95		Intermec Technologies AP
00104004E180	172.16.101.107		Intermec Technologies AP
00104004E181	172.16.101.101		Intermec Technologies AP
001040052542	172.16.101.94		Intermec Technologies AP
001040052548	172.16.101.98		Intermec Technologies AP
00104005254E	172.16.101.93		Intermec Technologies AP
001040052597	172.16.101.103		Intermec Technologies AP
001040052A1C	172.16.101.96		Intermec Technologies AP
001040052A23	172.16.101.97		Intermec Technologies AP
001040052A24	172.16.101.105		Intermec Technologies AP
001040052A2B	172.16.101.104		Intermec Technologies AP
001040052A73	172.16.101.102		Intermec Technologies AP
00104007E619	172.16.101.111		Intermec Technologies AP
00104007E620	172.16.101.114		Intermec Technologies AP
00104007E622	172.16.101.115		Intermec Technologies AP
00104007E623	172.16.101.109		Intermec Technologies AP
00104007EBB4	172.16.101.100		Intermec Technologies AP
00104007EBB9	172.16.101.112		Intermec Technologies AP
00104007EF56	172.16.101.113		Intermec Technologies AP

3.3 Elenco devices

Abbiamo rilevato i device collegati in rete e le porte di rete su cui sono connessi identificando lo switch a cui le porte appartengono.

In allegato il file: user.xls

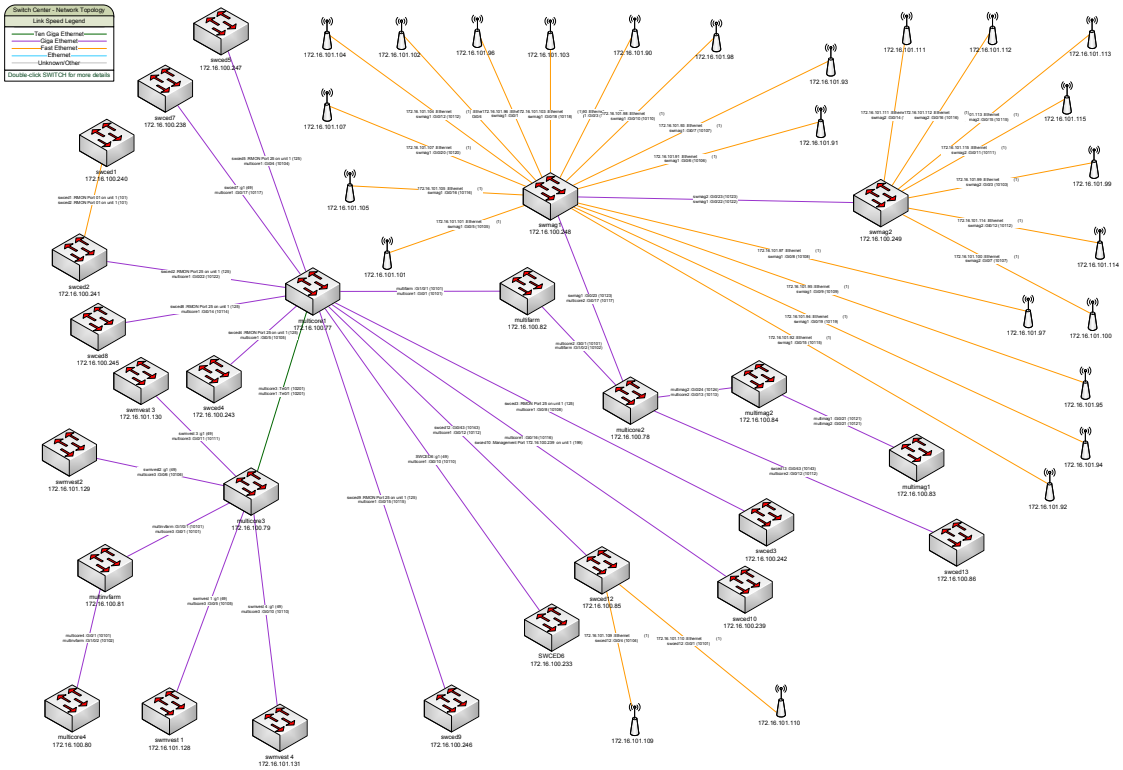
Se la porta è replicata più volte indica che c'è un device intermedio o un sistema con più ip (es. Access Point, HUB, Telefono VoIP, VMWare o simili)

Occorre prestare massima attenzione alla corrispondenza IP/Nome che potrebbe non essere corretta, sicuramente fa fede l'IP in quanto potrebbero esserci problemi sul DNS server.

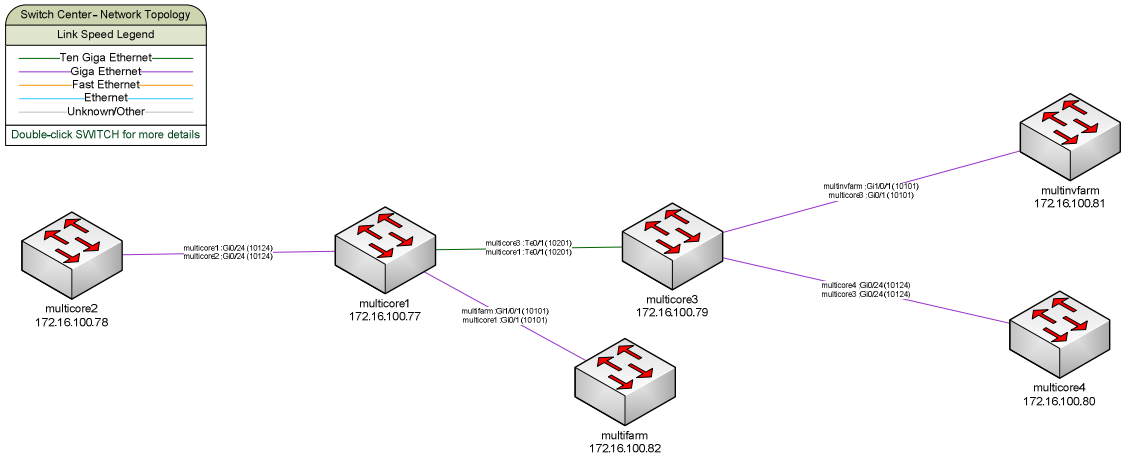
3.4 Topologia rete attuale

Gli schemi seguenti rappresentano l'attuale topologia di rete Pippo:

3.4.1 Schema connessioni switching:



3.4.2 Schema connessioni switch core:



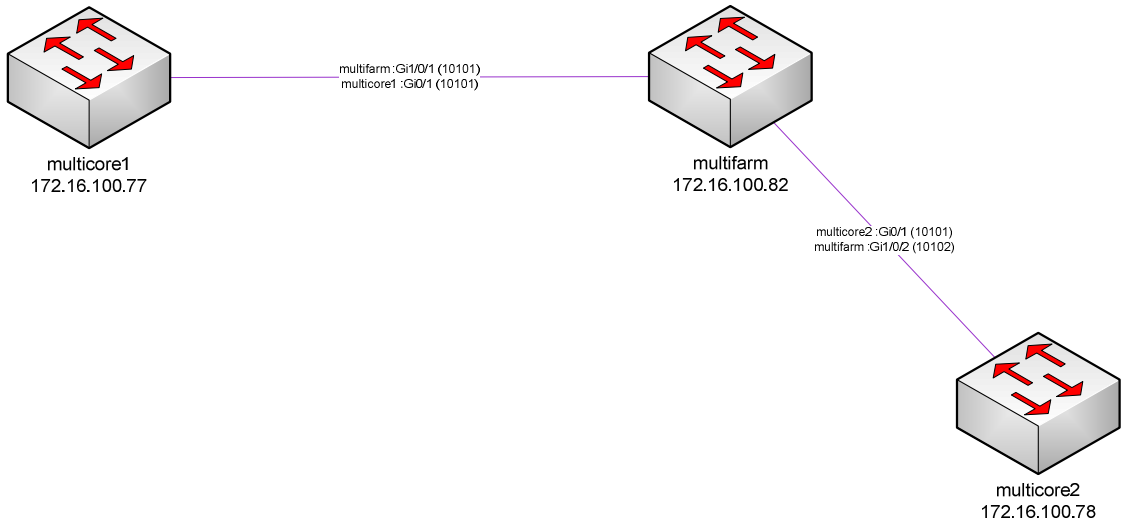
In allegato i files visio con schema generale e dettaglio di ogni apparato:

- network generale.vsd
- network core.vsd
- multifarm 172_16_100_82.vsd
- multimag1 172_16_100_83.vsd
- multimag2 172_16_100_84.vsd
- multinvfarm 172_16_100_81.vsd
- swced1 172_16_100_240.vsd
- swced2 172_16_100_241.vsd
- swced3 172_16_100_242.vsd
- swced4 172_16_100_243.vsd
- swced5 172_16_100_247.vsd
- swced6 172_16_100_233.vsd
- swced7 172_16_100_238.vsd
- swced8 172_16_100_245.vsd
- swced9 172_16_100_246.vsd
- swced10 172_16_100_239.vsd
- swced12 172_16_100_85.vsd
- swced13 172_16_100_86.vsd
- swvmvest 1 172_16_101.128.vsd
- swvmvest 2 172_16_101.129.vsd
- swvmvest 3 172_16_101.130.vsd
- swvmvest 4 172_16_101.131.vsd

