ΜΕΛΕΤΗ ΕΠΙΣΦΑΛΩΝ ΣΗΜΕΙΩΝ ΚΑΙ ΒΕΛΤΙΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΕ INTERNET HOSTS

Βροχίδης Ηλίας

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων Καθηγητής:
Χουβαρδάς Βασίλειος

Τμήμα Πληροφορικής και Επικοινωνιών
Α.Τ.Ε.Ι. Σερρών
Σέρρες

Μάρτιος 2006

Σκοπός

- Δημιουργία ενός ασφαλούς Η/Υ, που θα παίζει τον ρόλο του εξυπηρετητή (server), για τον έλεγχο απομακρυσμένων Η/Υ.
- Έλεγχος απομακρυσμένων Η/Υ (Internet Hosts).
- Μελέτη των προβλημάτων τους και αναζήτηση της λύσης αυτών.

Πρότυπα ασφαλείας

- Για την ασφάλεια του Η/Υ πρέπει να χρησιμοποιηθεί μία αυστηρά καθορισμένη πολιτική.
- Η πολιτική αυτή πρέπει να υπακούει σε κάποιο συγκεκριμένο πρότυπο ασφαλείας.
- Τα δύο πιο διαδεδομένα είναι το TCSEC και το ISO 17799 2005.

TCSEC

- Γεννήθηκε στις Ηνωμένες Πολιτείες της Αμερικής τον Αύγουστο του 1983 και είναι ευρέως γνωστό με την ονομασία «Orange Book».
- Απαιτήσεις:
  - Πολιτική Ασφαλείας
  - Κατηγοριοποίηση αντικειμένων σύμφωνα με τη σπουδαιότητα τους
  - Αναγνώριση υποκειμένων

TCSEC

- Υπευθυνότητα
- Διαβεβαίωση ασφάλειας
- Συνεχής προστασία

- Κλάσεις D, C1, C2, B1, B2, B3, A1, >A1. Λιγότερες απαιτήσεις ασφαλείας στην D και περισσότερες στην A1.

ISO 17799 2005

- Η πρώτη του έκδοση δημοσιεύτηκε στη Μεγάλη Βρετανία τον Φεβρουάριο του 1995 με την ονομασία BS 7799.
- Ενότητες:
  - Επιλογή Πολιτικής Ασφαλείας
  - Ασφάλεια επιχείρησης
  - Διαχείριση των πόρων της επιχείρησης
  - Ασφάλεια ανθρωπίνων πόρων
  - Φυσική ασφάλεια

ISO 17799 2005

- Διαχείριση συστήματος επικοινωνιών και κέντρου ελέγχου της επιχείρησης
- Έλεγχος πρόσβασης στις πληροφορίες
- Ασφάλεια πληροφοριακού συστήματος
- Διαχείριση συμβάντων σχετικών με την ασφάλεια
- Αδιάκοπη λειτουργία της επιχείρησης
- Συμμόρφωση με ανώτερους νόμους και κανόνες

Επιλογή Λ. Σ.

- Τα περισσότερο ασφαλή είναι τα Linux / Unix και τα BSD.
- Τα Linux έχουν μεγαλύτερη τεκμηρίωση και υποστήριξη.
- Ιδιαίτερα ασφαλής και διαδεδομένη είναι η διανομή Debian.

Απαραίτητες ρυθμίσεις

- Κρυπτογράφηση των κωδικών των χρηστών του λειτουργικού συστήματος
- Απενεργοποίηση των δικαιωμάτων του διαχειριστή συστήματος στους απλούς χρήστες.
- Απενεργοποίηση των περιττών υπηρεσιών.

AIDE

- Ελέγχει την ακεραιότητα των αρχείων του Η/Υ και έτσι ανιχνεύονται τυχόν εισβολές και αλλοιώσεις των αρχείων.
- Εγκαθίσταται όσο το δυνατόν νωρίτερα, διατηρεί Β. Δ. με την κατάσταση των αρχείων και την συγκρίνει με την κατάσταση των αρχείων σε μετέπειτα χρονικές στιγμές.

xinetd

- Δαίμονας που αντικαθιστά το inetd.
- Πολύ πιο ασφαλής.
- Καταγράφει τα συμβάντα που αφορούν στις υπηρεσίες.
- Παρ’ όλη την ασφάλεια που παρέχει, όπως και στο inetd, πρέπει να απενεργοποιηθούν οι περιττές υπηρεσίες.

