SARA

Software per scansioni

Introduzione: perché le scansioni

- I sistemi operativi installano servizi che non si usano
- Non tutti sanno cosa sta girando sul proprio calcolatore
- Non tutti sanno su quali porte ascoltano i propri computer
- Il software “invecchia” e diviene vulnerabile

Le scansioni possono essere utilizzate per scoprire eventuali vulnerabilità sui propri sistemi.

Gli scanner:

Esistono tanti tipi di programmi per svolgere scansioni, ciascuno con le sue peculiarità e caratteristiche.

- Nmap
- satan
- nessus
- sara
- ecc …

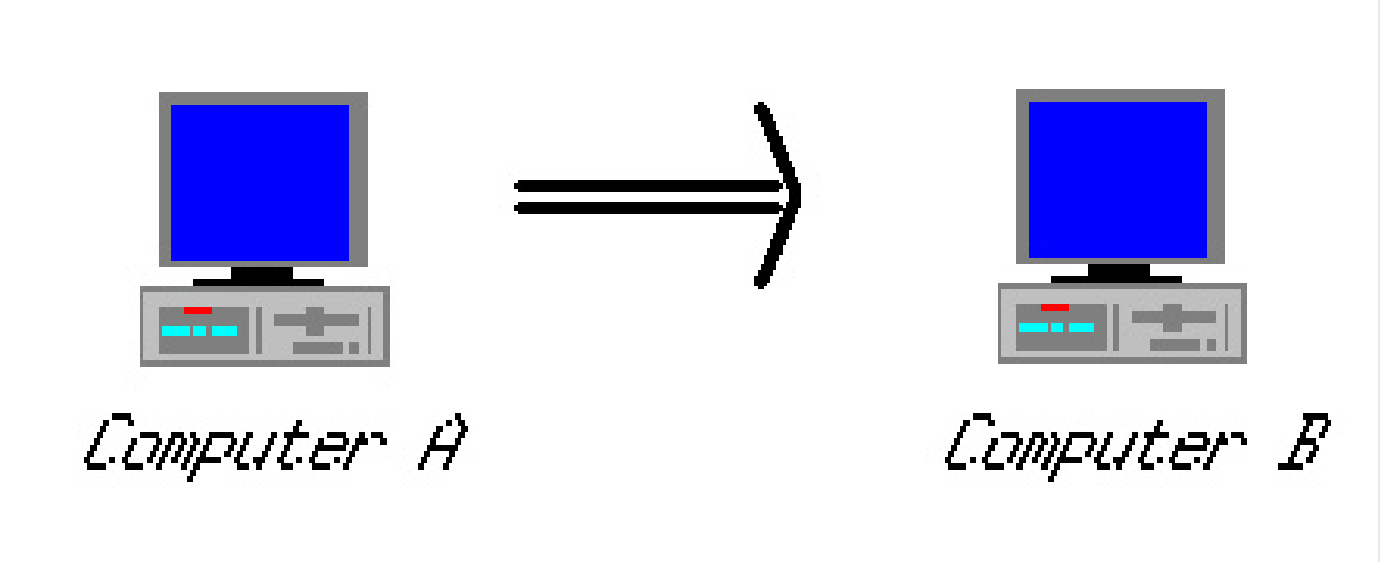
In questa occasione prenderemo in esame **SARA**

SARA (Security Auditor’s Research Assistant)

Caratteristiche:

- basato su SATAN
- interfaccia web
- intuitivo e facile da usare
- controlla se un host risponde poi lancia i test di vulnerabilità.
- visualizzazione dei risultati sotto vari aspetti.
- possibilità di creare dei database ove salvare i risultati di una o più scansioni
- l’utente può creare dei test a suo piacimento
- trust

TRUST



HP:

- Il computer B non presenta in sé vulnerabilità
- Il computer B “si fida” del computer A
- Il computer A presenta delle vulnerabilità

TS: il computer B è a rischio!

Requisiti per l’installazione

S.O.:
SunOS 4.1.3_U1
SunOS 5.3-5.7
Irix 5.3-6.5
Slackware Linux (3.x, 4.x)
Red Hat Linux (4.x, 5.x, 6.x)

Piattaforma:
All Sun Platforms
All SGI Platforms
All Intel platforms from i486

HW/SW:
20Mb disco + perl5 + browser
con 32 Mb ram non ci dovrebbero essere problemi a testare 4000 host.

Installazione e...

./reconfig

make linux

…problemi di utilizzo

Malfunzionamento di SARA con Netscape:
Nel momento in cui si svolge una qualche operazione utilizzando NETSCAPE, compare una finestra dove si richiede di salvare un file con estensione pl.