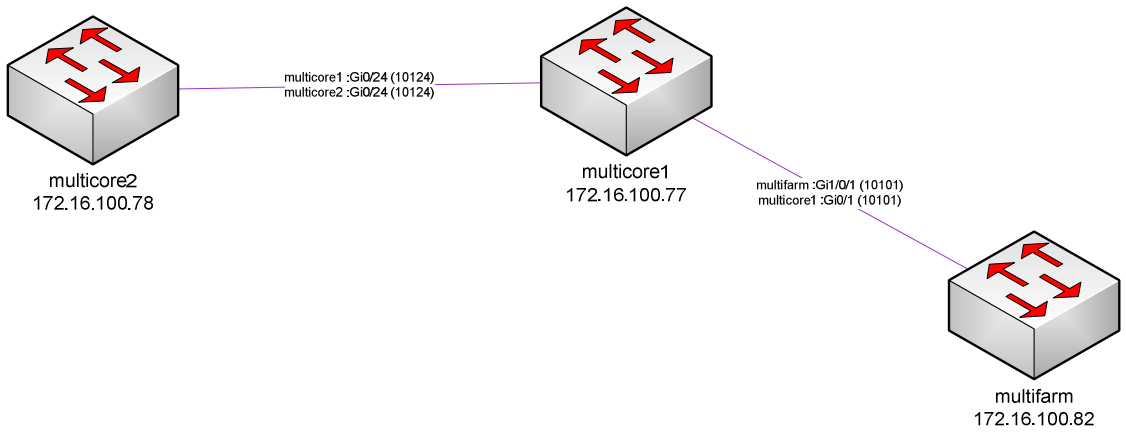
3.5 Analisi topologia

L'architettura di rete Pippo è composta da due CED connessi mediante Link a 10Gb attestati su due switch 3560 in ciascun CED, i server sono principalmente connessi a switch 3750 (uno per ciascun CED) e nel CED primario un ulteriore apparato 3750 gestisce la DMZ. Gli switch di distribuzione sono connessi ai 3650 con doppio link, utilizzando il protocollo di STP per la gestione dei link attivi.

Durante l'attività la topologia di rete ha subito variazioni, lo schema seguente mostra i due switch Multicore connessi mediante lo switch Multifarm:



Mentre in rilievi successivi risultava la seguente:

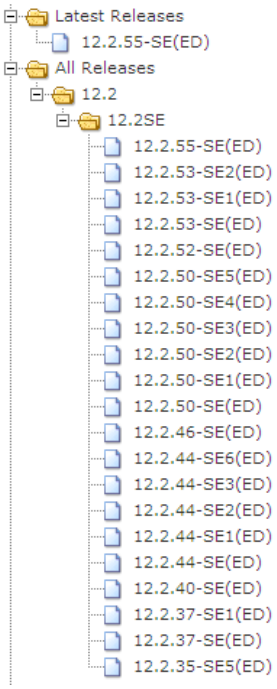


E' opportune verificare le configurazioni dello Spanning Tree.

Abbiamo verificato le release di software degli apparati Cisco che attualmente risultano essere le seguenti:

- C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)
- C3560E Software (C3560E-UNIVERSAL-M), Version 12.2(35)SE5
- C3750 Software (C3750-IPBASE-M), Version 12.2(35)SE5

Abbiamo rilevato che molti aggiornamenti di release intercorrono tra quella attualmente presente e l'ultima rilasciata da Cisco, gli aggiornamenti introducono nuove funzionalità ma fissano anch dei Bugs presenti nelle versioni precedenti.
Occorre fare una attenta analisi delle versioni attualmente in produzione e verificare se necessario ricorrere ad aggiornamento:



IOS Release Required	Catalyst Switch Support	
Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch	12.2(50)SE	3750, 3560, 2960
IEEE 802.1x with open access to allow a host to access the network before being authenticated	12.2(50)SE	3750, 3560, 2960
IEEE 802.1x authentication with downloadable ACLs and redirect URLs to allow per-user ACL downloads from a Cisco	12.2(50)SE	3750, 3560, 2960

Secure ACS server to an authenticated switch		
Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host	12.2(50)SE	3750, 3560, 2960
Multiple-user authentication to allow more than one host to authenticate on an 802.1x-enabled port	12.2(50)SE	3750, 3560, 2960
Cisco EnergyWise manages the energy usage of power over Ethernet (PoE) entities	12.2(50)SE	3750, 3560, 2960
Wired location service sends location and attachment tracking information for connected devices to a Cisco Mobility Services Engine (MSE)	12.2(50)SE	3750, 3560, 2960
CPU utilization threshold trap monitors CPU utilization	12.2(50)SE	3750, 3560, 2960
Support for the Cisco IOS Configuration Engine, previously referred to as the Cisco IOS CNS agent	12.2(50)SE	3750, 3560, 2960
LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signalling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode	12.2(50)SE	3750, 3560, 2960
RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group	12.2(50)SE	3750, 3560, 2960
Auto Smartports Cisco-default and user-defined macros for dynamic port configuration based on the device type detected on the port	12.2(50)SE	3750, 3560, 2960
Support for: SCP attribute in the CONFIG_COPY MIB, CISCO-AUTH-FRAMEWORK-MIB, CISCO-MAC-AUTH-BYPASS MIBs, LLDP MIB	12.2(50)SE	3750, 3560, 2960
Intermediate System-to-Intermediate System (IS-IS) routing supports dynamic routing protocols for Connectionless Network Service (CLNS) networks	12.2(50)SE	3750, 3560
Support for Embedded Event Manager Version 2.4.	12.2(50)SE	3750, 3560
These IPv6 features are now supported in the IP services and IP base software images: ACLs; DHCPv6 for the DCHP server, client, and relay device; EIGRPv6; HSRPv6; OSPFv3; RIP; Static routes	12.2(50)SE	3750, 3560
Stack troubleshooting enhancements	12.2(50)SE	3750
Support for 802.1x authentication with restricted VLANs (also known as *authentication failed VLANs*) in all switch images	12.2(50)SE	2960
IP source guard restricts traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings	12.2(50)SE	2960
Dynamic ARP inspection to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN	12.2(50)SE	2960
Generic message authentication support with the SSH Protocol and compliance with RFC 4256	12.2(46)SE	3750, 3560, 2960
Generic message authentication support	12.2(46)SE	3750, 3560, 2960
Disabling MAC address learning on a VLAN	12.2(46)SE	3750, 3560, 2960
PAgP Interaction with Virtual Switches and Dual-Active	12.2(46)SE	3750, 3560, 2960

Detection		
DHCP server port-based address allocation	12.2(46)SE	3750, 3560, 2960
IPv6 default router preference (DRP)	12.2(46)SE	3750, 3560, 2960
Voice aware IEEE 802.1x and mac authentication bypass (MAB) security violation	12.2(46)SE	3750, 3560
Local web authentication banner	12.2(46)SE	3750, 3560
Support for the CISCO-NAC-NAD and CISCO-PAE MIBs	12.2(46)SE	3750, 3560
Exclude a port in a VLAN from the SVI line-state up or down calculation	12.2(46)SE	3750, 3560
EOT and IP SLAs EOT static route support	12.2(46)SE	3750, 3560
Support for HSRP Version 2 (HSRPv2)	12.2(46)SE	3750, 3560
HSRP for IPv6 (requires the advanced IP services image)	12.2(46)SE	3750, 3560
DHCP for IPv6 relay, client, server address assignment and prefix delegation (requires the advanced IP services image)	12.2(46)SE	3750, 3560
Embedded event manager (EEM) for device and system management (IP services image only)	12.2(46)SE	3750, 3560
Dynamic voice virtual LAN (VLAN) for multidomain authentication (MDA)	12.2(46)SE	2960
Monitor and police the real-time power consumption on a per-PoE port basis	12.2(46)SE	2960
IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute	12.2(46)SE	2960
IEEE 802.1x readiness check	12.2(44)SE	3750, 3560, 2960
DHCP-based autoconfiguration and image update	12.2(44)SE	3750, 3560, 2960
Configurable small-frame arrival threshold	12.2(44)SE	3750, 3560, 2960
HTTP and HTTP(s) support over IPV6	12.2(44)SE	3750, 3560, 2960
Simple Network and Management Protocol (SNMP) configuration over IPv6 transport	12.2(44)SE	3750, 3560, 2960
IPv6 stateless autoconfiguration	12.2(44)SE	3750, 3560, 2960
Flex Link Multicast Fast Convergence	12.2(44)SE	3750, 3560, 2960
Digital optical monitoring (DOM)	12.2(44)SE	3750, 3560
Source Specific Multicast (SSM) mapping	12.2(44)SE	3750, 3560
/31 bit mask support for multicast traffic	12.2(44)SE	3750, 3560
Configuration replacement and rollback	12.2(40)SE	3750, 3560, 2960
Link Layer Discovery Protocol Media Extensions (LLDP-MED)	12.2(40)SE	3750, 3560, 2960
Support for Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6	12.2(40)SE	3750, 3560
Automatic quality of service (QoS) Voice over IP (VoIP)	12.2(40)SE	3750, 3560, 2960
Dynamic voice virtual LAN (VLAN) for multidomain authentication (MDA)-enabled ports	12.2(40)SE	3750, 3560
Internet Group Management Protocol (IGMP) helper	12.2(40)SE	3750, 3560
IP Service Level Agreements (IP SLAs)	12.2(40)SE	3750, 3560
IP SLAs EOT	12.2(40)SE	3750, 3560

