

LANguard Network Security Scanner 3.3

di **Andrea Pompili** (apompili@infomedia.it)

Circa tre anni fa la GFI propose in versione freeware uno strumento chiamato LANguard in grado di effettuare probe piuttosto approfonditi soprattutto sul versante Windows. Il programma era infatti in grado di eseguire sia query netbios, sia di verificare i contenuti del registry dell'host analizzato presentando quindi dei risultati piuttosto completi ed efficaci. Durante gli anni il prodotto si è evoluto ed ha assunto una dimensione più commerciale fino alla versione 3.3 in cui sono state incluse moltissime caratteristiche piuttosto interessanti per la gestione della sicurezza oltre che per l'analisi delle vulnerabilità.

Nonostante questa versione sia a pagamento, esiste comunque una versione freeware del prodotto che non include tutte le caratteristiche di gestione della sicurezza (patch management, gestione dei report, ecc.), ma che può sempre essere utile per realizzare analisi "al volo" all'interno della propria rete.

Eseguire un probe della rete

Una volta installato, LANguard è già pronto per eseguire uno scan della propria workstation o di una subnet semplicemente inserendo nell'apposito campo il nome dell'host, un indirizzo o un range di indirizzi IP o specificando un file contenente gli host da verificare.

Dopo aver fatto partire lo scan mediante il pulsante apposito, il programma inizierà ad eseguire una discovery sulla rete utilizzando un normale ping; nel caso non venga ottenuta alcuna risposta, viene inviata una query netbios, ed infine una query SNMP. Se tutte e tre le modalità non producono un risultato l'host è considerato non attivo e, nel caso sia stato eseguito uno scan specifico su di esso, viene suggerito all'utente di aumentare il timeout e di ritentare lo scan.

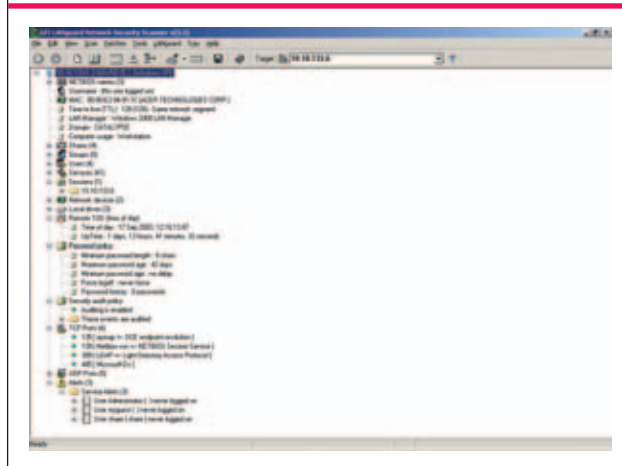
Una volta effettuata la discovery di tutti gli elementi di rete attivi (o aver verificato la raggiungibilità del particolare host selezionato), LANguard inizia ad eseguire una serie di probe più o meno sofisticati basandosi sui seguenti controlli:

1. Vengono inizialmente ricavati i nomi netbios del sistema (dominio di appartenenza, utente collegato e nome computer).
2. Vengono quindi verificate le share disponibili e le relative autorizzazioni. Durante l'analisi viene anche verificata la robustezza delle credenziali di accesso. È possibile configurare quest'attività specificando delle particolari credenziali da utilizzare o tentando addirittura un brute force (questa opzione, se abilitata, rallenta notevolmente lo scan).

LANguard è uno di quegli strumenti "tutto fare" indispensabili per chi si occupa di monitorare e gestire la sicurezza dei sistemi in rete. Le funzionalità offerte e lo stampo "buono" del prodotto contribuiscono inoltre a renderlo molto più efficace di altri strumenti analoghi piuttosto ambigui che ormai infestano il mercato corrente

3. Viene eseguito un collegamento al registro remoto per scaricare tutte le informazioni riguardanti la configurazione della macchina, agli audit abilitati, alle patch installate e ai servizi attivi.
4. Vengono estratte tutte le utenze configurate sull'host compresi i gruppi di appartenenza e i privilegi associati. Contestualmente viene compiuta una verifica preliminare della password (ad esempio se è inesistente o uguale all'identificativo dell'account).
5. Viene ricostruito l'intero albero SNMP associato all'host (solo se attivo).
6. Viene eseguito un *Vanilla scan* su tutte le porte TCP maggiormente conosciute e per ogni servizio scoperto viene estratto ed analizzato il banner restituito all'accesso. Lo scan TCP avviene quindi portando a termine il three-handshake-protocol su ciascuna porta controllata.
7. Viene effettuato un *ICMP port unreachable scanning* su tutte le porte UDP principali (viene inviato un pacchetto UDP e verificata la ricezione di un pacchetto ICMP di tipo ICMP_PORT_UNREACH, risposta tipica di alcuni sistemi operativi in caso di porta chiusa).