John the Ripper

- Προσπαθεί να μαντέψει τους κωδικούς των χρηστών του λειτουργικού συστήματος, δοκιμάζοντας συνεχώς ένα πλήθος κωδικών.
- Προειδοποιεί για ευνόητους κωδικούς.
- Λειτουργεί ακόμη και όταν οι κωδικοί είναι κρυπτογραφημένοι.

Bastille

- Αυτοματοποιεί τη διαδικασία της δημιουργίας ενός ασφαλούς Η/Υ, αναλαμβάνοντας τις ρυθμίσεις που απαιτούνται.
- Οι ρυθμίσεις διαμορφώνονται με την απάντηση 45 ερωτήσεων, που χωρίζονται σε 10 κατηγορίες.

nmap

- Ένα από τα πιο σοβαρά προγράμματα σάρωσης θυρών (Port Scanner).
- Ελέγχει την κατάσταση των θυρών απομακρυσμένων Η/Υ και προειδοποιεί για όσες είναι ανοιχτές.

The SYN Stealth Scan took 26785.04s to scan 65535 total ports.

Host dns2.teiser.gr (195.130.67.5) appears to be up ... good.

Interesting ports on dns2.teiser.gr (195.130.67.5):

PORT	STATE	SERVICE
21/tcp	open	ftp
53/tcp	open	domain
80/tcp	open	http

Sniffers

- Η λειτουργία τους είναι να υποκλέπτουν τα δεδομένα που μεταφέρονται μέσω των δικτυακών καλωδίων.
- Μπορούν να χρησιμοποιηθούν για να υποκλαπούν σημαντικοί κωδικοί, αλλά και για να λυθούν προβλήματα του δικτύου.
- Iris Network Traffic Analyzer, Sniffer Portable, Ultra Network Sniffer, ethereal, Snort.

Υποκλοπή κωδικού

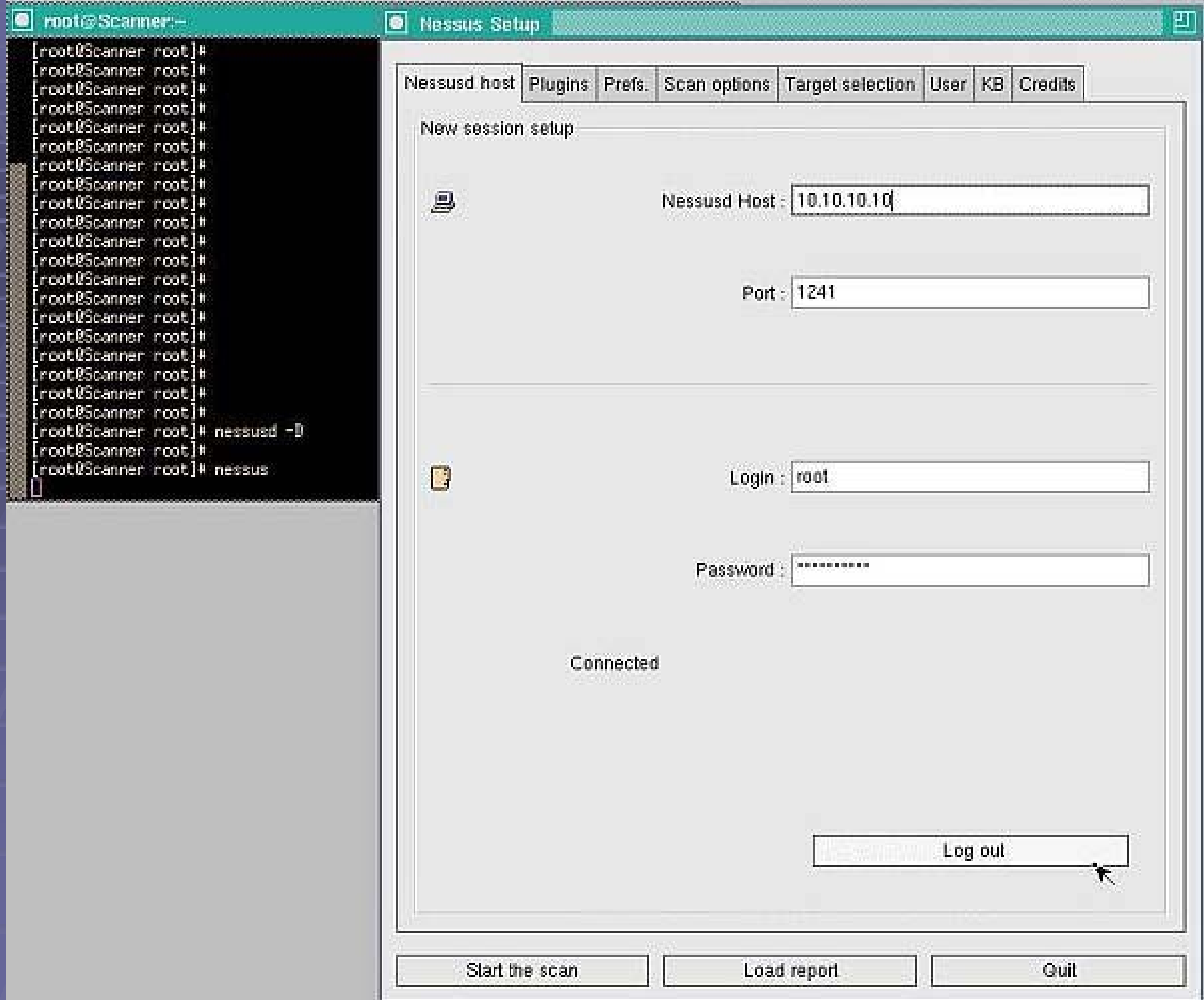
..O'C5.0.1A...E.
.|..@...u.....?
...c.P. .....P.
.sT...username=h
ackme01&password
=dokimi&URL=%2Fe
mail&Submit.x=55
&Submit.y=13&Sub
mit=Submit

