White Paper.

Lesson 5: Open Port – Protocolli layer 2 – Condivisione Rete

Security Audit: l'analisi di rete

L'esponenziale crescita dell'ICT (Information Communication Technologies) e il pervasivo aumento di reti per l'interconnessione dei sistemi informativi, impongono un'ostinata attenzione agli aspetti legati alla sicurezza informatica.

Non crea certo meraviglia il numero di personal computer compromessi, che ha subito in questi ultimi anni un aumento esponenziale, così come le reti di prestigiose organizzazioni violate oppure addirittura fermate perché oggettivamente non più sicure. Indietro ormai non si torna.
I computer rappresentano la nostra modalità di trasmissione dei dati. A loro abbiamo affidato il nostro business e ancora peggio il nostro **KNOW HOW**. Come fare allora per proteggersi?

Scopo della lezione è proprio quello di analizzare in prima persona le vulnerabilità a cui i nostri computer sono esposti, provare a identificarle e insieme cercare qualche strumento per difenderci magari in modo preventivo. L'argomento principale sarà quindi il **vulnerability scanning**.

E' meglio chiarire subito che per "vulnerability scanning" intendiamo esclusivamente "l'analisi lecita" della nostra rete o comunemente definito **forensic analysis**.

Non è nostra intenzione offrire i mezzi e le conoscenze per sferrare attacchi informatici illeciti.
A tal proposito ricordiamo che:

"l'accesso abusivo a sistemi informatici è un reato punito dal codice penale".

Gli strumenti messi a disposizione dalla comunità del software libero per analizzare e quindi **contrastare** le possibili vulnerabilità di un sistema sono molteplici.

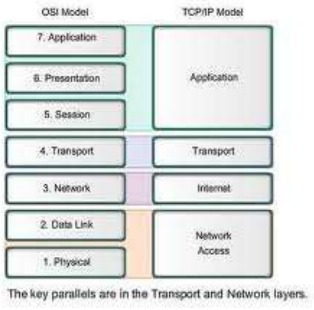
L'esposizione dei nostri sistemi ai rischi di attacchi **è una nostra responsabilità**, ignorare il problema non ci solleva dalle conseguenze che ne derivano. Le normative vigenti richiedono tra l'altro di tutelare l'utilizzatore dei sistemi e di garantirne la privacy. Molto spesso si tende a sottovalutare la cosa ma è fondamentale ricordarsi che quanto evidenziato…….

"spetta per legge al proprietario/gestore del sistema informativo".

Prima di procedere con l'argomento della lezione è bene chiarire che la quasi totalità delle reti dati utilizza come linguaggio lo **Stack TCP/IP**, per cui comprendere a pieno le sue modalità funzionali significa anche capire le possibili criticità. E' fondamentale conoscere la lingua per capirne i contenuti. Nel particolare ci soffermeremo sui due principali protocolli, il **TCP** e l'**UDP**.

Descrizione

Il **TCP** (Trasmission Control Protocol) può essere parificato al livello di trasporto (OSI level 4) del modello di riferimento OSI, e di solito è usato in combinazione con il protocollo di livello di rete (OSI level 3) **IP** (Internet Protocol). La corrispondenza con il modello OSI non è perfetta, in quanto il **TCP** e l'**IP** nascono prima del suddetto modello. La combinazione dei due livelli è comunemente indicata come TCP/IP.



The key parallels are in the Transport and Network layers.

EterNet
Vitalize your IT

Spesso è erroneamente considerato un unico protocollo. Da qui, la difficoltà di una classificazione univoca per un protocollo che comprende, a pieno titolo, due livelli completi dello Stack OSI.

Confronto con UDP

Le principali differenze tra **TCP** e **UDP** (*User Datagram Protocol*), quest'ultimo principale protocollo di trasporto della suite di protocolli Internet, sono:

- il TCP è un protocollo orientato alla connessione, pertanto per stabilire, mantenere e chiudere una connessione, è necessario inviare pacchetti di servizio i quali aumentano "l'overhead" di comunicazione. Al contrario, l'UDP è senza connessione e invia solo i datagrammi richiesti dal livello applicativo.
- L'UDP non offre nessuna garanzia sull'affidabilità della comunicazione ovvero sull'effettivo arrivo dei datagrammi e sul loro ordine in sequenza ed in arrivo. Al contrario il TCP, tramite i meccanismi di "acknowledgement" e di ritrasmissione su timeout, riesce a garantire la consegna dei dati, anche al costo di un maggiore overhead (raffrontabile visivamente confrontando la dimensione delle intestazioni dei due protocolli).
- L'oggetto della comunicazione di TCP è il flusso di byte, mentre quello di UDP è il singolo datagramma.