FIGURA 1 La mole di informazioni e la rapidità con cui queste vengono estratte è impressionante. In poco tempo è possibile avere un audit "adeguato" della propria rete senza aver bisogno di notevoli competenze in materia di sicurezza



- Viene fatto l'OS fingerprinting, ossia sono inviati dei pacchetti di test per identificare in maniera più o meno precisa il sistema operativo. Ad esempio, se il TTL dell'host risulta pari a 128, LANguard deduce che il sistema è "probabilmente uno Windows", ma se gli altri test sulle porte aperte o sui banner restituiti dai servizi disponibili restituiscono ulteriori risultati, la dicitura può essere confermata fino a stabilire la reale natura del sistema (98, 2000 o XP per esempio). I file di configurazione per questa attività sono nella directory *Fingerprint* di LANguard e possono essere facilmente estesi o modificati dall'utilizzatore del sistema.
- In base alle informazioni raccolte vengono eseguiti dei test sulle vulnerabilità e sui possibili errori di configurazione, come utenti mai utilizzati, share aperte o debolezze nel sistema d'autenticazione. Se il sistema è di tipo Windows, vengono anche verificate le patch o le service pack mancanti utilizzando le informazioni del registry. I test da compiere sono tutti contenuti all'interno di un database interno che può essere aggiornato connettendosi al sito della GFI mediante l'apposito menu *Check for Security Update* sotto la voce *Help* del menu principale.

Una volta portato a termine uno scan (Figura 1) è possibile eseguire alcuni test aggiuntivi come quello sulle credenziali di accesso mediante dictionary attack o semplice LanMan Hash crack per i sistemi Windows 9x. Nel primo caso è possibile specificare un file contenente un dizionario adeguato, ossia una lista di parole da provare in tutte le combinazioni possibili (LANguard contiene già un dizionario base contenente però solo parole inglesi nella directory *Config*). Nel secondo viene tentato un attacco noto sulle macchine Windows 9x basato sulla debolezza del hash immagazzinato (<http://support.microsoft.com/support/kb/articles/Q273/9/91.ASP&NoWebContent=1>).

Altre operazioni disponibili sono l'invio di messaggi mediante NETBIOS Messenger utilizzando un nome macchina o un IP spoofato o il deployment di patch o service pack.

Ovviamente, per ottenere uno scan ottimale è necessario prima configurare adeguatamente LANguard mediante il pannello *Options* sotto la voce *Scan* del menu principale. La quantità di opzioni configurabili è impressionante e consente di configurare tutti i probe illustrati nella precedente lista (compreso il timeout da utilizzare e le porte da verificare con i servizi associati), di specificare l'utenza da utilizzare per le connessioni netbios al file system e al registry remoto (scegliendo tra quella dell'utente connesso, una NULL session o un'utenza specifica) ed infine le verifiche da compiere su eventuali database o sulle patch installate.

Come specificato anche nel manuale utente, non sono previsti meccanismi per aggirare firewall o IDS come per l'ormai arcinoto *Nmap* o per *N-Stealth* (CGI scanner piuttosto efficace prodotto dalla Nstalker). Tutti i probe eseguiti possono essere quindi rilevati da questi strumenti di protezione e segnalati appunto come attacchi: è necessario quindi prima concordare queste attività con i responsabili dell'esercizio.

Inoltre lo scanner è molto orientato verso il lato Windows e, nonostante vengano scoperti con ottima approssimazione anche altri sistemi operativi (compresi gli IOS della Cisco), le vulnerabilità testate sono molto poche rispetto a quelle relative al sistema di casa Redmond.

C'è da considerare che, come vedremo più avanti, LANguard permette di scrive-

re autonomamente i test da eseguire consentendo quindi una grande versatilità anche sotto quest'aspetto.

Report e analisi dei risultati

Una volta terminato lo scan è possibile salvare su disco in formato HTML e XML tutte le informazioni ricavate specificando sia le intestazioni, sia la formattazione specifica del report. Per quest'attività LANguard si avvale di XSL e XML rispettivamente per la formattazione HTML e la memorizzazione dei dati ricavati. È possibile quindi definire il proprio template mediante una delle due seguenti procedure: scrivendo un file XSL opportuno da inserire nella directory *xsl* sotto *Config* e aggiungendo la relativa riga di registrazione nel file *custom_reports.xml* presente nella stessa directory, oppure personalizzando uno dei modelli predefiniti in maniera visuale al momento del salvataggio.