Vulnerability Analyzers

- Με αυτά γίνεται ο έλεγχος των απομακρυσμένων Η/Υ για σφάλματα στην ασφάλειά τους.
- Περιλαμβάνουν τη σάρωση των θυρών και την έρευνα για γνωστά προβλήματα ασφαλείας.
- Ένας πλήρης έλεγχος ενός Η/Υ διαρκεί κατά μέσο όρο 7 έως 9 ώρες.

nessus

- Λειτουργεί σε Linux.
- Η αρχιτεκτονική του είναι server – client.
- Ο client διατίθεται και για Windows.
- Είναι πρόγραμμα ανοιχτού κώδικα.
- Έχει πλούσια τεκμηρίωση και παρέχεται πολύ καλή υποστήριξη.
- Για τους ελέγχους του χρησιμοποιεί Plugins.


root@Scanner:~
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]#
[root@Scanner root]# nessusd -D
[root@Scanner root]#
[root@Scanner root]# nessus
Nessus Setup
Nessusd host
Plugins
Prefs.
Scan options
Target selection
User
KB
Credits
New session setup
Nessusd Host : 10.10.10.10
Port : 1241
Login : root
Password : ••••••••••
Connected
Log out
Start the scan
Load report
Quit

Α.Τ.Ε.Ι. Σερρών

- Βρέθηκαν 11 προβλήματα, εκ των οποίων κανένα δεν ήταν κρίσιμο, 2 ήταν προειδοποιητικά και 9 ήταν πληροφοριακά.
- Βρέθηκαν 4 θύρες ανοιχτές.
- Ο έλεγχος διήρκησε 9 ώρες και 1 λεπτό.

Synopsis :
A FTP server is listening on this port

Description :
It is possible to obtain the banner of the remote FTP server
by connecting to the remote port.