Pacchetto TCP

Vediamo velocemente insieme come è fatto un pacchetto TCP.

TCP Header

Bit offset	Bits 0–3	4–7	8–15	16–31
0	Source port			Destination port
32	Sequence number			
64	Acknowledgment number			
96	Data offset	Reserved	CWR ECE URG ACK PSH RST SYN FIN	Window Size
128	Checksum			Urgent pointer
160	Options (optional)			
160/192+	Data			

Gli argomenti che tratteremo ora sono i seguenti:

- **Port Scanning**: rilevazione porte TCP/UDP aperte (pericoli in agguato).
- **Sniffer**: rilevazione di protocolli che generano broadcast o multicast a livello 2.
- **Shared di rete**: permessi e accessi a cartelle condivise.

Port Scanning

In informatica il Port Scanning è una tecnica utilizzata per raccogliere informazioni su un computer connesso ad una rete stabilendo quali e quante porte sono in ascolto sulla macchina esaminata. Letteralmente significa "scansione delle porte" e consiste nell'inviare richieste di connessione al computer bersaglio (soprattutto pacchetti TCP, UDP e ICMP creati ad arte). Elaborando le risposte è possibile stabilire, anche con precisione, quali servizi di rete sono attivi su quel computer. Una porta si dice "in ascolto" (listening) o "aperta" quando vi è un servizio o programma che la usa. Di per sé il port scanning non è pericoloso per i sistemi informatici, e viene comunemente usato dagli amministratori di sistema per effettuare controlli e manutenzione.

Il suo impiego rivela però informazioni dettagliate che potrebbero essere facilmente usate da un eventuale attaccante per preparare una tecnica mirata a minare la sicurezza del sistema. Per questo viene posta molta attenzione dagli amministratori a come e quando vengono effettuati port scan verso i computer della loro rete. Un buon amministratore di sistema sa che un firewall ben configurato permette alle macchine di svolgere tutti i loro compiti, ma rende difficile, se non impossibile, la scansione delle porte. E' possibile comunque procedere implementando ad esempio, meccanismi di accesso selettivo basati sul **port knocking**.

TCP Port

Le porte sono numeri (TCP e UDP riservano 16 bit per un totale di 2^16=65536 porte possibili) utilizzati per identificare una particolare connessione di trasporto tra quelle al momento attive su un calcolatore.
I pacchetti appartenenti ad una connessione sono identificati dalla seguente quadrupla: **[<indirizzo IP sorgente>, <indirizzo IP destinazione>, <porta sorgente>, <porta destinazione>]**.
I pacchetti nella direzione opposta avranno ovviamente sorgente e destinazione scambiati.
Mentre la porta di destinazione è l'identificativo univoco del processo applicativo, la porta di sorgente è assegnata casualmente in maniera tale da identificare univocamente la connessione da parte del mittente col destinatario all'interno di una rete locale.
Il livello di trasporto (tipicamente realizzato dal sistema operativo) associa a ciascuna porta utilizzata un punto di contatto (ad esempio, una socket), utilizzata da uno o più processi applicativi per trasmettere e/o ricevere dati.
Per poter inviare con successo un pacchetto con una certa porta destinazione, ci deve essere un processo che è "in ascolto" su quella porta, ovvero che ha chiesto al sistema operativo di ricevere connessioni su quella porta.
La porta sorgente utilizzata in una connessione viene scelta dal calcolatore che inizia la connessione tra una di quelle al momento non impegnate.
In Internet, c'è una convenzione per cui ad alcuni numeri di porta sono associati determinati protocolli di livello applicativo. Ad esempio: se voglio contattare il server HTTP eventualmente in esecuzione su un certo calcolatore, so che devo tentare di stabilire una connessione verso la porta 80. I numeri di porta sono classificabili in tre gruppi:

- Le porte conosciute, assegnate dall'Internet Assigned Numbers Authority (IANA), sono quelle inferiori a 1024, e sono generalmente utilizzate a livello di sistema operativo o di processi di sistema.