Multicast virtual routing and forwarding (VRF) lite	12.2(40)SE	3750, 3560
SSM PIM protocol	12.2(40)SE	3750, 3560
VRF-aware support for these IP services: HSRP, uRPF, ARP, SNMP, IP SLA, TFTP, FTP, syslog, traceroute, and ping	12.2(40)SE	3750, 3560
MLD snooping	12.2(40)SE	2960
IPv6 host	12.2(40)SE	2960
IP phone detection enhancement	12.2(37)SE	3750, 3560, 2960
Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED)	12.2(37)SE	3750, 3560, 2960
PIM stub routing	12.2(37)SE	3750, 3560
Port security on a PVLAN host	12.2(37)SE	3750, 3560
VLAN aware port security option	12.2(37)SE	3750, 3560, 2960
Support for auto rendezvous point (auto-RP) for multicast	12.2(37)SE	3750. 3560
VLAN Flex Links load balancing	12.2(37)SE	3750, 3560, 2960
Web Cache Communication Protocol (WCCP)	12.2(37)SE	3750. 3560
Multidomain authentication (MDA)	12.2(35)SE	3750, 3560
Web authentication	12.2(35)SE	3750, 3560, 2960
MAC inactivity aging	12.2(35)SE	3750, 3560, 2960
Support for IPv6 with Express Setup	12.2(35)SE	3750, 3560
Generic online diagnostics to test the hardware functionality of the supervisor engine	12.2(35)SE	3560
Stack MAC persistent timer and archive download enhancements	12.2(35)SE	3750
HSRP enhanced object tracking	12.2(35)SE	3750, 3560
OSPF and EIGRP Nonstop forwarding capability (IP services image only)	12.2(35)SE	3750
IPv6 router ACLs for inbound Layer 3 management traffic in the IP base and IP services image	12.2(35)SE	3750, 3560

Ad esempio una piccola ricerca rileva:

- Cisco 3560: "Mac based security on 3560E" sulla release 12.2(35)SE5, legato alla pubblicazione dei Mac address se usi le porte taggate per PC e VoIP
- Cisco 3750: problema sull'IOS "3750 system crash Version 12.2(35)SE5" "the version of IOS you have is notorious for crashes and reloads. If you can't find the root cause of the crash, I suggest you update your IOS"

Mentre gli apparati 3com sono fuori produzione e quindi non aggiornabili e né manutenibili

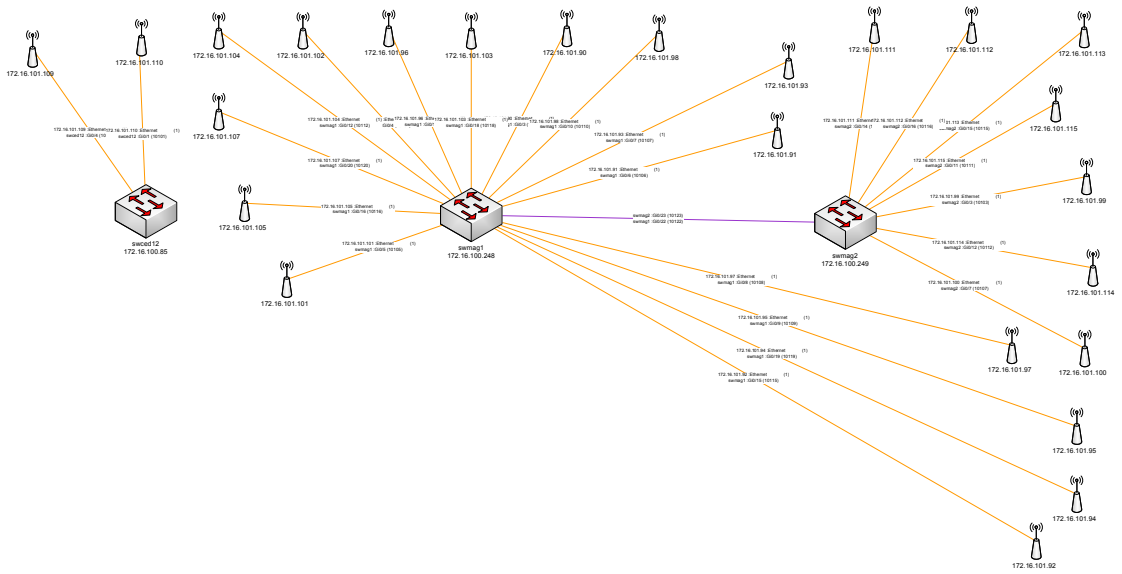
La serie Allied 8000s sono 10/100 stackable a 4Gb, supporta vlan tagging e l'ultima release del firmware è datata: 12/8/2010 (v2.3.2)

3.6 Rete Wireless

Pippo ha una rete wireless di cui sono stati rilevati 24 Access Point della Intermec Technologies AP.

La rete non presenta nessun tipo di protezione, è possibile connettersi ed acquisire un indirizzo di rete ed essendo questa piatta, è possibile effettuare scansioni e attacchi.

Di seguito lo schema:



La rete è stata implementata non rispettando le basilari norme di implementazione che prevedono al massimo 3 canali sussistenti nella stessa area di copertura. In ambito 802.11g, ad esempio, si possono affiancare e configurare massimo 3 access point operanti sui canali 1, 6, 11, in modo da offrire una banda triplicata rispetto ad una rete con un solo access point e occorre verificare che non ci sia sovrapposizione di canale.

Da analisi ambientale risultano invece molte sovrapposizioni, addirittura oltre 10 canali nella stessa area di copertura:

mac: 0:2:2d:ba:72:97
channel: 11
MaxRssi: -90
Security: None
Type: Access Point
FirstSeen: 2010-11-02 10:43:22

mac: 0:2:2d:ba:72:aa
channel: 1
MaxRssi: -92
Security: None
Type: Access Point
FirstSeen: 2010-11-02 10:43:22
mac: 0:2:2d:ba:72:d3
channel: 6
MaxRssi: -62
Security: None
Type: Access Point
FirstSeen: 2010-11-02 10:43:22
mac: 0:2:2d:ba:74:14
channel: 1
MaxRssi: -56
Security: None
Type: Access Point
FirstSeen: 2010-11-02 10:43:22
mac: 0:2:2d:ba:74:15
channel: 1
MaxRssi: -95
Security: None
Type: Access Point
FirstSeen: 2010-11-02 10:43:22
mac: 0:2:2d:ba:74:17
channel: 11
MaxRssi: -82
Security: None
Type: Access Point
FirstSeen: 2010-11-02 10:43:22
mac: 0:2:2d:ba:74:25
channel: 1
MaxRssi: -81
Security: None
Type: Access Point
FirstSeen: 2010-11-02 10:43:22
mac: 0:2:2d:ba:74:cd
channel: 11
MaxRssi: -82
Security: None
Type: Access Point
FirstSeen: 2010-11-02 10:43:22
mac: 0:2:2d:bc:a4:7d
channel: 11
MaxRssi: -72
Security: None
Type: Access Point
FirstSeen: 2010-11-02 10:43:28
mac: 0:2:2d:bc:a4:80
channel: 6
MaxRssi: -87
Security: None
Type: Access Point
FirstSeen: 2010-11-02 10:43:22
mac: 0:2:2d:bc:a9:9f
channel: 11
MaxRssi: -92
Security: None
Type: Access Point
FirstSeen: 2010-11-02 10:43:22

E’ opportune rivedere l’architettura wireless, su una estensione tale di access point l’ideale sarebbe implementare tecnologia con controller wireless ridondata, comunque modificare le attuali antenne con delle direzionali rifacendo idonea analisi ambientale.

3.7 Cablaggio Strutturato

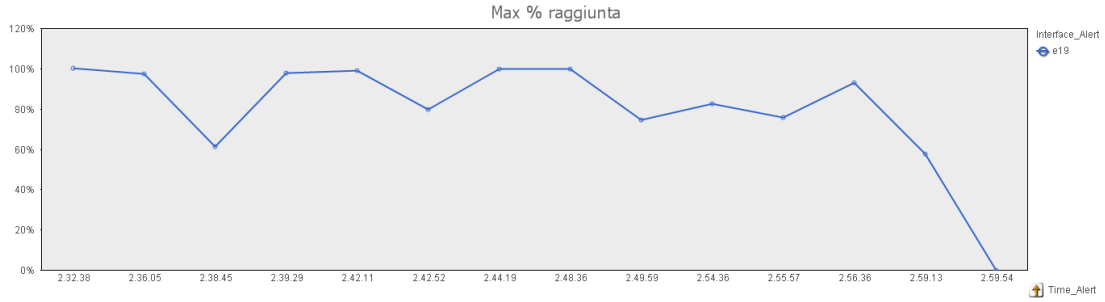
Il cablaggio strutturato è in cat. 5e per quanto riguarda la distribuzione orizzontale e in cat.6 per la distribuzione di dorsale con due link verso armadi periferici.

4 ANALISI PERFORMANCE DI RETE

4.1 Punti critici della rete

Durante l'attività di analisi non sono state riscontrate problematiche a livello di traffico (elevati broadcast, multi cast o unicast).

