



NESSUS



A cura di: Paletta R.
Schettino M.

Prof. Alfredo De Santis

1

Indice

- 1-INTRODUZIONE
sicurezza delle reti, vulnerabilità, prevenzione
- 2-SCANNER DI VULNERABILITA'
- 3-NESSUS
caratteristiche, esempi di utilizzo

2

INTRODUZIONE - sicurezza

L'espansione della rete ha portato all'aumento dei tentativi di intrusione che hanno inciso sul fattore sicurezza della rete stessa.

Secondo il Computer Security Institute nel 2004 le 494 società esaminate hanno subito danni per circa 142 milioni di dollari.

Causa principale di queste perdite economiche è stata la vulnerabilità delle proprie reti o dei propri sistemi.

3

INTRODUZIONE - vulnerabilità

Debolezza di un sistema di sicurezza che può essere utilizzata per causare danni.

La vulnerabilità di un sistema può essere rappresentata da:

- Disastri naturali
- Errori umani
- Buchi software o hardware
- Attacchi

4

INTRODUZIONE - vulnerabilità

Le vulnerabilità sono catalogate dal SANS Institute attraverso dei codici chiamati CVE (Common Vulnerabilities and exposures).

Tra le principali vulnerabilità troviamo ad esempio:

- Sistemi di autenticazione
- Browser Internet Explorer
- Condivisioni con NETBIOS
- Condivisioni Peer-to-Peer
- Servizi in chiaro (telnet, FTP,...)

5

INTRODUZIONE - tipi di attacchi

Probing e scanning

Attacchi alle password

Intercettazione di pacchetti (packet sniffing)

Compromissione di account (privilegiati e non)

Denial of Service

Codice malizioso (Virus, Worm, Cavalli di Troia)

Attacchi all'infrastruttura di rete (name server, access provider,...)

6

PROBING

Con un software di probing si possono ottenere diverse informazioni relative ad una rete, quali:

- Amministratori e utenti della rete
- Posizione del server
- Presenza o meno di intranet
- Sistemi di rilevamento delle intrusioni
- Server dns e sua configurazione
- Indirizzi IP assegnati
- Eventuale accesso telefonico

Un utente malizioso potrebbe utilizzare tali informazioni allo scopo di sfruttarne le vulnerabilità.

7

SCANNING

Con un software di scanning si possono ottenere informazioni relative a:

- Quali sono le macchine attive e raggiungibili
- Quali servizi sono disponibili

Utilizzando tecniche come:

- Il ping sweep
- Il portscanning
- Il rilevamento del sistema operativo tramite stack TCP/IP fingerprinting

8

PORTSCANNING

E' il processo che simula connessioni a porte TCP e UDP sul sistema nel quale si vuole tentare una penetrazione al fine di determinare quali servizi siano in esecuzione o in stato di LISTENING.

Per ciascun servizio identifica il tipo di server e ne determina il grado di vulnerabilità.

Eventuali servizi attivi in ascolto potrebbero consentire a utenti non autorizzati di accedere a sistemi mal configurati o su cui sia in esecuzione un software con problemi di sicurezza noti.

9

PREVENZIONE

Come fare per difendersi?

Per poter identificare le debolezze della propria rete e dei propri sistemi esistono strumenti appositi: gli scanner di vulnerabilità.

Il fine è quello di evitarne uno sfruttamento da parte di utenti maliziosi.

10

SCANNER DI VULNERABILITA'

Lo scanning delle vulnerabilità è il processo di controllo di tutti i metodi potenziali di attacco, atti a manomettere la rete di un'organizzazione.

Analizzando i tipi di software e di configurazioni di software presenti su una certa rete, gli scanner sono in grado di determinare i tipi di attacco che possono essere fatti ai danni di tale rete, consentendo a quest' ultima di difendersi appropriatamente.

11

SCANNER DI VULNERABILITA'

Due modi di vulnerabilità del software:

Vulnerabilità note: sono quelle che sono state identificate ed isolate da uno scanner per la sicurezza, il quale mette a conoscenza gli utenti della loro esistenza tramite un avviso.

Vulnerabilità sconosciute: non sono state scoperte o rese note pubblicamente, di conseguenza sono considerate una potenziale minaccia alla sicurezza.

12

SCANNER DI VULNERABILITA'

Alcuni scanner di vulnerabilità sono:

- NMAP
- SAINT
- PORTSCAN
- NESSUS

Analizziamo ora il più diffuso scanner di vulnerabilità, cioè il NESSUS.