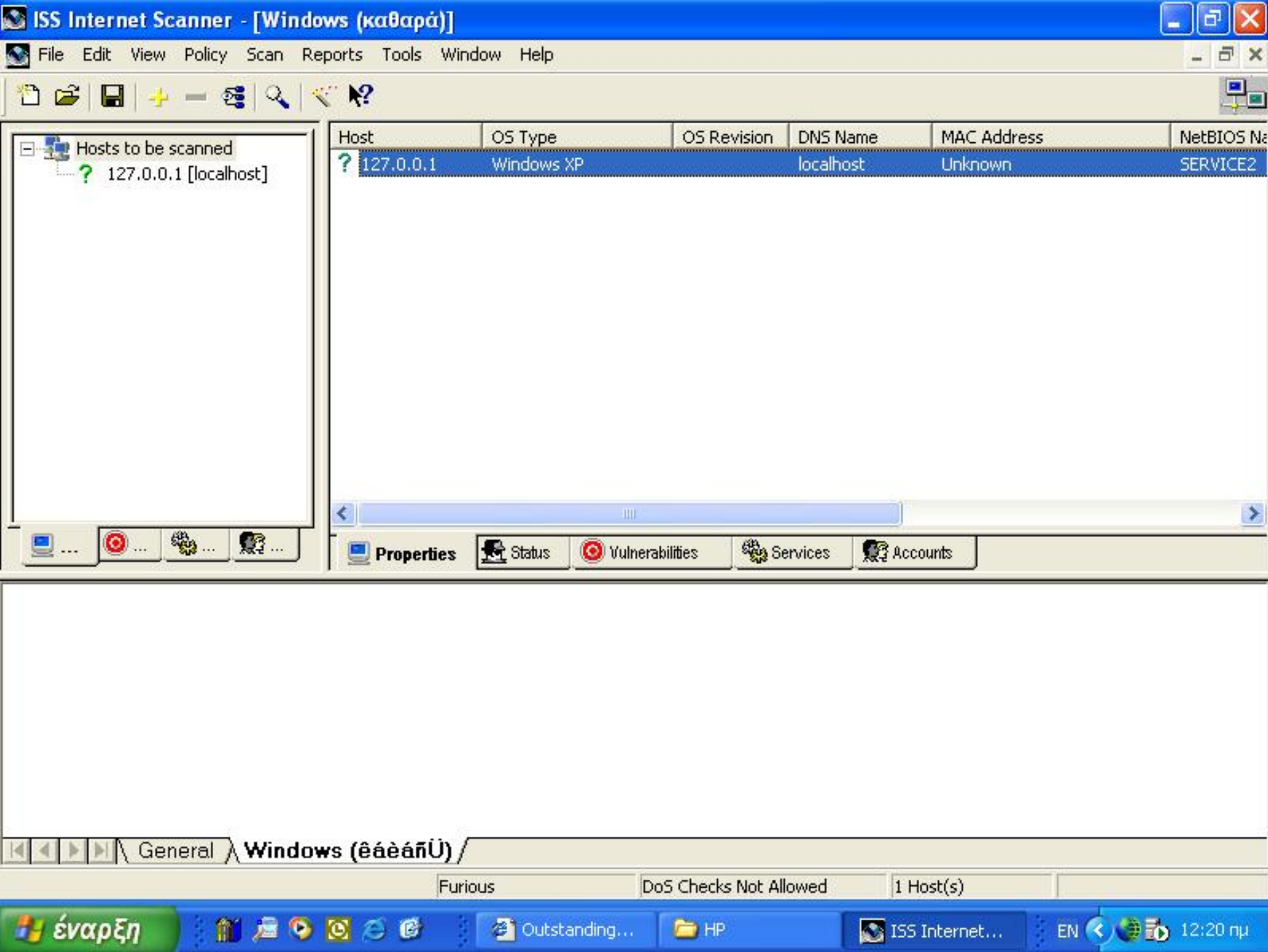
Risk factor :
None
Plugin output :
The remote FTP banner is :
220 Microsoft FTP Service

Nessus ID : 10092

ISS Internet Scanner

- Λειτουργεί σε Windows.
- Σε Η/Υ με Windows βρήκε 77 προβλήματα, εκ των οποίων 6 σοβαρά, 28 μέσης σημασίας και 43 χαμηλής σημασίας.
- Ανοιχτές θύρες δε βρέθηκαν.
- Ο έλεγχος διήρκησε 13 ώρες και 14 λεπτά.

Passfilt.DLL checksum: Passfilt.dll checksum incorrect: Passfilt.dll is referenced in the Lsa registry key, but the file found in %systemroot%\system32 had a checksum that did not match any known passfilt.dll files shipped by Microsoft. A file that is the correct size, but possesses the wrong checksum, could indicate an attacker
is capturing passwords.