Durante la notte dei picchi di banda utilizzata sono stati rilevati come di seguito evidenziati:



Switch Ip	172.16.100.233
Switch SysName	SWCED6
Switch Mac	0015774B81A0
Alert Interface	e19
Port Interface	19
Port Speed	100
Ip Node	172.16.100.165
Mac Node	0019BBEC9497
Name Node	MULTINVESTFTP

Sarebbe opportuno migrare su tecnologia Gigabit l'interfaccia di rete di questo device

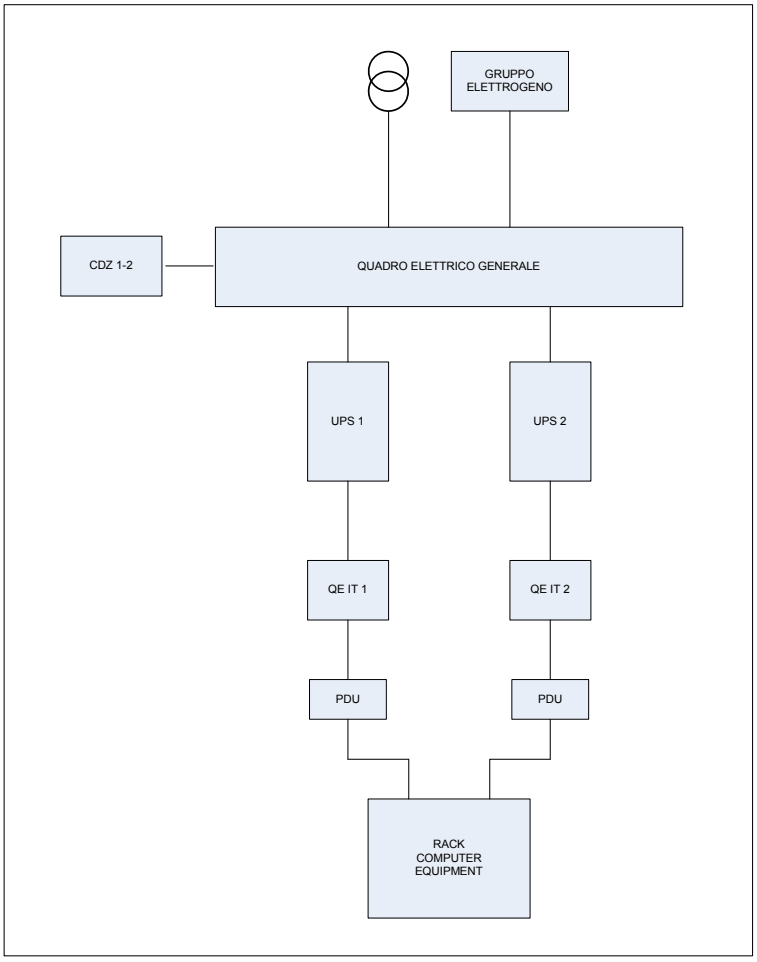
4.2 Sala CED

Abbiamo visitato il locale UPS di recente realizzazione, dagli schemi apposti sulla parete sembra che un gruppo è dedicato alla sala CED. Sarebbe opportuno verificare perché non è stato previsto un sistema di distribuzione realizzato mediante ridondanza degli stessi con alimentazione di due circuiti separati.

Il quadro in derivazione dalle due linee UPS gestirebbe i due circuiti separati verso le doppie barre di alimentazione dei rack.

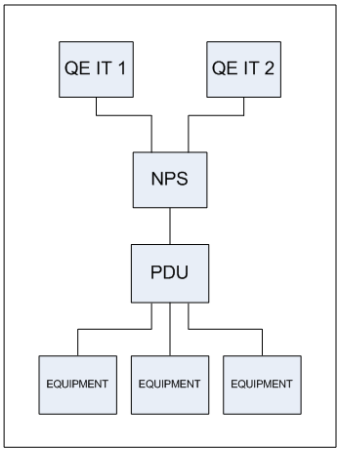
L'allestimento dovrebbe essere implementato secondo i criteri di alta affidabilità, sicurezza, standardizzazione e scalabilità, per far fronte alle tendenze tecnologiche IT emergenti e future, soddisfacendo l'esigenza di protezione dell'investimento.

Dovrebbero essere applicati i criteri di dimensionamento dell'infrastruttura di livello TIER 3 della normativa EN-942 secondo i quali l'architettura dei sistemi deve ottemperare le specifiche indicate nello schema sottostante:



i sistemi di distribuzione di energia elettrica devono avere due circuiti separati, attivi entrambi sotto UPS differenti

Nel caso di dispositivi con singola alimentazione (apparati di rete quali switch, firewall, router) è possibile utilizzare l'apparato STS per la gestione ridondata degli apparati a singola alimentazione.



Schema circuito NPS o STS

STS APC

4.3 Protocolli

La maggior parte dei protocolli rilevati a livello due sono nella norma, si evidenziano solo i protocolli utilizzati per monitorare la rete.

5 ANALISI DELLE VULNERABILITÀ DELLA RETE

5.1 Descrizione generale

Dagli schemi allegati si evince che una parte dell'architettura di rete dovrebbe essere rivista, sarebbe opportuno verificare la possibilità di utilizzare i Cisco 3750 in modalità stackable e connettere gli switch periferici ad essi in link aggregation in modo da avere tutti i link attivi e mantenere i 3560 solo per il collegamento a 10Gb e per i server che non riescono ad essere attestati sui 3750, i server invece attestati sui 3750 possono sfruttare anch'essi l'aggregazione dei link mantenendo attivi entrambi i collegamenti se presenti doppie schede di rete.

Abbiamo provato ad accedere agli switch via web interface e via console e abbiamo constatato che le password sono state impostate.

Anche le community dell'SNMP sono correttamente impostate anche se varie e sarebbe opportuno omogeneizzare con unica password conosciuta solo da Pippo e una password solo in read da utilizzare in caso di necessità da poter comunicare a società esterne ma da modificare dopo il suo utilizzo.

E' importante impostare correttamente le community SNMP in quanto tale comunicazione consiste in diversi tipi di messaggi scambiati tra le stazioni di gestione SNMP e i dispositivi di rete che eseguono quello che comunemente è definito come agent software.
Esistono una serie di vulnerabilità nel modo in cui i messaggi di richiesta e cattura sono gestiti e decodificati dalle stazioni di gestione e dagli agenti.
Sfruttando queste vulnerabilità gli aggressori possono arrivare a risultati che variano dal Denial of Service alla modifica della configurazione e del sistema di gestione delle macchine abilitate all'SNMP.
Le versioni 1 e 2 di SNMP utilizzano un meccanismo di autenticazione "community string" non crittata infatti è possibile acquisirla con uno sniffer di rete. La mancanza di crittografia è già abbastanza grave, ma in più la community string usata per default nella grande maggioranza dei dispositivi SNMP è "public," e quindi una impostazione diversa protegge la trasmissione delle informazioni più sensibili attraverso questo protocollo.

Gli apparati di rete hanno il firmware da verificare.

La rete wireless è da mettere in sicurezza

5.2 Port scanning

In questa sezione, abbiamo elencato le porte che sono generalmente esaminate e attaccate. Ovviamente il blocco di alcune delle porte elencate può disabilitare servizi necessari, solo chi gestisce la sicurezza in Azienda è in grado di comprendere se sono aperte per erogare servizi o sono aperte ma inutilmente. Prima di implementare queste raccomandazioni, occorre considerare i potenziali effetti.

Le principali porte sono descritte a livello di funzionalità nella tabella seguente:

Nome	Porta	Protocollo	Descrizione
Small services	<20	tcp/udp	small services
FTP	21	tcp	file transfer
SSH	22	tcp	login service
TELNET	23	tcp	login service
SMTP	25	tcp	mail
TIME	37	tcp/udp	time synchronization
WINS	42	tcp/udp	WINS replication
DNS	53	udp	naming services
DNS zone transfers	53	tcp	naming services
DHCP server	67	tcp/udp	host configuration
DHCP client	68	tcp/udp	host configuration
TFTP	69	udp	miscellaneous
GOPHER	70	tcp	old WWW-like service
FINGER	79	tcp	miscellaneous
HTTP	80	tcp	web
alternate HTTP port	81	tcp	web
alternate HTTP port	88	tcp	web (sometimes Kerberos)
LINUXCONF	98	tcp	host configuration
POP2	109	tcp	mail
POP3	110	tcp	mail
PORTMAP/RPCBIND	111	tcp/udp	RPC portmapper
NNTP	119	tcp	network news service
NTP	123	udp	time synchronization
NetBIOS	135	tcp/udp	DCE-RPC endpoint mapper
NetBIOS	137	udp	NetBIOS name service
NetBIOS	138	udp	NetBIOS datagram service
NetBIOS/SAMBA	139	tcp	file sharing & login service
IMAP	143	tcp	mail