Il problema e' dovuto ad una configurazione non appropriata di netscape, risolta nella versione 4.7.

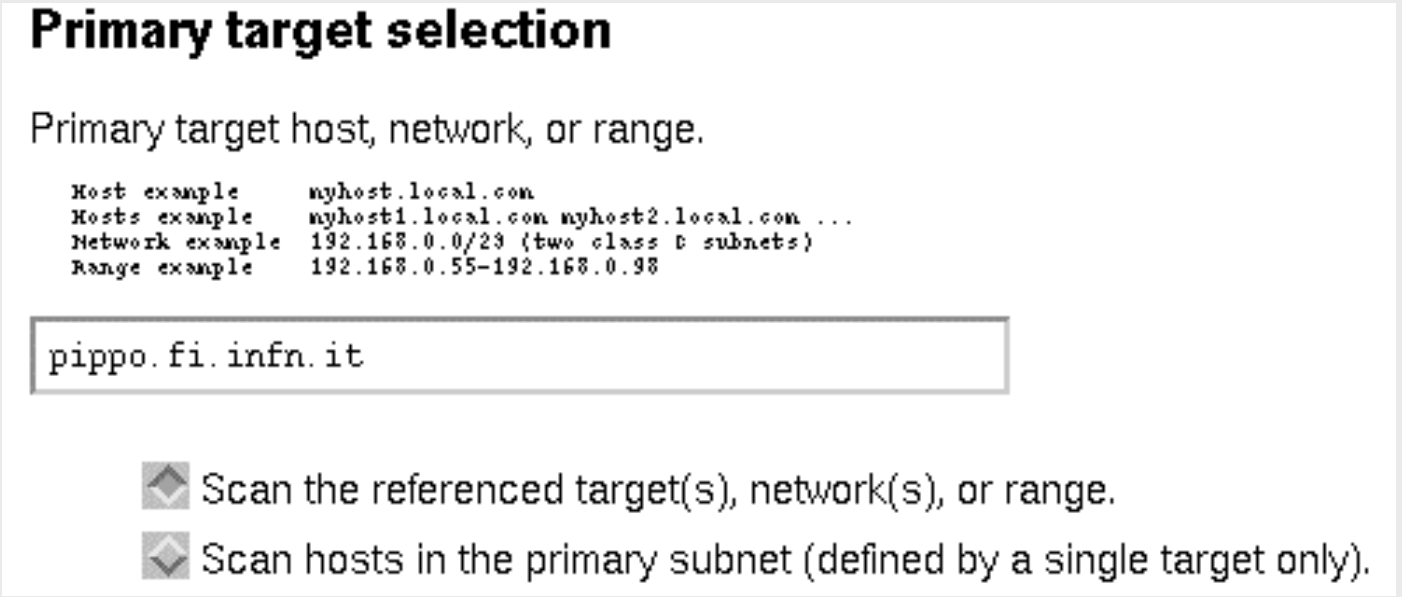
La soluzione consiste nell'effettuare la seguente operazione: settare **"MimeType"** a **text/html** e **"Handled By"** a **Navigator** nella finestra che appare cliccando su:

Edit -> Preferences -> Navigator -> Applications -> Perl Program -> Edit

Utilizzo

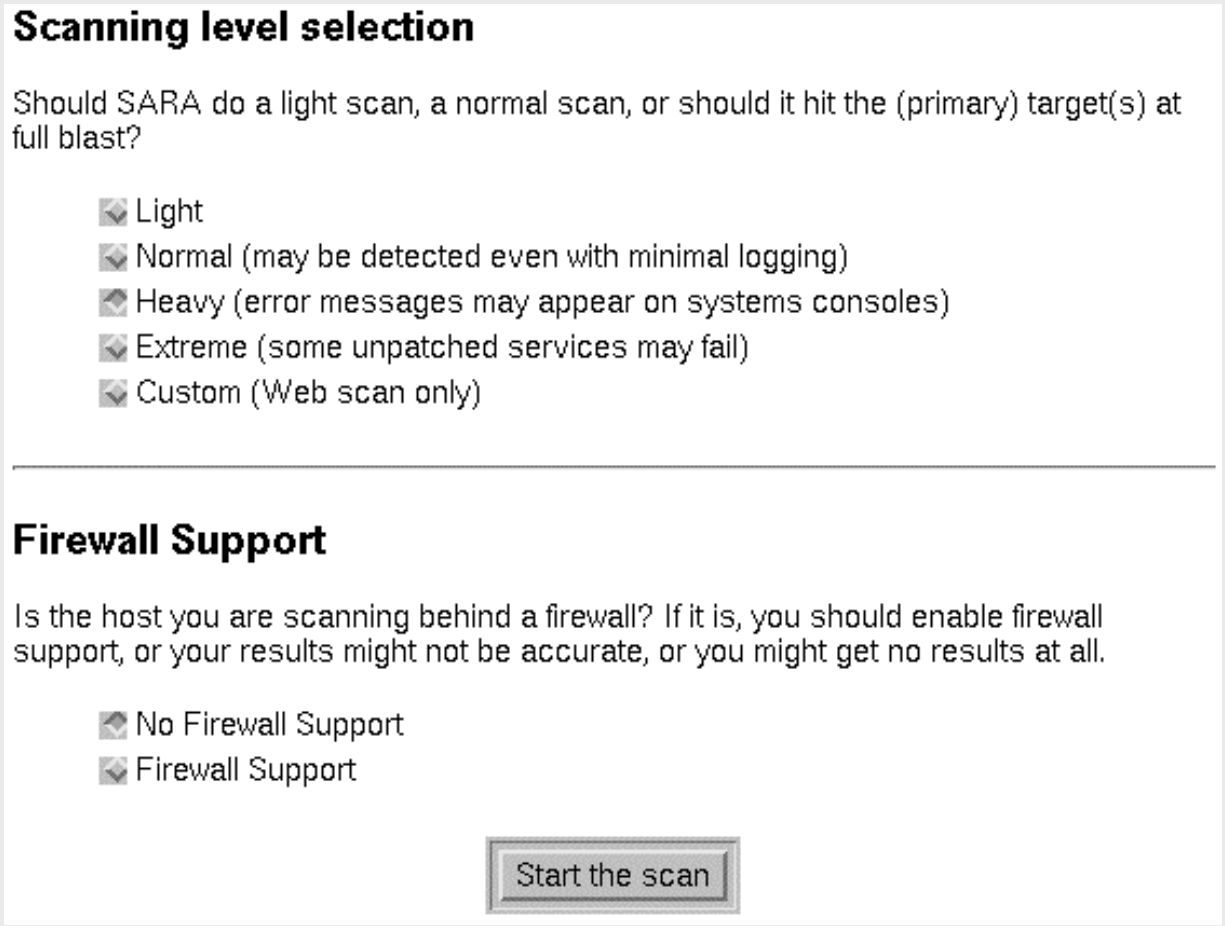
Dopo aver lanciato come **root** SARA, nella sezione Target selection è necessario svolgere le seguenti azioni:

1) riempire il campo target host e specificare se la scansione deve riguardare solo quell'host o l'intera rete a cui appartiene.



Utilizzo

2) specificare il livello di scansione e se l’host sta dietro un firewall; successivamente premere il pulsante “Start the scan”.

