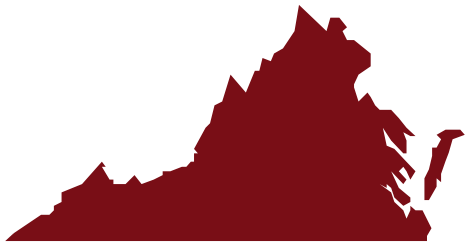
VirginiaTech

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY



Invent the Future

# SafetyNet:
## An Open Source, Self-Service, Proactive Security Scanner

By Marc DeBonis
Virginia Tech
SETI-MIG
Systems Architect, Sr.
060404 v1.1

# Obligatory Copyright Statement

# Agenda

- Introduction
- Background
- Proposal
- Development
- Production
- Post mortem
- Resources

# Introduction

- VT
  - Oddly enough, we're not Vermont! ;)
  - Full name is
    - Virginia Polytechnic Institute and State University
  - Well known for our football team.  Go Hokies!
  - Public land grant university established in 1872
    - Located in Montgomery County, SW Virginia
    - Largest full-time student population in VA
    - 2,600 acre main campus, 1,700 acre agri farm
    - ~28,000 students, 83% undergrad, 17% grad
    - 1,281 full time faculty, 66% tenured
    - 185,000 living alumni from over 100 countries
    - http://www.vtnews.vt.edu/factbook/FBabout.php

# Introduction

- Large salaried personnel base
  - 1,281 Full-Time Instructional Faculty
  - 1,463 Research Associates
  - 224 Instructional Associates
  - 3,515 Support Staff
- My group and I fall under the Support Staff category

# Introduction

- CIT - Central IT
  - Information Technology
    - I work under this branch
- DIT - Distributed IT
  - Every department, college, school, etc that has any sort of IT staff
    - Salaried, wage, co-opted, graduate student, etc

# Introduction

- Under CIT - Information Technology
  - SETI
    - Secure Enterprise Technology Initiatives
    - MIG
      - Microsoft Implementation Group
- I manage the MIG group

# Introduction

- MIG - Microsoft Implementation Group
  - ADOPT
    - new MS applications, systems and services in a controlled and timely manner
    - future MS technologies to showcase and highlight benefits, pros and cons
    - testing and feedback methodologies for existing MS products
    - http://vtmig.w2k.vt.edu

# Introduction

- MIG - Microsoft Implementation Group
  - ADAPT
    - existing MS technology and customize it for a university specific setting
    - computing infrastructure based on MS technology and provide to university customers
    - MS and open source technology to provide best-of-breed results

# Introduction

- MIG - Microsoft Implementation Group
  - IMPROVE
    - existing and "last-mile" service and support to avoid "dropped" issues
    - in-house hardware and software to gain greatest benefit from MS relations
    - between VT and MS marketing, support and developers

# Introduction

- Staff of five
  - Myself - Manager/Systems Architect
    - 1 full time web developer
    - 1 part time developer
    - 1 developer/system administrator
    - 1 data curator/developer

    - http://vtmig.w2k.vt.edu/staff

# Introductions

- Interface with Microsoft pre and post sales staff
- Monthly status meetings with our MS reps
- Contract with MS PSS (Premier Support Services) - TAM (Technical Account Manager) interface, support incidents and proactive hours
- Subscription to MSDN Universal
- Subscription to “Directions on Microsoft”
- Involved in many open and closed MS betas

# Introduction

- Main focus
  - Deployment, support and maintenance of the VT Windows 2003 Active Directory forest
  - Development of security related applications and services
  - Outreach and educational relations
  - Research and development
  - Commitment to open-source

# Introductions

- Recently completed projects
  - Hokies Self-Service
  - OU admin
  - Neighborhood Watch
  - Sunflower
  - Daisy
  - MFM (Medium Facilities Management)
  - *SafetyNet*

  - http://vtmig.w2k.vt.edu/progress.htm

# Introductions

- Works in progress
  - WSUS for F/S
    - http://wsuswiki.w2k.vt.edu
  - ADadmin
  - http://vtmig.w2k.vt.edu/progress.htm

# Introductions

- Q&A?