SNMP	161	tcp/udp	miscellaneous
SNMP	162	tcp/udp	miscellaneous
XDMCP	177	udp	X display manager protocol
BGP	179	tcp	miscellaneous
FW1-secureremote	256	tcp	CheckPoint FireWall-1 mgmt
FW1-secureremote	264	tcp	CheckPoint FireWall-1 mgmt
LDAP	389	tcp/udp	naming services
HTTPS	443	tcp	web
Windows 2000 NetBIOS	445	tcp/udp	SMB over IP (Microsoft-DS)
ISAKMP	500	udp	IPSEC Internet Key Exchange
REXEC	512	tcp	} the three
RLOGIN	513	tcp	} Berkeley r-services
RSHELL	514	tcp	} (used for remote login)
RWHO	513	udp	miscellaneous
SYSLOG	514	udp	miscellaneous
LPD	515	tcp	remote printing
TALK	517	udp	miscellaneous
RIP	520	udp	routing protocol
UUCP	540	tcp/udp	file transfer
HTTP RPC-EPMAP	593	tcp	HTTP DCE-RPC endpoint mapper
IPP	631	tcp	remote printing
LDAP over SSL	636	tcp	LDAP over SSL
Sun Mgmt Console	898	tcp	remote administration
SAMBA-SWAT	901	tcp	remote administration
Windows RPC programs	1025	tcp/udp	} often allocated
Windows RPC programs	to		} by DCE-RPC portmapper
Windows RPC programs	1039	tcp/udp	} on Windows hosts
SOCKS	1080	tcp	miscellaneous
LotusNotes	1352	tcp	database/groupware
MS-SQL-S	1433	tcp	database
MS-SQL-M	1434	udp	database
CITRIX	1494	tcp	remote graphical display
WINS replication	1512	tcp/udp	WINS replication
ORACLE	1521	tcp	database
NFS	2049	tcp/udp	NFS file sharing
COMPAQDIAG	2301	tcp	Compaq remote administration
COMPAQDIAG	2381	tcp	Compaq remote administration
CVS	2401	tcp	collaborative file sharing
SQUID	3128	tcp	web cache

Global catalog LDAP	3268	tcp	Global catalog LDAP
Global catalog LDAP SSL	3269	tcp	Global catalog LDAP SSL
MYSQL	3306	tcp	database
Microsoft Term. Svc.	3389	tcp	remote graphical display
LOCKD	4045	tcp/udp	NFS file sharing
Sun Mgmt Console	5987	tcp	remote administration
PCANYWHERE	5631	tcp	remote administration
PCANYWHERE	5632	tcp/udp	remote administration
VNC	5800	tcp	remote administration
VNC	5900	tcp	remote administration
X11	6000-6255	tcp	X Windows server
FONT-SERVICE	7100	tcp	X Windows font service
alternate HTTP port	8000	tcp	web
alternate HTTP port	8001	tcp	web
alternate HTTP port	8002	tcp	web
alternate HTTP port	8080	tcp	web
alternate HTTP port	8081	tcp	web
alternate HTTP port	8888	tcp	web
Unix RPC programs	32770	tcp/udp	} often allocated
Unix RPC programs	to	} by RPC portmapper	
Unix RPC programs	32899	tcp/udp	} on Solaris hosts
COMPAQDIAG	49400	tcp	Compaq remote administration
COMPAQDIAG	49401	tcp	Compaq remote administration
PCANYWHERE	65301	tcp	remote administration

Nella tabella che segue abbiamo identificato alcune porte principali aperte sui device di rete, principalmente le TCP più utilizzate, ovviamente non essendo a conoscenza dei vari servizi che le macchine svolgono lasciamo alla Pippo il compito di analizzare le eventuali porte che non dovrebbero essere aperte sulla base delle indicazioni fornite nella tabella precedente:

LAN Pippo

IP Address	Host Name	Port
172.16.100.2	ws1018	21
172.16.100.4	lgaudio.pippo.com	21
172.16.100.6	vmarra.pippo.com	21
172.16.100.7	cepparulonew.pippo.com	21
172.16.100.8	mag081new.pippo.com	21
172.16.100.10	rseveri.pippo.com	21

172.16.100.11	atrepiccione.pippo.com	21
172.16.100.12	mautieronew.pippo.com	21
172.16.100.13	mellusonb.pippo.com	21
172.16.100.15	scarnevale.pippo.com	21
172.16.100.16	agasparrino.pippo.com	21
172.16.100.17	ltrabucco.pippo.com	21
172.16.100.18	vcaliendo.pippo.com	21
172.16.100.19	gbarbano.pippo.com	21
172.16.100.20	cienco.pippo.com	21
172.16.100.21	vamatucci.pippo.com	21
172.16.100.24	mag07a.pippo.com	21
172.16.100.25	gaufieri.pippo.com	21
172.16.100.31	ortofrutta.pippo.com	21
172.16.100.35	sdilillonew.pippo.com	21
172.16.100.37	mag04new.pippo.com	21
172.16.100.38	mdellovo.pippo.com	21
172.16.100.40	gursillonew.pippo.com	21
172.16.100.42	frucco.pippo.com	21
172.16.100.45	pstolfi.pippo.com	21
172.16.100.47	epalmas.pippo.com	21
172.16.100.48	sdelprete.pippo.com	21
172.16.100.49	vfusco.pippo.com	21
172.16.100.50	fdeluca.pippo.com	21
172.16.100.52	srussonew.pippo.com	21
172.16.100.53	grusso.pippo.com	21
172.16.100.56	fdistefano.pippo.com	21
172.16.100.57	sdellarocca.pippo.com	21
172.16.100.62	mgemma.pippo.com	21
172.16.100.61	mag03.pippo.com	21
172.16.100.60	mag012new.pippo.com	21
172.16.100.72	lruotolo.pippo.com	21
172.16.100.88	sgiannini.pippo.com	21
172.16.100.89	mbernardonew.pippo.com	21
172.16.100.90	bganzerli.pippo.com	21
172.16.100.93	mag013.pippo.com	21
172.16.100.94	acoco.pippo.com	21
172.16.100.96	vromano.pippo.com	21
172.16.100.98	sdirauso.pippo.com	21
172.16.100.99	dlanna.pippo.com	21
172.16.100.101	vvitale.pippo.com	21
172.16.100.102	gcioppa.pippo.com	21
172.16.100.104	paghe.pippo.com	21
172.16.100.105	ndangelo.pippo.com	21
172.16.100.106	spalmieri.pippo.com	21
172.16.100.107	anuzzo.pippo.com	21
172.16.100.110	amartello.pippo.com	21
172.16.100.109	lliccardinew.pippo.com	21
172.16.100.112	amarinonbnew.pippo.com	21
172.16.100.113	calbanonew.pippo.com	21
172.16.100.115	fmargarita.pippo.com	21
172.16.100.116	amerolanew.pippo.com	21
172.16.100.119	fcucco.pippo.com	21
172.16.100.120	gdelianew.pippo.com	21
172.16.100.124	vcompagnone.pippo.com	21
172.16.100.126	asangermano.pippo.com	21
172.16.100.127	gloffredo.pippo.com	21
172.16.100.129	ubellini.pippo.com	21
172.16.100.130	mlombardi1.pippo.com	21
172.16.100.134	genatiempo.pippo.com	21
172.16.100.135	ccapolupo.pippo.com	21
172.16.100.137	lenovo-31e2f5ff	21

172.16.100.138	faxecon.pippo.com	21
172.16.100.151	consoleas400.pippo.com	21
172.16.100.152	windows-07ad976	21
172.16.100.153	idecristofaro.pippo.com	21
172.16.100.154	pmiele.pippo.com	21
172.16.100.162	mag11new.pippo.com	21
172.16.100.163	dmellusonb.pippo.com	21
172.16.100.164	autuori.pippo.com	21
172.16.100.167	cadduci.pippo.com	21
172.16.100.168	pandaserver.pippo.com	21
172.16.100.171	mag06.pippo.com	21
172.16.100.173	reception.pippo.com	21
172.16.100.175	asacco_new.pippo.com	21
172.16.100.179	mag02.pippo.com	21
172.16.100.181		21
172.16.100.182	rderosanew.pippo.com	21
172.16.100.183		21
172.16.100.185	gtornesi1.pippo.com	21
172.16.100.187		21
172.16.100.188		21
172.16.100.197	consolenew.pippo.com	21
172.16.100.204		21
172.16.100.205		21
172.16.100.206		21
172.16.100.207		21
172.16.100.209	cashcsgpdv.pippo.com	21
172.16.100.232		21
172.16.100.234		21
172.16.100.237		21
172.16.101.30		21
172.16.101.32		21
172.16.101.33		21
172.16.101.34		21
172.16.101.37		21
172.16.101.40		21
172.16.101.41		21
172.16.101.50		21
172.16.101.53		21
172.16.101.57		21
172.16.101.58		21
172.16.101.59		21
172.16.101.60		21
172.16.101.62		21
172.16.101.63		21
172.16.101.65		21
172.16.101.72		21
172.16.101.121	smarescanew.pippo.com	21
172.16.101.124		21
172.16.101.125		21
172.16.101.159		21
172.16.101.160		21
172.16.101.162		21
172.16.101.166		21
172.16.101.167		21
172.16.101.168		21
172.16.101.169		21
172.16.101.170		21
172.16.101.171		21
172.16.101.172		21
172.16.101.173		21
172.16.101.190		21