In genere rimangono in ascolto su queste porte applicazioni con funzioni di server. Alcuni esempi possono essere le applicazioni che utilizzano protocolli FTP (21), SSH (22), TELNET (23), SMTP (25) e HTTP (80). Sono dette porte ben note.

- Le porte registrate invece sono spesso utilizzate come riferimento fra applicazioni, come una specie di accordo.
- Le porte dinamiche sono tutte le altre. Sono liberamente utilizzabili da tutte le applicazioni utente, salvo l'occupazione contemporanea da parte di qualche altro processo.

Le porte più comuni

Supervisionare le porte "in ascolto" cioè aperte è di estrema importanza sul fronte della sicurezza dei dati per evitare attacchi informatici che nel caso più grave possono portare al controllo completo del computer da parte dell'intruso. Le porte normalmente più vulnerabili sono quelle legate a servizi e applicazioni di cui abbiamo già parlato nelle lezioni precedenti:

- Servizi di Login: Telnet (23/TCP), SSH (22/TCP), NetBIOS (139/TCP), ecc.
- Posta: SMTP (25/TCP), POP (109/TCP e 110/TCP), IMAP (143/TCP), ecc.
- Web: HTTP (80/TCP) e SSL (443/TCP, tranne quelle verso i server web esterni. Si dovrebbero bloccare anche le porte HTTP comuni (8000/TCP, 8080/TCP, 8888/TCP e così via)
- Piccoli servizi: porte prima delle 20/TCP e 20/UDP, NTP(TCP/UDP:123)

Ecco un elenco delle principali porte:

Porta	Descrizione
1/tcp	TCP Multiplexor
2/tcp	compressnet Management Utility
3/tcp	compressnet Compression Process
7/tcp	Echo Protocol
7/udp	Echo Protocol
8/udp	Bif Protocol
9/tcp	Discard Protocol
9/udp	Discard Protocol
13/tcp	Daytime Protocol
17/tcp	Quote of the Day
19/tcp	Chargen Protocol
19/udp	Chargen Protocol
20/tcp	FTP - Il file transfer protocol - data
21/tcp	FTP - Il file transfer protocol - control
22/tcp	SSH - Secure login, file transfer (scp, sftp) e port forwarding
23/tcp	Telnet insecure text communications
25/tcp	SMTP - Simple Mail Transfer Protocol (E-mail)
53/tcp	DNS - Domain Name Server
53/udp	DNS - Domain Name Server
67/udp	BOOTP Bootstrap Protocol (Server) e DHCP Dynamic Host Configuration Protocol (Server)
68/udp	BOOTP Bootstrap Protocol (Client) e DHCP Dynamic Host Configuration Protocol (Client)
69/udp	TFTP Trivial File Transfer Protocol
70/tcp	Gopher

79/tcp	finger Finger
80/tcp	HTTP HyperText Transfer Protocol (WWW)
88/tcp	Kerberos Authenticating agent
104/tcp	Dicom - Digital Imaging and Communications in Medicine
110/tcp	POP3 Post Office Protocol (E-mail)
113/tcp	ident vecchio sistema di identificazione dei server
119/tcp	NNTP usato dai newsgroups usenet
123/udp	NTP usato per la sincronizzazione degli orologi client-server
137/udp	NetBIOS Name Service
138/udp	NetBIOS Datagram Service
139/tcp	NetBIOS Session Service
143/tcp	IMAP4 Internet Message Access Protocol (E-mail)
161/udp	SNMP Simple Network Management Protocol (Agent)
162/udp	SNMP Simple Network Management Protocol (Manager)
389/tcp	LDAP
411/tcp	Direct Connect Usato per gli hub della suddetta rete
443/tcp	HTTPS usato per il trasferimento sicuro di pagine web
445/tcp	Microsoft-DS (Active Directory, share di Windows, Sasser-worm)
445/udp	Microsoft-DS SMB file sharing
465/tcp	SMTP - Simple Mail Transfer Protocol (E-mail) su SSL
500/udp	IKE chiave di scambio Internet. associazione di sicurezza nella suite di protocolli IPSec
514/udp	SysLog usato per il system logging
563/tcp	NNTP Network News Transfer Protocol (newsgroup Usenet) su SSL
591/tcp	FileMaker 6.0 Web Sharing (HTTP Alternate, si veda la porta 80)
631/udp	IPP / CUPS Common Unix printing system
636/tcp	LDAP su SSL
636/udp	LDAP su SSL
666/tcp	Doom giocato in rete via TCP
993/tcp	IMAP4 Internet Message Access Protocol (E-mail) su SSL
995/tcp	POP3 Post Office Protocol (E-mail) su SSL