ISS Internet Scanner - [Windows (καθαρά)]
File Edit View Policy Scan Reports Tools Window Help
Hosts to be scanned
127.0.0.1 [localhost]
Host
OS Type
OS Revision
DNS Name
MAC Address
NetBIOS Na
127.0.0.1
Windows XP
localhost
Unknown
SERVICE2
Properties
Status
Vulnerabilities
Services
Accounts
General
Windows (êáèáñÜ)
Furious
DoS Checks Not Allowed
1 Host(s)
έναρξη
Outstanding...
HP
ISS Internet...
EN
12:20 πμ

Retina Network Security Scanner

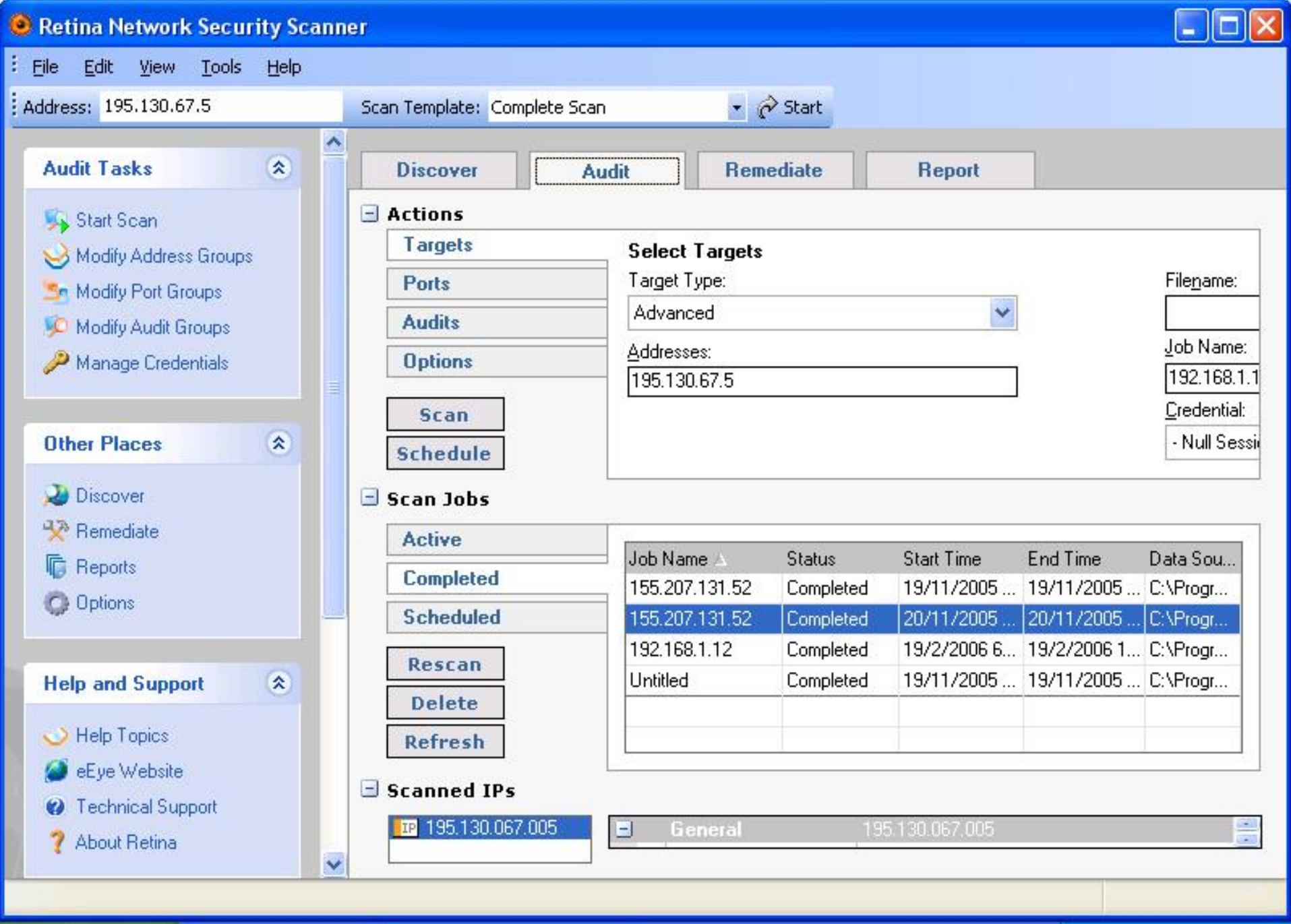
- Λειτουργεί σε Windows.
- Στον εξυπηρετητή του Α.Τ.Ε.Ι. Σερρών βρέθηκε μόνο ένα πρόβλημα μέσης σημασίας.
- Βρέθηκαν 5 ανοιχτές θύρες.
- Ο έλεγχος διήρκησε 4 ώρες και 17 λεπτά.