172.16.101.191		21
172.16.101.192		21
172.16.101.193		21
172.16.101.194		21
172.16.101.195		21
172.16.101.196		21
172.16.101.197		21
172.16.101.198		21
172.16.101.199		21
172.16.101.200		21
172.16.101.201		21
172.16.101.202		21
172.16.101.203		21
172.16.101.204		21
172.16.101.205		21
172.16.101.207		21
172.16.101.209		21
172.16.101.210		21
172.16.101.211		21
172.16.101.212		21
172.16.101.213		21
172.16.101.214		21
172.16.101.215		21
172.16.101.217		21
172.16.101.219		21
172.16.101.220		21
172.16.101.221		21
172.16.101.222		21
172.16.101.223		21
172.16.101.224		21
172.16.101.225		21
172.16.101.226		21
172.16.101.227		21
172.16.101.228		21
172.16.101.229		21
172.16.101.230		21
172.16.101.231		21
172.16.101.232		21
172.16.101.233		21
172.16.101.234		21
172.16.101.235		21
172.16.101.236		21
172.16.101.237		21
172.16.101.238		21
172.16.101.239		21
172.16.101.240		21
172.16.101.241		21
172.16.101.242		21
172.16.101.243		21
172.16.101.244		21
172.16.101.245		21
172.16.101.246		21
172.16.101.247		21
172.16.101.248		21
172.16.101.249		21
172.16.101.250		21
172.16.101.251		21
172.16.101.252		21
172.16.101.253		21
172.16.100.23	mnardiellonew.pippo.com	80
172.16.100.195	multisv005.pippo.com	110, 143, 21, 25, 443,

		80
172.16.100.198	attila1.pippo.com	110, 21, 25
172.16.100.216		111, 21, 22, 23
172.16.100.1		111, 21, 22, 23, 37, 512, 513, 514
172.16.100.202		111, 21, 22, 23, 80
172.16.100.203		111, 21, 22, 23, 80
172.16.101.187	voiceconsole.pippo.com	111, 21, 22, 37
172.16.100.215		111, 21, 80
172.16.100.174	dbserver.pippo.com	19, 21, 25, 443, 7, 80, 9
172.16.100.83		21, 22, 23, 443, 80
172.16.100.84		21, 22, 23, 443, 80
172.16.100.85		21, 22, 23, 443, 80
172.16.100.86		21, 22, 23, 443, 80
172.16.100.248		21, 22, 23, 443, 80
172.16.100.249		21, 22, 23, 443, 80
172.16.100.192	multifw1.pippo.com	21, 22, 37
172.16.100.252		21, 22, 37
172.16.100.180	multisv011.pippo.com	21, 22, 443, 80
172.16.100.194	squid.pippo.com	21, 22, 80, 8080
172.16.100.189	mcedi1new.pippo.com	21, 23, 25, 37, 512, 515
172.16.100.199	datamcedi2.pippo.com	21, 23, 25, 37, 512, 515
172.16.100.200	mcedi2.pippo.com	21, 23, 25, 37, 512, 515
172.16.100.201	mcedi1.pippo.com	21, 23, 25, 37, 512, 515
172.16.101.177	asmuti1.pippo.com	21, 23, 25, 37, 512, 515
172.16.101.179	asmulti2.pippo.com	21, 23, 25, 37, 512, 515
172.16.100.225		21, 23, 443, 515, 80
172.16.100.226		21, 23, 443, 515, 80
172.16.101.133		21, 23, 443, 515, 80
172.16.101.134		21, 23, 443, 515, 80
172.16.101.175		21, 23, 443, 515, 80
172.16.101.188		21, 23, 443, 515, 80
172.16.101.90		21, 23, 443, 80
172.16.101.91		21, 23, 443, 80
172.16.101.92		21, 23, 443, 80
172.16.101.93		21, 23, 443, 80
172.16.101.94		21, 23, 443, 80
172.16.101.95		21, 23, 443, 80
172.16.101.96		21, 23, 443, 80
172.16.101.97		21, 23, 443, 80
172.16.101.98		21, 23, 443, 80
172.16.101.99		21, 23, 443, 80
172.16.101.100		21, 23, 443, 80
172.16.101.101		21, 23, 443, 80
172.16.101.102		21, 23, 443, 80
172.16.101.103		21, 23, 443, 80
172.16.101.104		21, 23, 443, 80
172.16.101.105		21, 23, 443, 80
172.16.101.107		21, 23, 443, 80
172.16.101.109		21, 23, 443, 80
172.16.101.110		21, 23, 443, 80
172.16.101.111		21, 23, 443, 80
172.16.101.112		21, 23, 443, 80
172.16.101.113		21, 23, 443, 80
172.16.101.114		21, 23, 443, 80
172.16.101.115		21, 23, 443, 80
172.16.100.170		21, 23, 515
172.16.100.222		21, 23, 515
172.16.100.223		21, 23, 515
172.16.100.220		21, 23, 515, 80

172.16.100.228		21, 23, 515, 80
172.16.100.235		21, 23, 515, 80
172.16.100.244		21, 23, 515, 80
172.16.100.77		21, 23, 80
172.16.100.78		21, 23, 80
172.16.100.79		21, 23, 80
172.16.100.80		21, 23, 80
172.16.100.81		21, 23, 80
172.16.100.82		21, 23, 80
172.16.100.233		21, 23, 80
172.16.100.238		21, 23, 80
172.16.100.239		21, 23, 80
172.16.100.240		21, 23, 80
172.16.100.241		21, 23, 80
172.16.100.242		21, 23, 80
172.16.100.243		21, 23, 80
172.16.100.245		21, 23, 80
172.16.100.246		21, 23, 80
172.16.100.247		21, 23, 80
172.16.101.80		21, 23, 80
172.16.101.81		21, 23, 80
172.16.101.82		21, 23, 80
172.16.101.83		21, 23, 80
172.16.101.84		21, 23, 80
172.16.101.128		21, 23, 80
172.16.101.129		21, 23, 80
172.16.101.130		21, 23, 80
172.16.101.131		21, 23, 80
172.16.100.165		21, 25, 443, 80
172.16.101.126	gtrepiccione.pippo.com	21, 25, 443, 80
172.16.100.161	multisv009.pippo.com	21, 443, 80
172.16.100.229		21, 443, 80
172.16.100.236		21, 443, 80
172.16.101.164		21, 515, 7, 80
172.16.101.186		21, 515, 7, 80
172.16.101.189		21, 515, 7, 80
172.16.100.218		21, 515, 80
172.16.101.184		21, 515, 80
172.16.100.172		21, 7, 80
172.16.101.183		21, 7, 80
172.16.100.74	mzurolo.pippo.com	21, 80
172.16.100.166	multisv004.pippo.com	21, 80
172.16.100.169		21, 80
172.16.100.178		21, 80
172.16.100.190	multisv001.pippo.com	21, 80
172.16.100.191	multisv002.pippo.com	21, 80
172.16.100.212		21, 80
172.16.100.231	ayoka.pippo.com	21, 80
172.16.101.123		21, 80
172.16.101.181	multisv010.pippo.com	21, 80
172.16.101.182		21, 80
172.16.100.186	dboracletst.pippo.com	21, 8080
172.16.101.122	multisv007.pippo.com	21, 8080

LAN Marcianise

IP Address	Host Name	Port
192.168.8.1		21, 23, 80
192.168.8.4	plus07.pippo.com	21
192.168.8.5	plus09.pippo.com	21
192.168.8.7	gemma.pippo.com	21
192.168.8.6	apalmieri.pippo.com	21
192.168.8.10	plus01.pippo.com	21, 80
192.168.8.12	plus03.pippo.com	21
192.168.8.11	plus06.pippo.com	21
192.168.8.13		21
192.168.8.15	plus05.pippo.com	21
192.168.8.16	plus02.pippo.com	21
192.168.8.26		21
192.168.8.28		21
192.168.8.27		21
192.168.8.29		21
192.168.8.50		21, 23, 80

WAN Pippo

IP Address	Host Name	Port
85.43.190.193	host193-190-static.43-85-b.business.telecomitalia.it	
85.43.190.198	mail.pippo.com	110, 25, 443, 80
85.43.190.199	host199-190-static.43-85-b.business.telecomitalia.it	110, 21, 25, 443, 80
85.43.190.197	host197-190-static.43-85-b.business.telecomitalia.it	110, 25, 80
85.43.190.200	host200-190-static.43-85-b.business.telecomitalia.it	110, 25, 80
85.43.190.202	host202-190-static.43-85-b.business.telecomitalia.it	110, 25, 80
85.43.190.203	host203-190-static.43-85-b.business.telecomitalia.it	
85.43.190.201	host201-190-static.43-85-b.business.telecomitalia.it	110, 25, 80
85.43.190.204	host204-190-static.43-85-b.business.telecomitalia.it	
85.43.190.205	host205-190-static.43-85-b.business.telecomitalia.it	110, 25, 80
85.43.190.194	host194-190-static.43-85-b.business.telecomitalia.it	110, 25, 80
85.43.190.192	host192-190-static.43-85-b.business.telecomitalia.it	
85.43.190.195	host195-190-static.43-85-b.business.telecomitalia.it	110, 25, 80
85.43.190.196	host196-190-static.43-85-b.business.telecomitalia.it	22
85.43.190.206	host206-190-static.43-85-b.business.telecomitalia.it	
85.43.190.207	host207-190-static.43-85-b.business.telecomitalia.it	

5.3 Shared Folder

Abbiamo anche verificato l'esistenza di risorse shared sulla rete e il riscontro è stato positivo in alcuni casi ma anche qui spetta al responsabile sistemi informativi comprenderne o meno la gravità di poter accedere a delle cartelle e dei file su cui poter anche scrivere senza alcuna policy di file system.