13

NESSUS



- Autore: R. Deraison.
- Nasce in Francia agli inizi del 1998.
- Sicurezza nelle trasmissioni.
- Aggiornabile mediante degli script in NASL (Nessus Attack Script Language)

14

NESSUS



- Un Port Scanner.
- Un server (solo Unix-like).
- Un client (anche Win32).
- Offre molti servizi (test di sicurezza).

15

NESSUS

Nessus è un progetto che ha come scopo quello di fornire alla comunità uno strumento potente, facile e free per analizzare e scoprire le vulnerabilità di una rete, al fine di evitarne uno sfruttamento da parte di utenti maliziosi.

E' probabilmente il più completo ed evoluto strumento di vulnerability scanning disponibile nel mondo open-source.

16

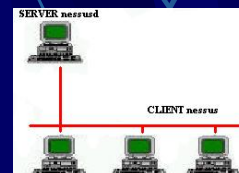
CARATTERISTICHE DI NESSUS

- Gratuito
- Open-Source
- Aggiornato (plug-in)
- Pignolo
- Veloce

17

ARCHITETTURA DI NESSUS

- Logica Client/Server



Il server (nessusd) è il motore che esegue lo scan vero e proprio, esiste solo in versione Unix-like ed è la parte del pacchetto che offre i servizi.

18

ARCHITETTURA DI NESSUS

Il client (nessus) è l'interfaccia con cui si può configurare una sessione di scan (indirizzi target, tipi di check da eseguire ecc.) da far eseguire sul server.

Il client (nessus) e il server (nessusd) possono essere installati nella stessa macchina oppure su macchine diverse. Esistono inoltre client grafici per Windows, Posix/GTK+ (Linux, Solaris, ...) e JAVA.

19

ARCHITETTURA DI NESSUS

- Struttura a Plug-in

Nessus presenta una struttura modulare, con dei plug-in che possono essere aggiornati per individuare vulnerabilità recenti.

Tale struttura è il punto di forza di Nessus, i plug-in sono veri e propri moduli esterni al progetto originale e ad esso perfettamente integrabili.

20

ARCHITETTURA DI NESSUS



In qualsiasi momento si possono scaricare dalla rete plug-in aggiuntivi.

Ogni utente può creare un proprio plug-in e metterlo a disposizione di altri utenti (dopo opportuno test).

21

ARCHITETTURA DI NESSUS

- Ciascun test di sicurezza è scritto come plug-in esterno.
- Giornalmente, chiunque può segnalare un nuovo bug.
- Esiste una lista di plug-in ancora da scrivere.
- Qualunque utente registrato può offrirsi volontario per scrivere un plug-in.
- E' scritto in C o in Nessus Attack Script Language (NASL).
- Ciascun plug-in sarà testato dall'autore di Nessus.

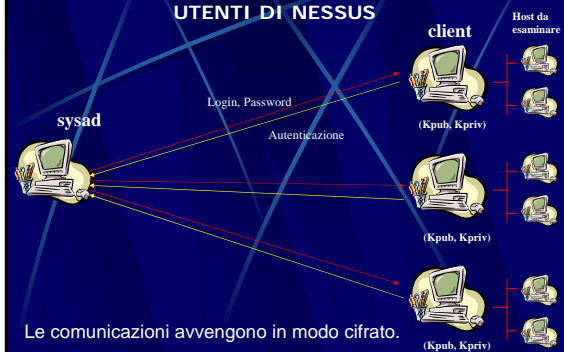
22

UTENTI DI NESSUS

- Il sysad è l'amministratore del server.
- Gli utenti del sistema possono essere utenti di Nessus client.
- Il sysad stabilisce nome utente e password per ogni utente.
- Ogni utente sarà provvisto di una coppia di chiavi pubblica e privata.
- L'accesso degli utenti avviene in modo autenticato.
- Le comunicazioni avvengono in modo cifrato.
- Ciascun utente può avere delle restrizioni sul numero di macchine che può esaminare.

23

UTENTI DI NESSUS



24

COSA OFFRE NESSUS

SICUREZZA

- Le comunicazioni tra client e server avvengono in modo cifrato (chiave pubblica).
- Gli accessi avvengono in modo autenticato.

AFFIDABILITA'

- I test di sicurezza sono in continuo aggiornamento.
- Tutti i test sono garantiti dall'autore.

25

NESSUS - installazione



Il primo passo è quello di installare nessusd (server) e nessus (client). Il software Nessus è reperibile all'indirizzo:

www.nessus.org

26

CREAZIONE ACCOUNT nessusd

Il server nessusd ha un proprio database di utenti, quindi bisogna aggiungere un nuovo utente al database del sistema di servizio.

Ciascun utente può avere delle restrizioni sul numero delle macchine che può esaminare.

Per creare un nuovo utente utilizziamo il comando **nessusd -P username,passwd**.