# Background

- A major Windows system vulnerability appeared on the scene
  - MS03-026 (Buffer overrun in RPC interface)
  - It affected all version of Windows (NT and up)
- I emailed our technical support listserv list about it but got very little response

# Background

- MS released a hotfix for it on July 16th, 2003
- There was very little noise about it and the CIT/DIT community seemed pretty apathetic about it
- VT's network is "open"
  - Each IP by default is publicly network accessible
- I began to worry that the vulnerability was potentially a "super worm" issue

# Background

- I decided (with *indirect* management approval) to attempt a reactive scan of our two class-B IP ranges
  - Scanned using the Eeye tool on July 30th
    - 128.173.x.x and 198.82.x.x
    - Out of 15,000 pingable systems
      - Found over 2,000 still vulnerable
- I posted my results to the listserv and emailed the NLs (network liaisons)
  - A primary and secondary NL are identified for each Department/DNS zone within the IP space

# Background

- Sample of NL list
  - Department name — Administrative Info Systems
  - Sub-domain — ais.vt.edu
  - Liaision name — Joe User
  - Liaison e-mail address — jouser@vt.edu
  - Alternate Liaison — Jane User
  - Alternate Liaison e-mail — jauser@vt.edu
- NLs originally created to act as “liaisons” to our DNS hostmaster
  - There are now probably close to ≈300 entries

# Background

- Proactive scanning
  - Aug 14th (+2 weeks)
    - 105 systems still vulnerable
  - Aug 18th (+2.5 weeks)
    - 77 systems still vulnerable
    - Exploit now in the wild so I added likely trojan port scanning…

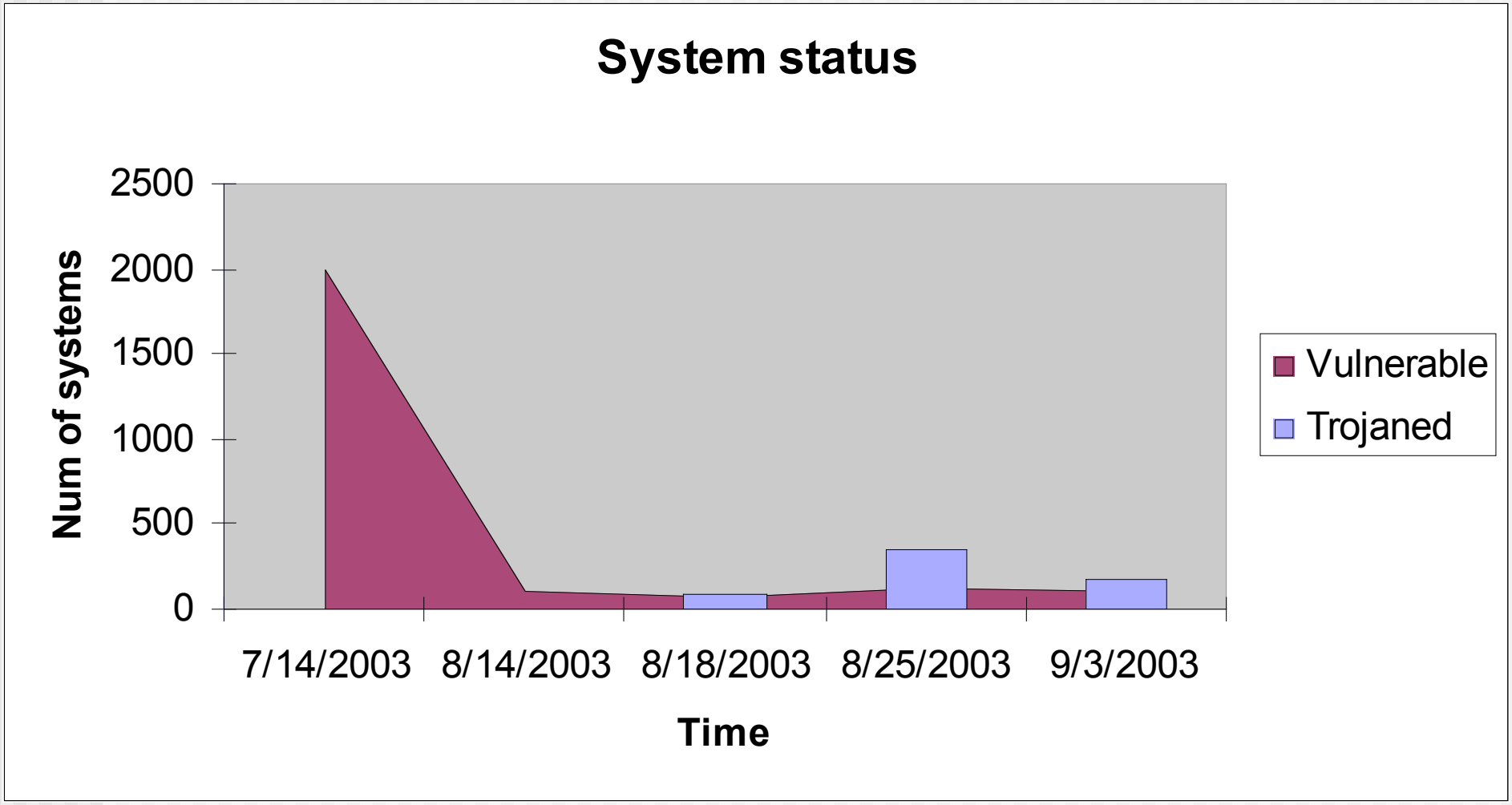
# Background

- Reactive scanning
  - Aug 18th (+2.5 weeks)
    - 81 systems likely trojaned
  - Aug 25th (+3 weeks)
    - Students return from break
    - 126 systems vulnerable
    - 347 systems likely trojaned