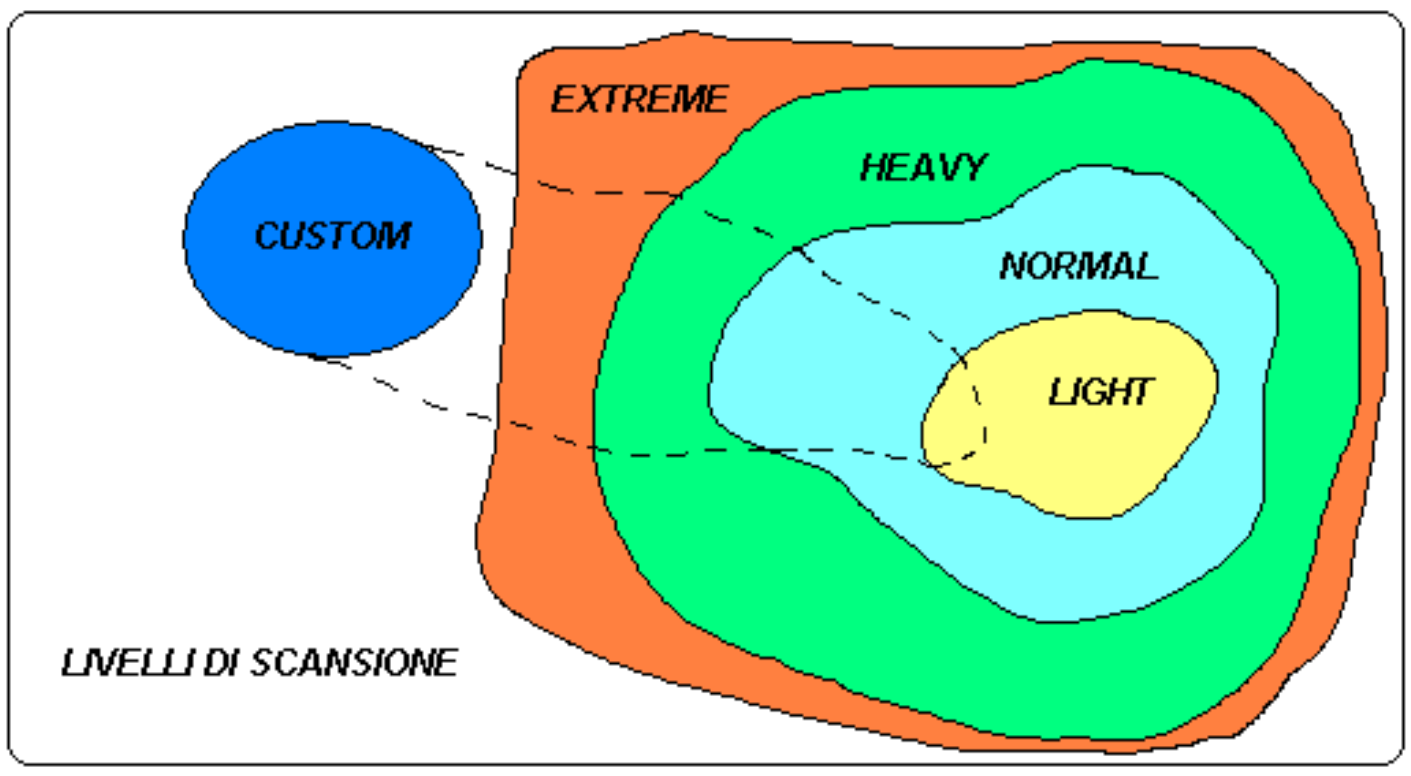


Livelli di scansione

- **Light**: raccoglie informazioni dal dns, prova a stabilire quali servizi rpc offre l'host e quali file system condivide via rete.
- **Normal**: SARA testa la presenza di servizi di rete come www, ftp rlogin ecc...
- **Heavy**: controlla se l'ftp anonimo è scrivibile al mondo, se X windows server ha il suo access control disabilitato, se c'è un "*" nel file host.equiv ecc. Non testa alcune vulnerabilità di Microsoft Windows.
- **Extreme**: Come heavy in più controlla anche Windows.
- **Custom**: personalizzabile. Si può modificare a piacimento configurandolo nel file sara.cf

Più sofisticata è la scansione maggiore risulta il tempo di esecuzione

Schema sui livelli delle scansioni



Funzionamento effettivo di SARA

Una volta lanciata una scansione SARA si comporta così:

- cerca di stabilire in base al file sara.cf se la scansione "*ha da farsi*".
- viene determinato il livello della scansione
- viene creata una lista di host da testare
- viene creata una lista di test da effettuare
- vengono lanciati i test
- I test generano "fatti" che vengono raccolti ed elaborati in modo tale da poter poi generare un ipertesto dinamico che mostri i risultati della scansione.

Gestire i database di SARA

Sara consente di memorizzare i risultati delle scansioni in database creati ad hoc.

Questi sono utili non solo per tenere traccia di ciò che si è fatto, ma anche per rieffettuare le scansioni dopo gli eventuali aggiornamenti e notare ciò che e' cambiato.