Per verificare che tutto è andato bene scriviamo **nessusd -L**.

27

CREAZIONE ACCOUNT nessusd

Possiamo adesso aggiungere un nuovo utente che può eseguire il Nessus con delle regole utilizzando l'utility

nessus-adduser

```
nessus-adduser
Addition of a new nessusd user
-----
Login : rafmax
Authentication (pass/cert) [pass] : pass
Password : secret
User rules
-----
nessusd has a rules system which allows you
to restrict the hosts
that renaud2 has the right to test. For
instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser(8) man page
for the rules syntax

Enter the rules for this user, and hit ctrl-D
once you are done :
(the user can have an empty rules set)

//deny 127.0.0.1
accept 127.0.0.1
default deny

Login : rafmax
Password : secret
DN :
Rules :

//deny 127.0.0.1
accept 127.0.0.1
default deny

Is that ok (y/n) ? [y] y
user added.
```

Abbiamo quindi registrato un utente di nome rafmax che ha il permesso di eseguire il nessus solamente sul proprio sistema quindi se rafmax è l'amministratore, ha il permesso di fare uno scan dettagliato sul proprio sistema per trovare possibili bug.

28

CONFIGURAZIONE DEL nessus-daemon

Il file di configurazione è di default:

/usr/local/etc/nessus/nessus.conf

Possiamo far funzionare Nessus tranquillamente con le impostazioni di default, in ogni caso fra i parametri configurabili ci sono:

- PATH vari
- Impostazioni sul numero di test simultanei da eseguire
- Impostazioni sul range di porte su cui fare lo scan
- Impostazioni sui settaggi utilizzati per il canale criptato fra client e server

E' possibile ora avviare il nessusd come root:

nessusd-D

29

CONFIGURAZIONE DEL CLIENT

Possiamo adesso finalmente avviare il client scrivendo in una console

nessus

Apparirà così la schermata di dialogo

30

CONFIGURAZIONE DEL CLIENT

- Inseriamo l'indirizzo dell'host su cui è in ascolto il nessusd-server e la porta su cui è in ascolto (3001 per default)
- Eseguiamo il login con relativa password cliccando su "Log in"

31

CONFIGURAZIONE DEL CONTROLLO DI SICUREZZA

- E' possibile scegliere i vari test a cui siamo interessati. Ogni test utilizza un diverso plugin.
- Nel pannello sottostante appare una breve descrizione di cosa fa il plugin selezionato.

32

PREFERENZE DEI PLUG-IN

- Possibilità di modificare il comportamento di default di un plugin.
- Possibilità di specificare informazioni aggiuntive in modo che il controllo e la revisione siano più completi.

33

OPZIONI DI SCAN

- E' possibile settare:
 - Il range di porte da controllare
 - Il numero di host da visionare contemporaneamente
 - Il numero di plugin da utilizzare contemporaneamente contro un singolo host

34

SELEZIONE HOST DA CONTROLLARE

Vengono settati gli indirizzi degli host che vogliamo controllare.

- **10.163.156.1** un solo indirizzo IP
- **10.163.156.1-254** una serie di indirizzi IP
- **Hope** un hostname
- **Prof,10.163.156.0-24,...** una combinazione delle forme menzionate sopra separate da virgola

35

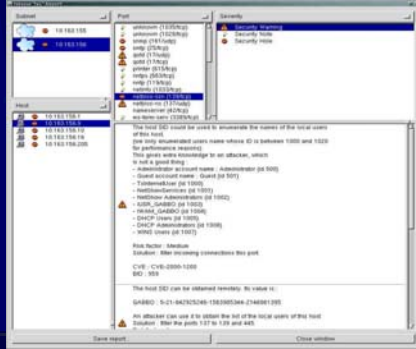
SELEZIONE DELLE REGOLE

Permettono ad un utente di restringere il suo test. Ad esempio esaminiamo gli indirizzi 10.163.156.1/24 eliminando dalla scansione l'indirizzo 10.163.156.5

A questo punto avviamo la scansione cliccando su "Start the scan"

36

RAPPORTO



Dal rapporto risulta che su 10 host controllati sono stati trovati:

54 buchi di sicurezza

303 warning

113 security note

37

CONSIDERAZIONI

- Nessus è senz'altro un buon portscanner dal punto di vista della sicurezza.
- Il controllo degli accessi impedisce che possa farsene un uso illecito o comunque che si possano subire dei danni a causa della inesperienza o della distrazione degli utenti.
- Nessus non è stato pensato come tool per hacker.
- E' bene abituarsi a lanciare regolarmente un Nessus con i plugin aggiornati sui propri server.

38