Anonymous FTP

Risk Level: Medium

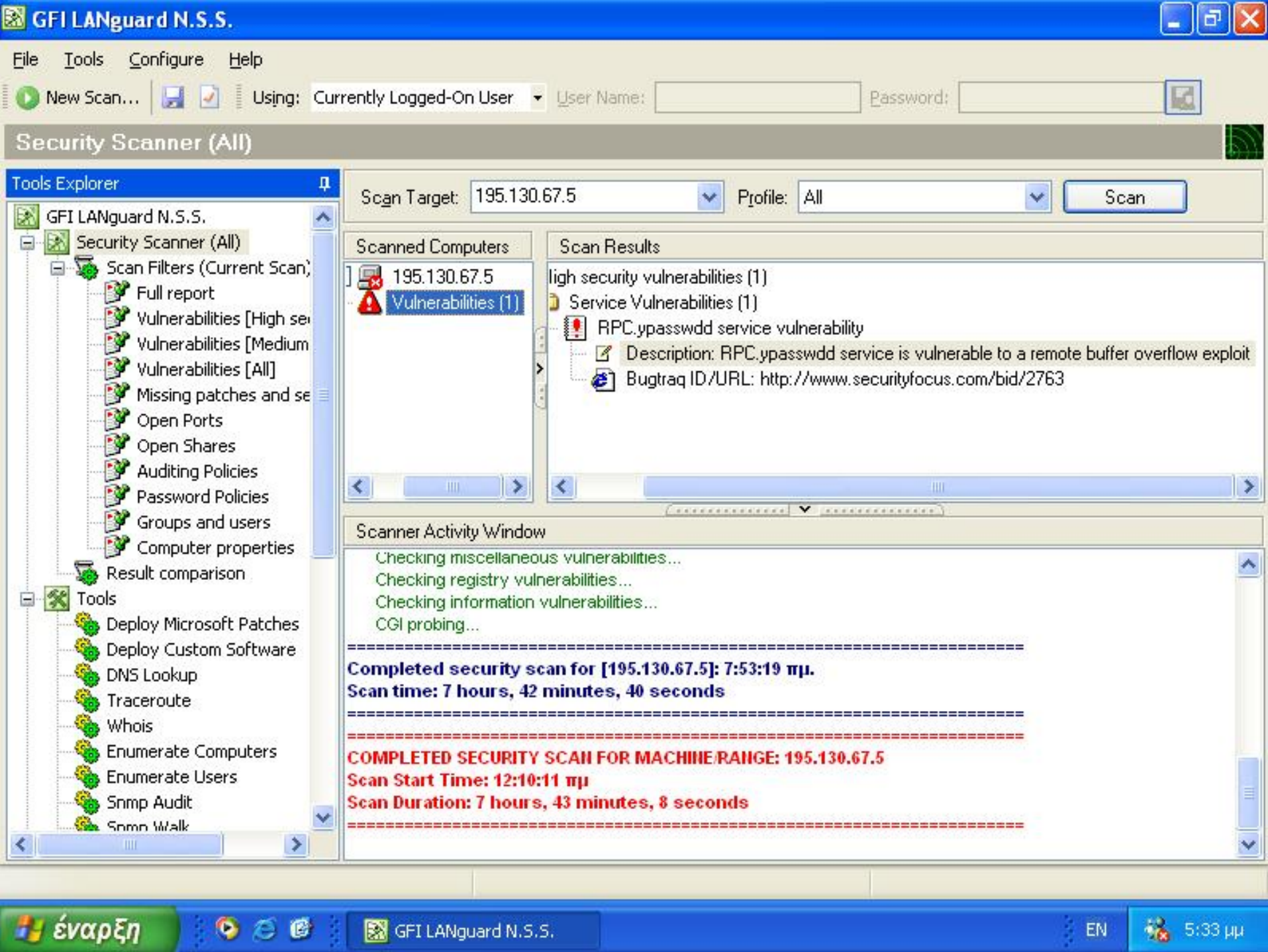
Category: FTP Servers

Description: It is recommended that you disable anonymous FTP access if it is not needed. Anonymous FTP access can lead to an attacker gaining information about your system that can possibly lead to them gaining access to your system.