Classificazione delle porte

I sistemi di port scanning classificano le porte secondo queste 6 categorie (nmap):

- **Open** (aperta)
- **Closed** (chiuse)
- **Filtered** (filtrata)
- **Unfiltered** (non filtrata)
- **Open|filtered** (aperta|filtrata)
- **Closed|filtered** (chiusa|filtrata)

Questi stati non sono proprietà intrinseche delle porte stesse, ma descrivono come i port scanning le vedono. Ad esempio, uno scan Nmap proveniente dalla stessa rete nella quale risiede l'obbiettivo può mostrare la porta 135/tcp come aperta, mentre una scansione nello stesso momento con gli stessi parametri ma proveniente da internet può mostrare quella stessa porta come filtered.

Open: un'applicazione accetta attivamente su questa porta connessioni TCP o UDP. La ricerca di questo tipo di porte è spesso l'obbiettivo primario del port scanning. Chi si dedica alla sicurezza sa che ogni porta aperta può diventare una strada per un possibile attacco. Gli attaccanti e i tester di sicurezza (penetration testers), conosciuti anche come "pen-testers" hanno come obbiettivo quello di trovare e trarre vantaggio dalle porte aperte, mentre d'altro canto gli amministratori di rete e i sistemisti provano a chiuderle o a proteggerle con firewall cercando di limitare il meno possibile gli utenti autorizzati al loro uso. Le porte aperte sono anche interessanti per tutta una serie di scansioni non indirizzate unicamente alla sicurezza ma perché mostrano i servizi disponibili sulla rete.

Closed: una porta chiusa è comunque accessibile (riceve e risponde ai pacchetti di probe) ma non vi è alcuna applicazione in ascolto su di essa. Si rendono utili perché possono mostrare l'attività di un host su un particolare indirizzo IP (host discovery o ping scanning), oppure per evidenziare le tipologie di sistemi operativi installati (operating system discovery). Poiché una porta chiusa rimane raggiungibile, per verificare se queste vengono aperte è sempre consigliato effettuare scansioni a posteriori. Chi amministra una macchina o una rete può bloccare tali porte con un firewall che, in questo caso, le farebbe apparire "filtrate", come mostrato in seguito.

Filtered: in questo caso non si può determinare con esattezza se la porta sia aperta o meno, perché un filtro attivo sui pacchetti in transito impedisce ai probe di raggiungere la porta. Questo filtro può esser dovuto a un firewall dedicato, alle regole di un router, o a un firewall software installato sulla macchina stessa. Per loro natura queste porte forniscono poche informazioni e rendono frustrante il lavoro dell'attaccante. Questa tipologia di porta a volte può rispondere con un messaggio ICMP del tipo 3, codice 13 ("destination unreachable: communication administratively prohibited", ovvero "destinazione non raggiungibile: comunicazione impedita da regole di gestione"). In genere è molto più comune il filtraggio di tutti i pacchetti che semplicemente ignorano i tentativi di connessione senza rispondere. Questa modalità di "non risposta" obbliga a riprovare molte volte, semplicemente per essere sicuri che il pacchetto non sia stato perduto a causa di una congestione di rete o di problemi simili piuttosto che dal firewall o dal filtro stesso. Questo riduce drammaticamente la velocità della scansione.

Unfiltered: lo stato "unfiltered" indica che una porta è accessibile, ma che non siamo in grado di determinarne lo stato di aperta o chiusa. Solo la scansione di tipo ACK, usata per trovare e classificare le regole di un firewall, può correttamente indicare una porta in questo stato. Una ricerca di porte in questo stato ("non filtrate") mediante altri tipi di scansione come il "Window scan" (scan per finestre di connessione), il "SYN scan" o il "FIN scan" aiuta a determinare se la porta sia aperta o chiusa.