La prima modalità è molto più flessibile e consente di personalizzare anche il layout grafico del report, cosa magari necessaria nel caso si voglia avere il logo della propria società nel frontespizio o si vogliano utilizzare dei colori o dei formati specifici. La seconda, invece, consente solo di modificare l'intestazione e il fondo pagina del report e di specificare quali informazioni visualizzare e quali no.

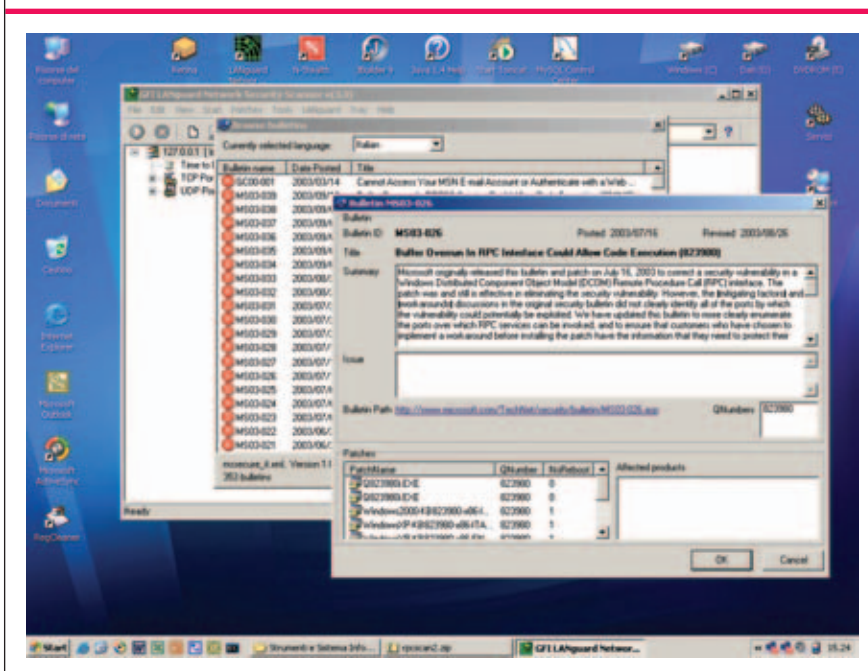
I report generati possono essere quindi ricaricati sul sistema mediante il *Report Generator*, all'interno del quale è possibile anche fare interrogazioni, ricerche e ulteriori formattazioni.

Un'altra funzionalità interessante è la possibilità di comparare i risultati di due scan successivi mediante la funzione *Results Comparison*. Basta specificare due report in formato XML ed il sistema verificherà tutte le differenze esistenti presentandole su schermo insieme ad una nota esplicativa.

Questa funzionalità viene utilizzata anche per gli scan schedulati che LANguard può gestire mediante l'apposito pannello sotto la voce *Scan* del menu principale. Per questa attività è necessario che sia in esecuzione il servizio *GFI LANguard N.S.S. Scheduled Scans Service* che il programma configura al momento dell'installazione.

Basta specificare il giorno e l'ora dello scan, le subnet interessate e LANguard è in grado di eseguire i test autonomamente salvando il report generato nella cartella di default. Il

FIGURA 2 Il database interno delle hotfix di Microsoft. È possibile navigare all'interno della lista e curiosare tra le varie vulnerabilità per capirne l'origine e la pericolosità



programma può quindi fare una comparazione con i risultati precedenti e, nel caso siano presenti delle differenze, può avvisare mediante E-mail l'amministratore di sistema.

Patch management

Nonostante le apparenze, LANguard risulta comunque molto più orientato alla prevenzione e alla gestione della sicurezza. La caratteristica principale di questo strumento è, infatti, la possibilità di distribuire patch e service pack su sistemi Windows da remoto una volta identificate le vulnerabilità o gli aggiornamenti mancanti.

Le patch possono essere semplici hotfix, intere service pack o programmi e correzioni realizzate autonomamente. LANguard si comporta come un sistema di software distribution e permette di stabilire quali host aggiornare, la modalità di aggiornamento e quali elementi installare.