IP Address	Host Name	Shared Folders
172.16.100.2	ws1018	AZ001 (readonly), server (readonly), IPC$ (ipc), ADMIN$ (password), C$ (password), E$ (password), BackupOpen (writable), SYNCCLIENT (writable), Documenti (writable), SyncServer (writable)
172.16.100.4	lgaudio.pippo.com	commerciali$ (readonly), s.informativi (password), pippo (password), s.riunioni (password), support_388945a0 (password), 881b1ad4-0366-4448-a (password), root (password), logistica (password), consumatori (password), deco526 (password), deco1570 (password), retevendita (password), sviluppofranchising (password), portale (password), iusr_multisv002 (password), f.autuori (password), g.barbano (password), denovellis (password), a.gasparrino (password), s.carnevale (password), c.ienco (password), n.dangelo (password), administrator (password), krbtgt (password), iusr_multisv001 (password), guest (password), tomei (password), multiadm1 (password), multiadm2 (password), deco1566 (password), l.sagliocco (password), f.rucco (password), a.coco (password), retedettaglio (password), scanner (password), adhocash (password), ordini (password), g.stagliano (password), ordcli1 (password), l.masotti (password), e.palmas (password), s.oscurato (password), v.dipalo (password), g.ursillo (password), g.caimano (password), m.dirubba (password), m.ferraro (password), n.lamberti (password), g.pezzella (password), multinvest_cedi (password), b.piscitiello (password), g.dilillo (password), fidelity (password), deco711 (password), deco469 (password), a.dimaio (password), r.dilillo (password), s.delprete (password), v.marra (password), c.adduci (password), cdauser (password), a.martello (password), reception (password), m.palumbo (password), m.zito (password), g.delia (password), s.maresca (password), rifatturazione (password), c.albano (password), a.milone (password), m.bernardo (password), s.giannini (password), s.cioppa (password), r.derosa (password), c.suberino (password), p.stolfi (password), a.sangermano (password), g.tornesi (password), p.basso (password), g.russo (password), m.lombardi (password), l.trabucco (password), l.spagnuolo (password), f.distefano (password), s.dellarocca (password), u.bellini (password), v.compagnone (password), v.romano (password), s.russo (password), p.miele (password), f.delucabossa (password), n.iacovelli (password), g.giarretta (password), l.liccardi (password), a.ciavattone (password), s.palmieri (password), f.marano (password), a.palmieri (password), v.caliendo (password), freschi (password), r.severi (password), a.merola (password), e.mandara (password), v.amatucci (password), a.sangiovanni (password), a.sammarco (password), r.genatiempo

		(password), m.vitale (password), ultrafreschi (password), surgelati (password), f.cucco (password), a.marino (password), m.gemma (password), a.rocco (password), m.autiero (password), s.cepparulo (password), e.romano (password), a.trepiccione (password), deco2155 (password), plus05 (password), deco2188 (password), developer (password), deco2099 (password), t.lemma (password), deco2130 (password), EDP$ (password), Ittico$ (password), ufficio tecnico$ (password), direzione$ (password), f.falace (password), adhoc$ (password), amministrazione$ (password), plus01 (password), plus03 (password), plus06 (password), deco1899 (password), helpretevendita (password), helpcontabilita (password), p.palmieri (password), irollo (password), plus02 (password), c.mazzola (password), muletto (password), help (password), deco1177 (password), u.legale (password), magazzino$ (password), a.nuzzo (password), a.russo (password), ayoka (password), c.desimone (password), bckoldcommon (password), fedora (password), w.zanghi (password), r.robusto (password), deco1890 (password), IPC$ (password), deco2270 (password), b.ganzerli (password), deco2266 (password), deco2277 (password), Marketing$ (password), deco2211 (password), deco2190 (password), multinvest$ (password), sysinfo$ (password), Pluservice$ (password), ortofrutta$ (password), deco2244 (password), Personale (password), d.melluso (password), d.lanna (password), Ufficio Premi (password), provvisoria (password), v.salvetti (password), m.leuci (password), deco1660 (password), deco1616 (password), l.sarnataro (password), retedettaglio1 (password), mari (password), a.sacco (password), multinvestaversa (password), openteam (password), p.nappo (password), c-sannitica-limatola (password), deco1670 (password), commercialesannitica (password), c-sannitica-airola (password), g.cioppa (password), trasmissioni (password), fax (password), m.zurolo (password), g.trepiccione (password), s.dirauso (password), attila (password), f.margarita (password), g.aufieri (password), servizio.clientideco (password), videocontrollo (password), pluservice (password), sipe (password), fax1 (password), m.normando (password), domini (password), m.dellovo (password), ragozzino (password), deco1940 (password), v.fusco (password), deco1922 (password), deco590 (password), deco1888 (password), helpportale (password), helphardware (password), helplogistica (password), helpcommerciale (password), deco1970 (password), l.gaudio (password), s.dilillo (password), a.velona (password), tesoreria (password), sindaci (password), m.nardiello (password), l.ruotolo (password), v.vitale (password), g.loffredo (password), riscontro (password), iwam_multisv002 (password), c.capolupo (password), deco1930 (password), iwam_multisv001 (password), deco547 (password), Backups (writable), public (writable), domain (writable), common$ (writable)
172.16.100.6	vmarra.pippo.com	HPColorL (printer), HPColorL.2 (printer), KONICAMI (printer), HPLaserJ (printer), ENERJ (readonly), print$ (readonly), IPC$ (ipc), report (password), C$ (password), E$ (password), FatturePro (password), ADMIN$ (password), FileBatch (password), Error (writable), PreScanner (writable), In (writable), Pre

		(writable)
172.16.100.7	cepparulonew.pippo.com	HPLaserJ (printer), OKI_Cioppa (printer), print$ (readonly), IPC$ (ipc), C$ (password), ADMIN$ (password), SharedDocs (writable)
172.16.100.8	mag081new.pippo.com	IPC$ (ipc), C$ (writable), ADMIN$ (writable)
172.16.100.10	rseveri.pippo.com	IPC$ (ipc), OPTICON (password), TCOM201 (password), ORDINI (password), AMODIO (password), ORDINIAM (password), MARIO (writable)
172.16.100.11	atrepiccione.pippo.com	IPC$ (password), print$ (password)
172.16.100.12	mautieronew.pippo.com	OSCURATO (password), IPC$ (password), PUBLIC (writable), MARKETING (writable)
172.16.100.13	mellusonb.pippo.com	REPERTI (password), IPC$ (password), BACKUPORACLE (writable), PUBLIC (writable), BACKUPFILESERVER (writable), BACKUPDBSERVER (writable)
172.16.100.15	scarnevale.pippo.com	Stampante (printer), Stampante2 (printer), OKIB410 (printer), print$ (readonly), IPC$ (ipc), C$ (password), ADMIN$ (password), SharedDocs (writable), W98_01_C (writable)
192.168.8.5	plus09.pippo.com	IPC$ (ipc), ADMIN$ (password), C$ (password), Documenti (writable)
192.168.8.7	gemma.pippo.com	HPLaserJ.2 (printer), HP1020 (printer), HPLaserJ (printer), Documenti (readonly), print$ (readonly), IPC$ (ipc), C$ (password), ADMIN$ (password)

6 SICUREZZA E TIPOLOGIA DI TRAFFICO DI RETE

6.1 Attacchi

I passi tipici di un attacco sono:

- Identificare il sistema da attaccare (per trovare il punto più vulnerabile e le modalità d'attacco)
- Ottenere un accesso utente (per penetrare nel sistema e tentare di ottenere accessi privilegiati)
- Ottenere un accesso privilegiato (per prendere il controllo completo del sistema tramite un attacco diretto a servizi o account con questi livelli)
- Coprire le proprie tracce (in modo che non sia possibile risalire all'attaccante e agli eventi esaminando i log del sistema)
- Installare backdoors (per rientrare nel sistema qualora venga individuato e/o eliminato il precedente metodo di penetrazione)
- Attaccare altri sistemi (una volta resosi anonimo e non individuabile)
- Prendere o alterare informazioni (presenti sulla macchina o sulla rete)
- Attuare altre attività non autorizzate (al fine di procurarsi un vantaggio o profitto)

6.2 Soluzioni

Chiunque può rimanere vittima di un'intrusione o un attacco!
Le ragioni di questa affermazione possono anche sfuggire a chi si considera "low profile" o non comprende bene l'importanza dei dati che custodisce sui propri sistemi.
Sono estremamente diffusi nelle comunità hacker tool che permettono di verificare con estrema facilità ed in breve tempo la presenza di determinate vulnerabilità partendo da un elenco "pseudocasuale" di ip (per esempio, tutti i domini.it, oppure tutte le macchine della subnet 151.4.*.*, etc.).
Esistono soluzioni hardware e software ma, per la natura intrinseca di questi prodotti, non saranno mai sufficienti al problema.
Non esiste e non esisterà mai una soluzione definitiva.