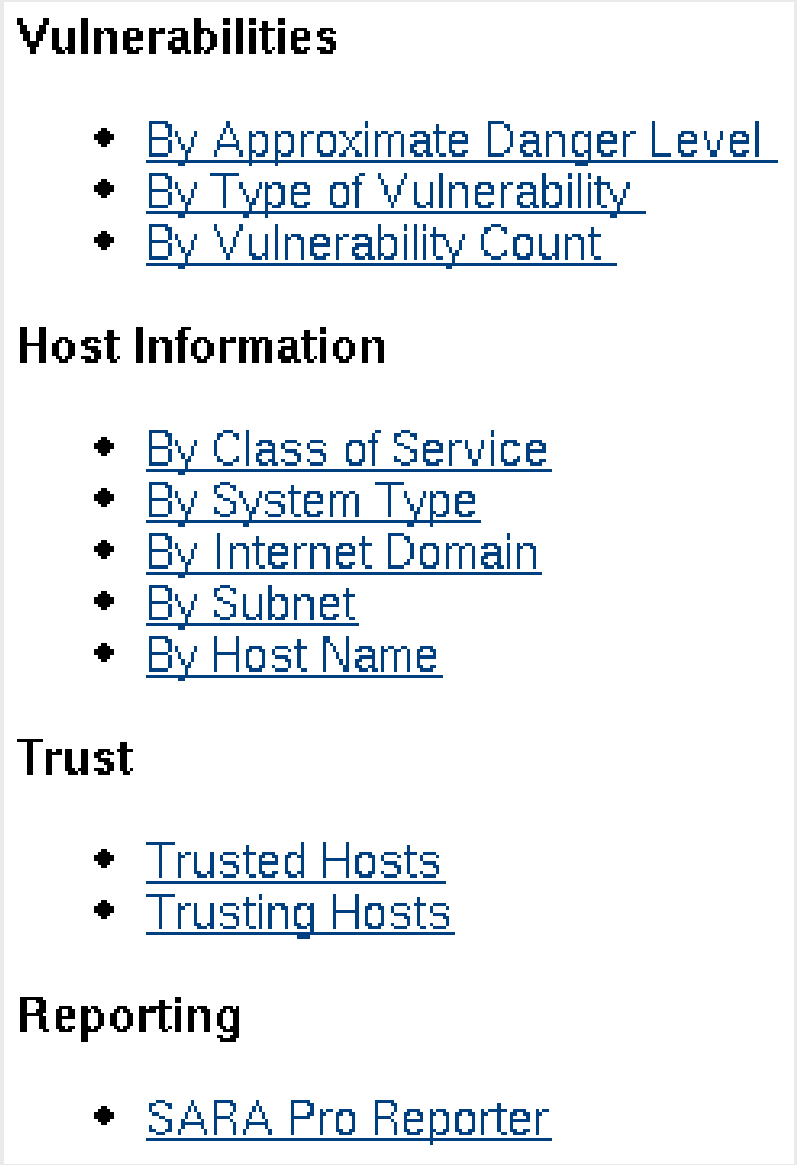
È sufficiente, sotto la sezione **"data management"**, inserire il nome del nuovo archivio da creare e premere il bottone ***open or create***. È anche possibile distruggere e fare il merge di database.

Esiste un database di default che si chiama: sara-data

Analisi delle scansioni

Sara costruisce un ipertesto che può essere sfogliato a piacimento seguendo tre tipologie di percorso:

- Vulnerabilità
- Informazioni sugli host
- Trust



Come leggere i risultati delle scansioni

Host:

- Pallina nera: l'host analizzato non presenta vulnerabilità (non significa che l'host sia sicuro per sempre)
- Pallina rossa: l'host presenta qualche vulnerabilità.

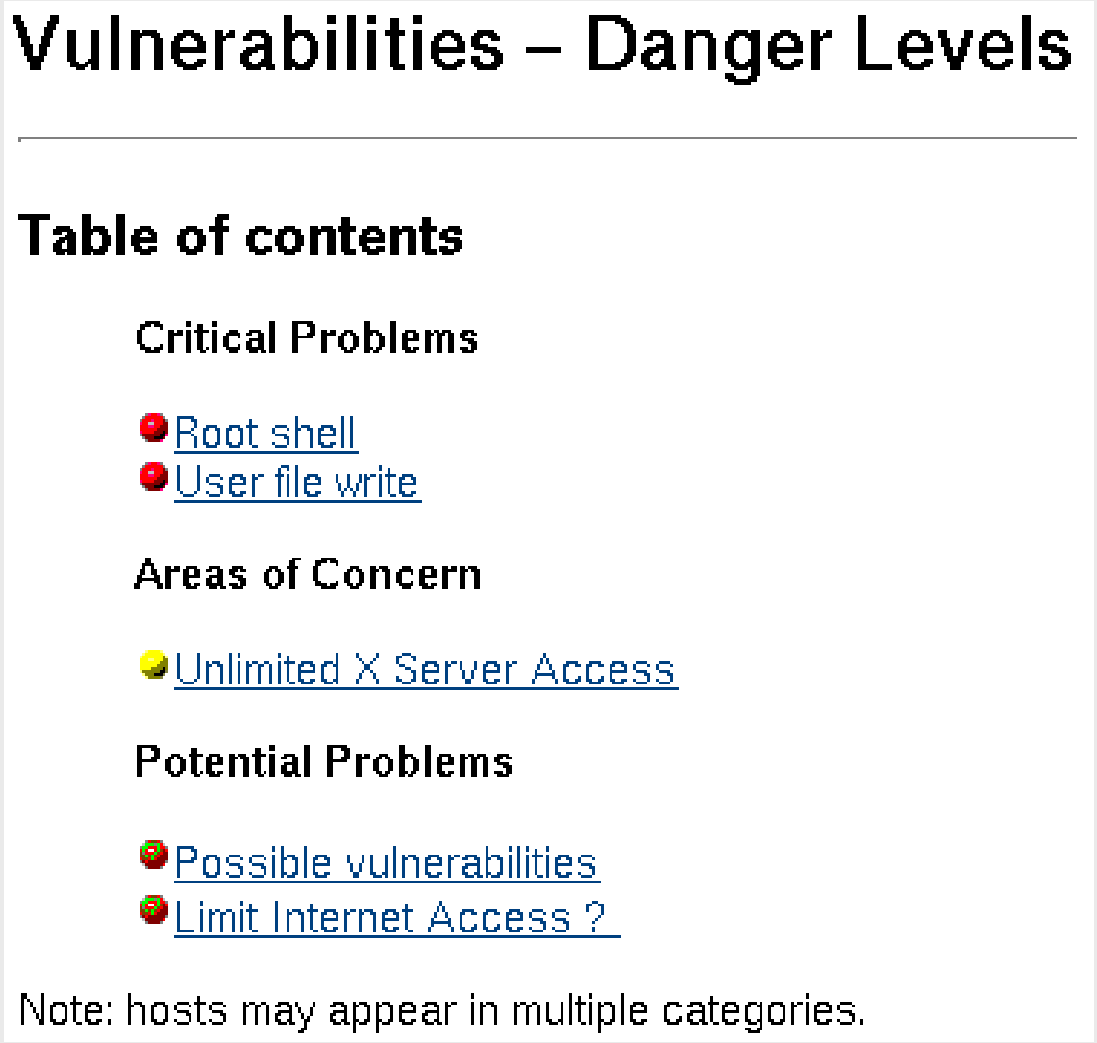
Servizi:

- Pallina verde: il servizio non è stato trovato vulnerabile
- Pallina marrone: il servizio può essere vulnerabile a degli exploit, ma SARA non è in grado di determinarlo con certezza
- Pallina rossa: il servizio presenta vulnerabilità gravi; sono possibili compromissioni dei dati o degli account.
- Pallina gialla: il servizio ha delle vulnerabilità che possono aiutare gli hacker.

Alcuni esempi di report:

Esempio 1:

si sfoglia l'ipertesto analizzando il livello di pericolosità delle vulnerabilità



Vulnerabilities – Danger Levels

Table of contents

Critical Problems

- Root shell
- User file write

Areas of Concern

- Unlimited X Server Access

Potential Problems

- Possible vulnerabilities
- Limit Internet Access ?

Note: hosts may appear in multiple categories.

Esempio 2: numero di vulnerabilità

Vulnerabilities – By Counts

Hosts by descending vulnerability counts.

- pluto.fi.infn.it Red: 1 Yellow: 1 Brown: 2
- pippo.fi.infn.it Red: 1 Brown: 2
- paperino.fi.infn.it Yellow: 1 Brown: 1
- topolino.fi.infn.it Brown: 1
- minnie.fi.infn.it Brown: 1

Esempio 3: tipo di vulnerabilità

Vulnerabilities – By Type

Number of hosts per vulnerability type.