Open|filtered: la porta rilevata in questo stato non consente di determinare se sia aperta o filtrata. Questo accade quando una porta aperta non risponde in alcun modo. La mancanza di informazioni potrebbe anche significare che un filtro di pacchetti ha lasciato cadere ("drop") il probe o qualsiasi risposta sia stata generata in seguito. Le ricerche che classificano porte in questo stato sono le scansioni IP, UDP, FIN, Null, e Xmas.

Closed|filtered: questo stato è usato quando non si è in grado di determinare se una porta sia chiusa o filtrata. Esso viene usato solo per l'IPID "Idle scan".

Sniffing

Tutto ciò che è trasferito e lasciato circolare in una rete è suddiviso e ”incapsulato” in unità ben definite chiamate “pacchetti”. Ogni pacchetto viene etichettato con un indirizzo IP e/o un indirizzo MAC che specifica la sua destinazione, e ad esso sono associati altri parametri (header) che serviranno ad instradare e riassemblare i pacchetti, operazione compiuta dalla macchina del destinatario. Poiché tutto il traffico di una rete deve essere ridotto in pacchetti lo **sniffer** non deve far altro che raccogliere tale traffico e analizzarlo sia nella sua forma frammentata sia nella sua forma riassemblata, alla ricerca delle informazioni a cui si mira.
Le funzioni tipiche degli **sniffer** possono sinteticamente essere riassunte in:

- filtraggio e conversione dei dati e dei pacchetti in una forma leggibile dall'utente;
- analisi dei difetti di rete, ad es. perché il computer A non riesce a dialogare con B;
- analisi di qualità e della quantità dei dati trasportati dalla rete (performance analisys);
- ricerca automatizzata di password e nomi di utenti (in chiaro o cifrati) per successiva analisi;
- creazione di log: lunghi elenchi contenenti traccia del traffico sulla rete;
- scoperta di intrusioni in rete attraverso l’analisi dei log del traffico.

Livelli di rischio

Gli **sniffer** rappresentano un rischio elevato per una rete o per il PC dell'utente medio. La semplice esistenza di uno **sniffer** in rete rappresenta una falla e una minaccia alla sicurezza e alla riservatezza delle comunicazioni all'interno della rete stessa. Quando la LAN che si utilizza è sottoposta al controllo di uno **sniffer** ci sono di solito due possibilità:

1. un intruso, dall'esterno, è riuscito ad entrare all'interno della rete e ad installare lo sniffer;
2. oppure un utente o il gestore della rete stessa sta combinando qualcosa che potrebbe andare ben oltre la manutenzione e il monitoraggio delle connessioni.

In ogni caso la privacy, o peggio, la sicurezza stessa delle comunicazioni, è compromessa.

TCP/IP agevola gli sniffer

TCP/IP non offre nessun meccanismo di verifica o protezione dei dati. I dati viaggiano in chiaro e non è fornito nessun modo per garantire l'autenticità degli interlocutori, sebbene ciò possa essere fatto dalle applicazioni. Ciascuna macchina su cui viaggiano i dati potrebbe visualizzarli o anche modificarli. Se un'applicazione gestisce a basso livello la connessione può addirittura falsificare la propria identità (man in the middle) in quanto TCP/IP si ***fida*** semplicemente dell'indirizzo specificato dal mittente. Anche a livello applicativo non vengono adottati automaticamente strumenti per garantire l'autenticità e la privacy dei dati.

Utilità dello sniffer

Ovviamente uno degli scopi della lezione non è quello di impiegare lo **sniffer** per acquisire informazioni perché abbiamo parlato di questa possibilità nelle lezioni precedenti. L’obiettivo è invece quello di utilizzare lo strumento per identificare gli eventuali problemi della nostra rete. Uno **sniffer** deve essere solitamente connesso ad un dominio di collisione, ad un hub o, se si utilizza uno switch, ad una porta configurata in monitor sugli apparati di rete di layer 2.

In questo modo viene filtrato tutto il traffico in transito da una specifica porta.
L'utilizzo invece da noi consigliato è quello di attivarlo connessi alla propria rete aziendale in modo da verificare quali pacchetti raggiungono la nostra interfaccia di rete in quanto broadcastati sulla stessa e che potrebbero rappresentare un problema. Alcune applicazioni o una rete mal costruita, possono generare un traffico anomalo a livello 2, quindi può capitare di ricevere pacchetti che per loro natura generano traffico e rallentano le prestazioni della nostra rete.