Il programma può essere configurato per scaricare la lista degli ultimi aggiornamenti direttamente dal sito della Microsoft nella lingua desiderata (nella precedente versione la funzionalità era disponibile solo per i sistemi Windows in lingua inglese). È possibile quindi navigare tutte le patch disponibili e scaricarle localmente sul proprio sistema in modo da poterle successivamente distribuire sulle macchine controllate.

Ogni patch è corredata di un'ampia descrizione e di tutti i riferimenti ufficiali in modo da aiutare l'amministratore di rete ad identificare quelle più importanti e di informarsi sulla tipologia di vulnerabilità associata (Figura 2).

LANguard gestisce sia gli aggiornamenti relativi al sistema operativo (NT, 2000 ed XP), sia quelli di Internet Explorer (dalla versione 4.0 alla 6.0), quelli di Office 2000 ed XP, fino alle applicazioni server di Windows come ISA Server, IIS (dalla 3.1 alla 5.1), SQLserver 7 e 2000 ed Exchange 5.5 e 2000.

Per quanto riguarda le patch custom, LANguard permette di specificare sia il sistema operativo, sia il programma specifico a cui fanno riferimento in modo da guidarne l'installazione nella fase successiva. Mediante questa funzionalità è possibile, ad esempio, installare programmi aggiuntivi come plug-in Flash, aggiornamenti DirectX o programmi veri e propri.

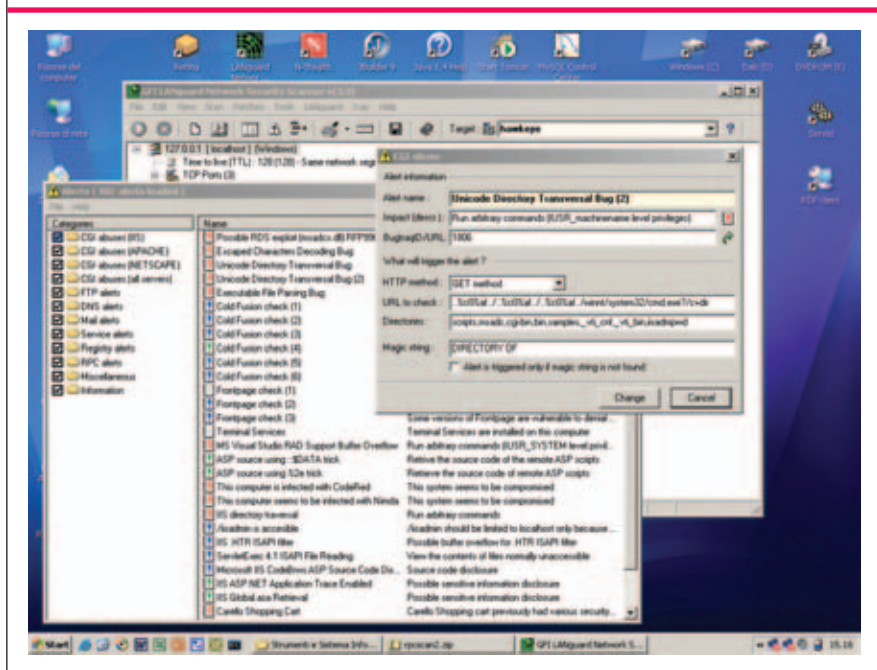
Il deployment delle patch può essere compiuto manualmente dopo aver terminato lo scan del proprio network: è possibile decidere cosa installare (hotfix, service pack o programmi custom) e se installarle su tutte le macchine rilevate o su una singola macchina. LANguard verificherà automaticamente quali sono gli elementi mancanti e li installerà sul sistema remoto (è necessario utilizzare delle credenziali associate ad utenti amministrativi sulle macchine remote per poter eseguire correttamente l'operazione).

È possibile anche specificare un messaggio di avvertimento da presentare all'utente al momento dell'installazione, decidere se fermare o meno i servizi da aggiornare, forzare o meno il reboot della macchina aggiornata (la maggior parte delle patch richiedono questa attività a fine installazione) ed infine se fare un'installazione immediata o ritardarla specificando un orario ed un giorno particolare.

Test personalizzati e LANS

Un'altra delle caratteristiche di LANguard è sicuramente la sua versatilità sulla tipologia di test eseguibili. A parte il da-

FIGURA 3 Esempio di test CGI per IIS su Unicode Traversal Directory. Viene tentata una get HTTP verso l'host cercando di lanciare il comando dir mediante CMD DOS. Se il risultato contiene la stringa "DIRECTORY OF" la macchina viene considerata vulnerabile



tabase interno aggiornabile fornito dalla GFI è, infatti, possibile scrivere autonomamente i propri test utilizzando più di una modalità a seconda della complessità del test da realizzare. Mediante il pannello *Configure Alerts* sotto la voce *Scan*, è possibile infatti gestire il database dei test interno selezionando i test da eseguire, rimuovendone alcuni o aggiungendone di nuovi.