Retina Network Security Scanner
File Edit View Tools Help
Address: 195.130.67.5
Scan Template: Complete Scan
Start
Audit Tasks
Start Scan
Modify Address Groups
Modify Port Groups
Modify Audit Groups
Manage Credentials
Other Places
Discover
Remediate
Reports
Options
Help and Support
Help Topics
eEye Website
Technical Support
About Retina
Discover
Audit
Remediate
Report
Actions
Targets
Ports
Audits
Options
Scan
Schedule
Select Targets
Target Type:
Advanced
Addresses:
195.130.67.5
Filename:
Job Name:
192.168.1.1
Credential:
- Null Sessi
Scan Jobs
Active
Completed
Scheduled
Rescan
Delete
Refresh
Job Name
Status
Start Time
End Time
Data Sou...
155.207.131.52 Completed 19/11/2005 ... 19/11/2005 ... C:\Progr...
155.207.131.52 Completed 20/11/2005 ... 20/11/2005 ... C:\Progr...
192.168.1.12 Completed 19/2/2006 6... 19/2/2006 1... C:\Progr...
Untitled Completed 19/11/2005 ... 19/11/2005 ... C:\Progr...
Scanned IPs
195.130.067.005
General
195.130.067.005
έναρξη
Retina Network Secur...
EN
9:18 πμ

GFI LANguard Network Security Scanner

- Λειτουργεί σε Windows.
- Στον εξυπηρετητή του Α.Τ.Ε.Ι. Σερρών βρέθηκε ένα σοβαρό πρόβλημα.
- Δε βρέθηκαν ανοιχτές θύρες.
- Ο έλεγχος διήρκησε 7 ώρες και 43 λεπτά.


GFI LANguard N.S.S.
File Tools Configure Help
New Scan... Using: Currently Logged-On User User Name: Password:
Security Scanner (All)
Tools Explorer
GFI LANguard N.S.S.
Security Scanner (All)
Scan Filters (Current Scan)
Full report
Vulnerabilities [High se
Vulnerabilities [Medium
Vulnerabilities [All]
Missing patches and se
Open Ports
Open Shares
Auditing Policies
Password Policies
Groups and users
Computer properties
Result comparison
Tools
Deploy Microsoft Patches
Deploy Custom Software
DNS Lookup
Traceroute
Whois
Enumerate Computers
Enumerate Users
Snmp Audit
Snmp Walk
Scan Target: 195.130.67.5 Profile: All Scan
Scanned Computers
195.130.67.5
Vulnerabilities (1)
Scan Results
ligh security vulnerabilities (1)
Service Vulnerabilities (1)
RPC.ypasswdd service vulnerability
Description: RPC.ypasswdd service is vulnerable to a remote buffer overflow exploit
Bugtraq ID/URL: http://www.securityfocus.com/bid/2763
Scanner Activity Window
Checking miscellaneous vulnerabilities...
Checking registry vulnerabilities...
Checking information vulnerabilities...
CGI probing...
Completed security scan for [195.130.67.5]: 7:53:19 πμ.
Scan time: 7 hours, 42 minutes, 40 seconds
COMPLETED SECURITY SCAN FOR MACHINE/RANGE: 195.130.67.5
Scan Start Time: 12:10:11 πμ
Scan Duration: 7 hours, 43 minutes, 8 seconds
έναρξη
GFI LANguard N.S.S.
EN
5:33 μμ

Σύνοψη

- Δημιουργία ασφαλούς Η/Υ:
  - Σχεδιασμός βάση κάποιου προτύπου ασφαλείας
  - Εγκατάσταση κατάλληλου Λ. Σ.
  - Ρυθμίσεις ασφαλείας
- Μελέτη επισφαλών σημείων σε Internet Hosts:
  - Port Scanners
  - Sniffers
  - Vulnerability Analyzers
- Βελτίωση της ασφάλειας σε Internet Hosts:
  - Εγκατάσταση αρχείων διόρθωσης (patches)
  - Εγκατάσταση και ρύθμιση προγραμμάτων για τη βελτίωση του βαθμού ασφαλείας του Η/Υ
  - Ρυθμίσεις στο λειτουργικό σύστημα