Analisi

L'analisi dei pacchetti ricevuti è fondamentale per individuare ed isolare il problema. Quanto espresso nel precedente capitolo inerente alle porte TCP/UDP aperte è in stretta correlazione con l'utilizzo dello sniffer quale strumento utile all'identificazione dei protocolli dannosi o applicazioni mal configurate. L'uso di sistemi come le chat, diffuse in molti social network, potrebbe aprire altre porte di comunicazione che, senza un controllo adeguato, potrebbero rappresentare una strada per fare entrare software molto pericolosi. Al fine di ridurre il livello di potenziale vulnerabilità delle macchine di una rete (ma anche di una singola macchina), è opportuno verificare che siano attivi soltanto i servizi e/o protocolli necessari. La presenza di elementi superflui, infatti, rappresenta una grave minaccia alla sicurezza.

Una buona abitudine è quella di verificare periodicamente questo genere di cose sia durante il processo di installazione del sistema operativo, sia in seguito, al fine di assicurarsi che non siano stati attivati, anche involontariamente, servizi e/o protocolli non necessari. La presenza di elementi del genere non utilizzati, apre verso l'esterno un certo numero di porte TCP/IP, che diventano fonte di numerosi problemi sia sotto l'aspetto delle prestazioni, in quanto la loro presenza consuma risorse di sistema, sia sotto quello della sicurezza. Siccome l'utente ignora la loro presenza non si farà neppure carico di applicare le patch per la sicurezza rilasciate dal produttore, dando così spazio agli exploit dei potenziali aggressori.

Facciamo un esempio pratico:

- mediante l'attivazione di uno sniffer verifichiamo il traffico che transita dalla nostra scheda di rete non connessa in stealth (in modo furtivo sulla rete tramite hub o monitor port) ma in modo tradizionale alla rete;

- mediante uno strumento di port scan analizziamo le porte aperte dei client connessi alla nostra rete.

I risultati del test potrebbero essere i seguenti, lo sniffer rileva un traffico UDP di tipo multimediale (voce o video) broadcastato sulla rete come di seguito indicato:

24/11/2010 - 11:56:40	24/11/2010 - 11:56:40	192.168.20.106:52834 (MPA,90Khz,Mono)	224.0.0.252:5355	IP1 codec n...
24/11/2010 - 13:03:05	24/11/2010 - 13:03:05	192.168.20.5:58667 (LPC,8Khz,Mono)	224.0.0.252:5355	IP1 codec n...
24/11/2010 - 16:12:13	24/11/2010 - 16:12:13	192.168.20.5:56894 (GSM,8Khz,Mono)	224.0.0.252:5355	IP1 codec n...
24/11/2010 - 18:08:14	24/11/2010 - 18:08:14	192.168.20.5:56631	224.0.0.252:5355	
24/11/2010 - 19:00:40	24/11/2010 - 19:00:40	192.168.20.5:49671 (QCELP,8Khz,Mono)	224.0.0.252:5355	IP1 codec n...
24/11/2010 - 22:24:01	24/11/2010 - 22:24:01	192.168.20.5:52789 (PCMU,8Khz,Mono)	224.0.0.252:5355	
25/11/2010 - 02:44:35	25/11/2010 - 02:44:35	192.168.20.5:50587 (G722,8Khz,Mono)	224.0.0.252:5355	
25/11/2010 - 08:58:29	25/11/2010 - 08:58:29	192.168.20.5:50616 (G728,8Khz,Mono)	224.0.0.252:5355	IP1 codec n...
25/11/2010 - 09:30:25	25/11/2010 - 09:30:25	192.168.20.5:59011 (G729,8Khz,Mono)	224.0.0.252:5355	IP1 codec n...
25/11/2010 - 10:14:21	25/11/2010 - 10:14:21	192.168.20.5:57548 (LPC,8Khz,Mono)	224.0.0.252:5355	IP1 codec n...

Verificando quali porte sono aperte su uno dei client che genera quel tipo di traffico riscontriamo:

IP Address	MAC Address	Open Port
192.168.20.5	00-0F-20-CF-B6-50	21, 443, 80

Analizzando le porte di un client in rete ci chiediamo il motivo per cui siano in ascolto le porte 80 e 443 non essendo un web server o non erogando alcun servizio.