In particolare tutti i test sono divisi in categorie predefinite e possono essere attivati e disattivati solo per famiglia di appartenenza a meno di non rimuoverli singolarmente dal database interno.

Creare un nuovo test è piuttosto semplice: basta selezionare una categoria, impostare le informazioni relative al tipo di vulnerabilità e al Bugtraq ID ed infine aggiungere mediante wizard i test elementari che determineranno la presenza o meno del problema.

Per i test CGI, ossia quelli utilizzati per controllare le vulnerabilità su servizi Web, la configurazione è ancora più semplice poiché basta specificare l'URL da lanciare, la modalità di richiesta http e la stringa da verificare all'interno della risposta HTTP ottenuta.

In Figura 3 è riportato un esempio di test CGI su IIS per lo *Unicode Traversal Directory bug*.

I test elementari possono invece essere di diverso tipo:

- Tipo di sistema operativo.
- Apertura o meno di specifiche porte TCP/UDP.
- Installazione o meno di determinati servizi (IIS, RPC, ecc.).
- Installazione o meno di determinate hotfix o service pack.
- Presenza o meno di percorsi o chiavi di registro e verifica di valori particolari contenuti.
- Verifica dei banner dei servizi rilevati (stringhe contenute, espressioni regolari, ecc.).
- Valore restituito da uno script LANS (true o false).

Le prime verifiche sono tutte configurabili tramite wizard specificando la condizione di validità, l'elemento da verificare e, in alcuni casi, il valore di confronto.

L'ultima possibilità, invece, mette in gioco una delle caratteristiche principali del prodotto: il LANguard Scripting language

ge o LANS. Il LANS non è altro che un linguaggio di scripting proprietario dalla sintassi molto simile al C che permette di realizzare dei test piuttosto complessi mediante delle funzioni predefinite per il networking e la gestione delle stringhe.

Scheda Prodotto

Nome e versione	LANguard N.S.S.
Categoria	Vulnerabilità scanner e patch management system
Produttore	GFI Software Ltd. 15300 Weston Parkway Suite 104 Cary, NC 27513 USA Tel. +1 (888) 2 GFIFAX Fax +1 (919) 388 5621 Tech support +1 (919) 297-1350
Distributore	GFI Divisione Italia GFI House San Andrea Street San Gwann SGN 05 Malta - Tel. 049 8649076
Trial prelevabile da	http://www.gfi.com http://www.gfi-italia.com
Prezzo	Fino a 25 IP: 295 € Fino a 50 IP: 375 € Fino a 100 IP: 475 € Fino a 250 IP: 750 € Unlimited IP: 925 € (a persona che utilizza il prodotto)
Sistema Operativo	Windows NT - 2000 - XP
Spazio Disco	~ 17 Mb

Uno script LANS può quindi restituire un valore vero o falso che viene interpretato dal motore di LANguard e gestito a seconda della condizione specificata nel relativo test implementato. La scrittura di questi script può essere fatta mediante un apposito editor installato insieme a LANguard che, oltre a fare syntax highlighting, consente di eseguirli in un ambiente sicuro per eseguire test e verifiche di correttezza.

Per la sintassi del linguaggio e le funzioni definite si fa riferimento alla guida inclusa nella distribuzione di LANguard che è piuttosto completa e dettagliata e fornisce una serie di ottimi esempi per iniziare.

Conclusioni

LANguard è sicuramente uno strumento fondamentale per chi gestisce reti di piccole dimensioni o ha bisogno di uno strumento "rapido" per la verifica di specifiche LAN all'interno della propria Intranet. La versatilità del programma e le funzionalità incluse sono inoltre un'enorme garanzia che, paragonate al prezzo ufficiale, lo rendono molto appetibile rispetto ad altre soluzioni molto più costose.

Bibliografia

- [1] GFI Software Ltd., "GFI LANguard Network Security Scanner 3.3 Manual", 10/07/2003

Note Biografiche

Andrea Pompili è laureato in Ingegneria Informatica. Inizialmente ha svolto attività di analisi e sviluppo per la realizzazione di Portali di tipo Enterprise su piattaforma Java. Successivamente si è occupato di architetture e assessment per la sicurezza informatica nell'ambito delle Telecomunicazioni. Attualmente lavora presso il gruppo Telecom Italia S.p.A.