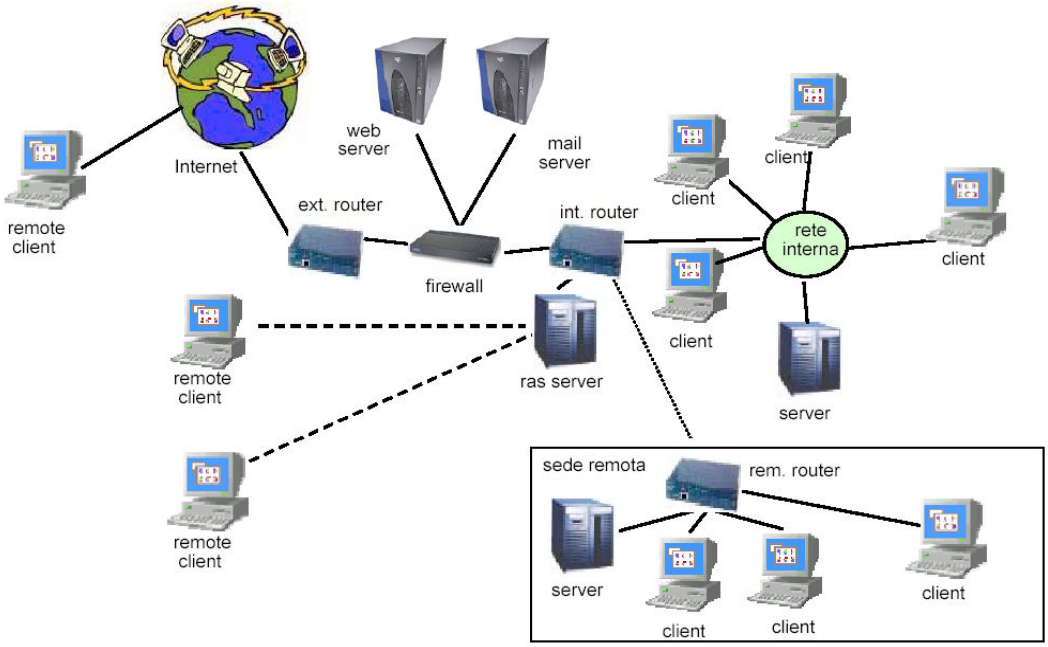
La sicurezza di un sistema viene valutata dalla resistenza del suo anello più debole, per ottenere un sistema che riesca a garantire al meglio gli obbiettivi di sicurezza richiesti, bisogna valutare nelle varie componenti i rischi che si vengono a generare, tenendo conto dei livelli di protezione che vengono garantiti.

6.3 Sovrabbondanza di informazioni

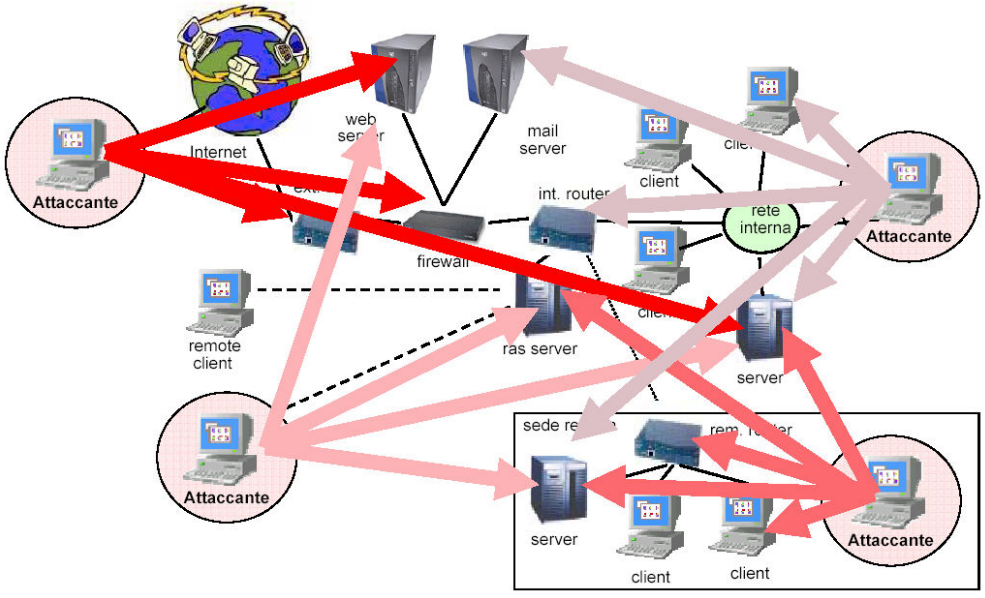
Le informazioni che consideriamo banali o di scarsa importanza, possono risultare invece estremamente interessanti per altri, spesso si ignora quale sovrabbondanza di dati passi tramite le legittime informazioni considerate pubbliche:

- versione di S.O.
- tipo e versione applicativi
- utenti e gruppi
- configurazione zone DNS
- configurazione SMTP
- servizi di informazioni erroneamente accessibili come SNMP, NetBIOS, sunrpc, finger

Tutti i servizi superflui e le informazioni che sono liberamente accessibili sono un potenziale problema per la sicurezza dell'intero sistema.
La non conoscenza o la diffusione di informazioni false aiuta in minima parte a mantenere la sicurezza e viene definita come "Security through obscurity" e guardata con superiorità dai puristi della sicurezza, comunque può essere uno degli strumenti utili per ottenere lo scopo di sicurezza che ci si prefigge.
E' comunque consigliabile impedire l'accesso a tutte le informazioni superflue per mantenere la sicurezza dei sistemi.
Questa è una rete che funziona…….ma…..


Internet
web server
mail server
remote client
ext. router
firewall
int. router
client
client
rete interna
client
client
remote client
ras server
server
remote client
sede remota
rem. router
server
client
client
client

….è sicura ?


Attaccante
Internet
web server
mail server
client
int. router
rete interna
Attaccante
firewall
remote client
ras server
server
Attaccante
server
client
client
Attaccante

La tipologia di attacco che va sotto il nome di man-in-the-middle consiste nel dirottare il traffico generato durante la comunicazione tra due host verso un terzo host (attaccante) il quale fingera' di essere l'end-point legittimo della comunicazione. Il tipico attacco man in the middle è cosi strutturato:
vi è la vittima, il cattivo ed il server dhcp. La vittima fa una richiesta di IP address, a chi risponde prima gli viene assegnato un indirizzo IP e un gateway che corrisponde ad una certa interfaccia (gli diamo dei parametri nostri). Da questo punto in poi tutte le comunicazioni della vittima passano qui, io me le leggo e per non farmi accorgere di nulla le mando a chi le devo mandare, ricevo la risposta e leggo anche la risposta. Questa tipologia di attacco si chiama MAN IN THE MIDDLE e si applica a diversi contesti ed ha come caratteristica l'avere qualcosa in mezzo tenendo conto sempre che ci troviamo sempre sul layer 2 principalmente.
Qual è può essere l'obiettivo dell'attaccante?
Rubare le credenziali oppure memorizzare tutto il traffico che un utente fa con un altro utente.

Un aiuto fondamentale può arrivare proprio dalla suddivisione dei singoli domini di broadcast onde evitare scansioni di livello 2 in presenza di server sullo stesso dominio, anche l'assegnazione del DHCP non dovrebbe essere disponibile a tutti coloro che si connettono in rete, onde evitare i problemi che ne possono derivare da tool disponibili che consentirebbero di arrecare danno alla rete stessa.

Una volta connessi gli ospiti possono utilizzare tutti i protocolli tranne http/https anche senza autenticazione

7 CONCLUSIONI

In conclusione riprendiamo alcuni punti fondamentali analizzati durante i precedenti capitoli e che sono:

- Collegamento tra gli switch di Centro Stella
- Verifica configurazione SPT
- Aggiornamento Firmware apparati Cisco
- Omogeneizzare Community SNMP
- Rete Wireless aperta
- Rete wireless ridistribuzione segnali
- Device 172.16.100.165 MULTINVESTFTP se possibile connettere in Gb
- Verifica collegamento UPS CED
- Verifica DNS zone
- Collegamento ospiti nessun blocco tranne http/https
- Verifica porte TCP aperte
- Verifica Shared condivise
- Verificare compliance con documento programmatico DPS

Tutte le aziende devono redigere il DPS in base alla legge 196/03 e farne menzione a bilancio, il documento prevede l'implementazione dei minimi requisiti di sicurezza che in questo caso vengono a mancare. E' stato modificato ulteriormente per l'anno 2009 includendo anche la parte di controllo dettato dalla legge 231 contro i crimini informatici e quindi i client di rete devono avere un controllo molto serrato sulle attività svolte.

Alleghiamo alla presente relazione:

- nbinv.xls
- user.xls
- network generale.vsd
- network core.vsd
- multifarm 172_16_100_82.vsd
- multimag1 172_16_100_83.vsd
- multimag2 172_16_100_84.vsd
- multinvfarm 172_16_100_81.vsd
- swced1 172_16_100_240.vsd
- swced2 172_16_100_241.vsd
- swced3 172_16_100_242.vsd

- swced4 172_16_100_243.vsd
- swced5 172_16_100_247.vsd
- swced6 172_16_100_233.vsd
- swced7 172_16_100_238.vsd
- swced8 172_16_100_245.vsd
- swced9 172_16_100_246.vsd
- swced10 172_16_100_239.vsd
- swced12 172_16_100_85.vsd
- swced13 172_16_100_86.vsd
- swvmvest 1 172_16_101.128.vsd
- swvmvest 2 172_16_101.129.vsd
- swvmvest 3 172_16_101.130.vsd
- swvmvest 4 172_16_101.131.vsd