La risposta è molto semplice……..**SKYPE!**

In pratica il client ha installato **Skype**. Aziendalmente le policy non consentono l'utilizzo di questo strumento inibendo tramite firewall il suo utilizzo, ma il client cerca comunque di terminare le connessioni per conto terzi continuando a trasmettere pacchetti broadcasting in rete non potendo portare a termine le connessioni richieste a causa del firewall stesso.

E' possibile verificare di come l'accesso a **Skype** apra porte in modalità "ascolto" sul client in grado di bypassare il firewall (80 e 443). Il client in queste condizioni si comporta come un "**super nodo**" al quale terzi possono collegarsi per effettuare chiamate. Queste connessioni generano traffico e aprono falle di sicurezza. Per questo alcuni enti hanno bandito **Skype** dalle proprie reti aziendali in quanto giudicata come un'applicazione precaria in termini di sicurezza.

Se sul nostro client proviamo a verificare il numero delle porte in ascolto, con e senza **Skype** avviato, potremo appurare che l'applicazione in oggetto ha aperto un certo numero di connessioni che rimangono "pericolosamente aperte" nonostante non sia utilizzata. Davvero un'amara sorpresa.

Condivisioni di rete

Durante gli audit ci capita sovente di riscontrare configurazioni di autorizzazioni non corrette, che di fatto consentono a chiunque l'accesso alle cartelle di rete. Esistono due scenari tipici per cui potrebbe risultare necessario tenere sotto controllo le autorizzazioni di accesso:

1. se il nostro PC è condiviso da più persone;
2. se condividiamo file su una rete.

In entrambi i casi ciò che vogliamo evitare è che un utente non autorizzato possa dare una sbirciatina ai nostri file o che, ancora peggio, possa involontariamente cancellarli. Ma ancora più pericoloso è che quando i file sono condivisi in rete il cestino non funziona e così l'operazione di eliminazione di un file lo "distrugge" immediatamente.

Le opzioni di controllo attribuibili possono essere le seguenti:

- Controllo completo.
- Modifica.
- Lettura ed esecuzione.
- Visualizzazione contenuto cartella.
- Lettura.
- Scrittura.
- Autorizzazioni Speciali.

Ognuno di queste opzioni comprende delle regole che debbono essere consentite o negate. Nella maggior parte delle situazioni è sempre sufficiente applicare il comando "Consenti". Raramente è necessario utilizzare le "Autorizzazioni Speciali" ma soprattutto è sconsigliabile il loro impiego qualora non si comprenda appieno il significato delle impostazioni.

Durante l'utilizzo delle opzioni di controllo potrebbe succedere che alcuni segni di spunta non siano disponibili e quindi impostabili. Questo succede quando l'oggetto su cui si sta operando eredita le opzioni dall'oggetto padre. Per modificare anche queste impostazioni è necessario cliccare sul comando "Avanzate" e quindi procedere a rimuovere le **Autorizzazioni Ereditabili dal Padre.**

Non è oggetto della lezione quello di insegnare come applicare le policy, cosa molto semplice se si è all'interno di un Dominio AD (Active Directory), ma che un utente ospite, sfogliando la rete possa accedere a cartelle condivise, rappresenta sicuramente un fatto molto grave.

Possono presentarsi diversi casi:

- Le cartelle contengono documenti aziendali.
- Le cartelle contengono documenti personali.
- Le cartelle non contengono nulla.

Inoltre:

- L'utente ha creato in autonomia la condivisione.
- L'amministratore di rete non ha configurato correttamente le policy.

Quanto sopra può esprimere responsabilità aziendali e rientra nella violazione del codice privacy, oppure nelle responsabilità personali sempre previste dal codice in quanto:

tutti gli utenti sono incaricati al trattamento dei dati.

Attenzione: anche l'esposizione di una cartella vuota può essere un grosso problema in quanto può consentire di scriverci dentro oppure di depositare file compromettenti che potrebbero poi essere utilizzati contro di noi in quanto proprietari della rete.

Conclusioni

In questa lezione abbiamo potuto constatare come gli strumenti usati solitamente per attaccare e creare danni ad una rete aziendale, possono, anzi **devono**, essere usati per controllare l'affidabilità e la corretta configurazione della propria rete.

Sottovalutare porte aperte, protocolli non sicuri od esporre le proprie informazioni, rischia di tradursi in un danno che alle volte può diventare irreparabile per cui…….

Molto meglio porvi rimedio per tempo!!!

Il Tuo EtterNet Team