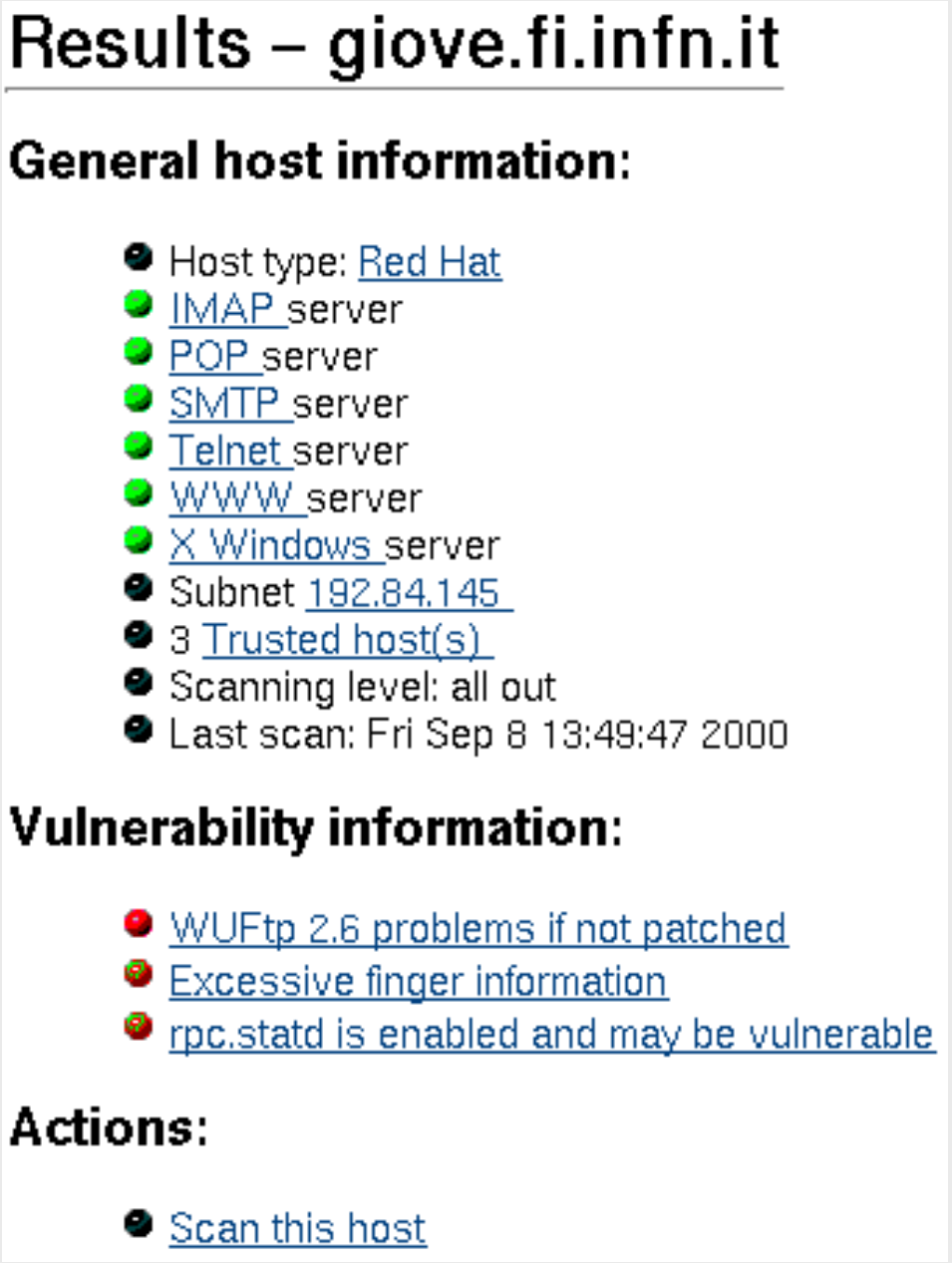
- rpc statd access – 3 host(s)
- netbios over the internet – 2 host(s)
- WUftpd vulnerabilities – 1 host(s)
- unrestricted X server access – 1 host(s)
- SSH–26 vulnerabilities – 1 host(s)
- unrestricted NFS export – 1 host(s)
- excessive finger info – 1 host(s)
- possible printer version – 1 host(s)

Note: hosts may appear in multiple categories.

Ecco i risultati della scansione su Giove:

- Il servizio di ftp è vulnerabile
- Finger fornisce troppe informazioni a chi lo interroga.
- Rpc.stand può essere vulnerabile

Si noti che cliccando sopra i link nella sezione vulnerabilità vengono fornite informazioni sui problemi a cui si va incontro e su come risolverli.



Results – giove.fi.infn.it

General host information:

- Host type: Red Hat
- IMAP server
- POP server
- SMTP server
- Telnet server
- WWW server
- X Windows server
- Subnet 192.84.145
- 3 Trusted host(s)
- Scanning level: all out
- Last scan: Fri Sep 8 13:49:47 2000

Vulnerability information:

- WUFtp 2.6 problems if not patched
- Excessive finger information
- rpc.statd is enabled and may be vulnerable

Actions:

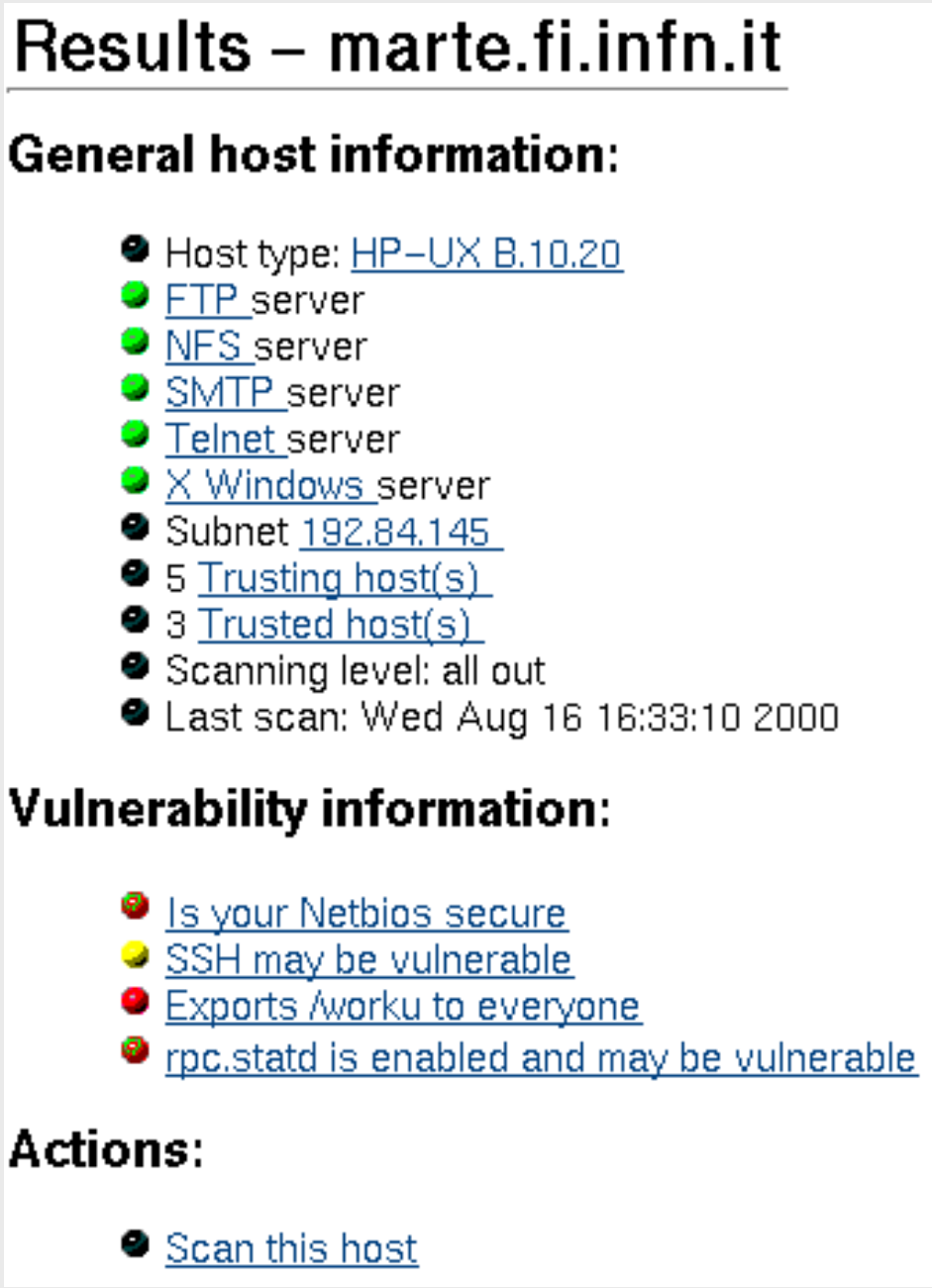
- Scan this host

Ecco i risultati della scansione su Marte:

Marte ha come sistema operativo HP- UX e fornisce molti servizi:

ftp, nfs, smtp, telnet ecc...

La vulnerabilità più grave è il fatto che esporta un disco a chiunque.



Results – marte.fi.infn.it

General host information:

- Host type: HP-UX B.10.20
- FTP server
- NFS server
- SMTP server
- Telnet server
- X Windows server
- Subnet 192.84.145
- 5 Trusting host(s)
- 3 Trusted host(s)
- Scanning level: all out
- Last scan: Wed Aug 16 16:33:10 2000

Vulnerability information:

- Is your Netbios secure
- SSH may be vulnerable
- Exports /worku to everyone
- rpc.statd is enabled and may be vulnerable

Actions:

- Scan this host

Personalizzare i test di SARA

- È sufficiente costruire un file eseguibile che svolga il test
- l’estensione del file deve essere .sara
- il test deve prendere in input l’indirizzo di un host
- il test deve restituire l’output in formato compatibile con quello accettato da sara.
- È possibile associare al file .sara un file .html che verrà inserito nell’ipertesto costruito al termine delle scansioni
- l’eseguibile deve essere contenuto nella sotto directory bin di SARA.

Dove reperire SARA

- L’autore è Bob Todd
- Il sito di distribuzione è http://www-arc.com
- la mailinglist è sara-l@mail-arc.com
- ulteriori informazioni si possono trovare sul sito http://www-arc.com/sara/ e sulla documentazione

Conclusioni

- È bene fare scansioni (solo ai propri calcolatori)
- È importante prendere atto dei risultati e risolvere i problemi che emergono.
- Non è detto che se un calcolatore risulta non vulnerabile oggi non lo sia in futuro, perciò è opportuno effettuare scansioni periodiche.