# Background

- Reactive scanning
  - Sep 3rd (+4 weeks)
    - 110 systems vulnerable
    - 179 systems likely trojaned
  - Management intervenes and cancels scanning…

# Background


System status
Num of systems
2500
2000
1500
1000
500
0
7/14/2003
8/14/2003
8/18/2003
8/25/2003
9/3/2003
Time
Vulnerable
Trojaned

# Background

- Responses to scanning
  - "The /dev/null"
    - Absolutely no response on list or off
    - No email, phone call or CIT helpdesk trouble tickets
    - Partially a turnover and provisioning issue with the NL list
    - Partially an issue with the opt-in process of joining IT related listservs
    - NL primary and/or secondary were students on break
    - Invalid or missing IP->DNS mapping
    - Many were ephemeral (modem pool or DHCP)
    - Other reasons?

# Background

- Responses to scanning
  - “The huh?”
    - Get contacted about my warning email with very general or mis/uninformed questions
    - NLs generally tend to be co-opted staff with little to no IT exp
    - NLs original intent was to interface with hostmaster
    - Attempted to reference them to our CIT helpdesk

# Background

- Responses to scanning
  - “The how-dare-you!/you-are-breaking-the-law!”
    - IT admins from different departments telling me I was invading their “walled gardens”
    - Several contacted my management attempting to misquote the AUP (Acceptable User Policy)
    - Wanted me to specifically exclude their IP ranges from future scans or me to tell them the ranges I was scanning from
    - Our policy isn’t specific about network scans…
    - * insert funny/ironic story here *

# Background

- Responses to scanning
  - "The quiet thanks-I'll-fix-it"
    - Didn't want to see their departments get a bloody nose on the IT listserv (wall of shame)
    - Didn't patch or remediate when patch was first available (constant fire-fighting mode)
    - Wanted to stop or avoid the "scorched earth approach" to rebuilding trojaned systems
    - Majority of responses were of this type
      - Which was positive but was never reiterated externally to my management

# Background

- Responses to scanning
  - “The outspoken thanks a lot!”
    - Admitted fully to the problem
    - Appreciated the help
    - Was willing to accept constructive criticism
    - Told my management the scanning was helpful to them and their computing infrastructure

# Background

- Management intervention
  - Didn’t like the bad publicity from the noisy walled garden crowd
  - Told me to specifically exclude these ranges (with the Eeye tool) or stop scanning all together
  - Since this wasn’t specifically in my job description and I thought the situation was resolving itself I voluntarily stopped

# Background

- Situation analysis
  - Where the process broke down
    - Lack of proactive patching
    - Lack of proper communications channels
    - Lack of local control of scans
    - Lack of good tools to do scans
    - Lack of good feedback/instructions
    - Lack of historic measurement

# Background

- Q&A?

# Proposal

- General discovery phase to identify existing closed source or open source technology that would solve the issues raised

# Proposal

- Close source
  - Moderate to expensive closed source solutions
    - Most lacked delegated management
    - Some required yearly subscriptions
    - Most charged based off # of IPs
    - Still needed to build local KB articles
    - Many of them were just badly written!

# Proposal

- Open source
  - Found one or two potential solutions
    - Many where unix only (nessus based)
    - Didn’t allow for the necessary level of granularity
    - Were more designed for quarantine than penetration testing

# Proposal

- Built a project request Sep 9, 2003
  - Goal:
    - “To develop a centralized web application for VT computer users to proactively and remotely scan their systems for vulnerabilities and penetration testing”
  - Requirements:
    - Modular
    - Centralized
    - Delegated authority model
    - Keep historical data of scans

# Proposal

- Requirements document defined Jan 27, 2004
- Received sponsorship from the IT Security Office on March 3, 2004
- Sponsorship is required for production application and hardware support for almost all MIG projects
  - This delineation (in the Windows world) is usually somewhat awkward and arbitrary
  - Required we build a MOU (Memorandum of Understanding) with our sponsor

# Proposal

- Project plan developed and costs spec'ed
  - Timeline for completion was July 1, 2004
  - Executive management included the additional requirements of:
    - Enhanced scalability
    - Restrict to Faculty and Staff access
    - Allow IT security office unfettered access to scan histories

# Proposal

- Q&A?

# Development

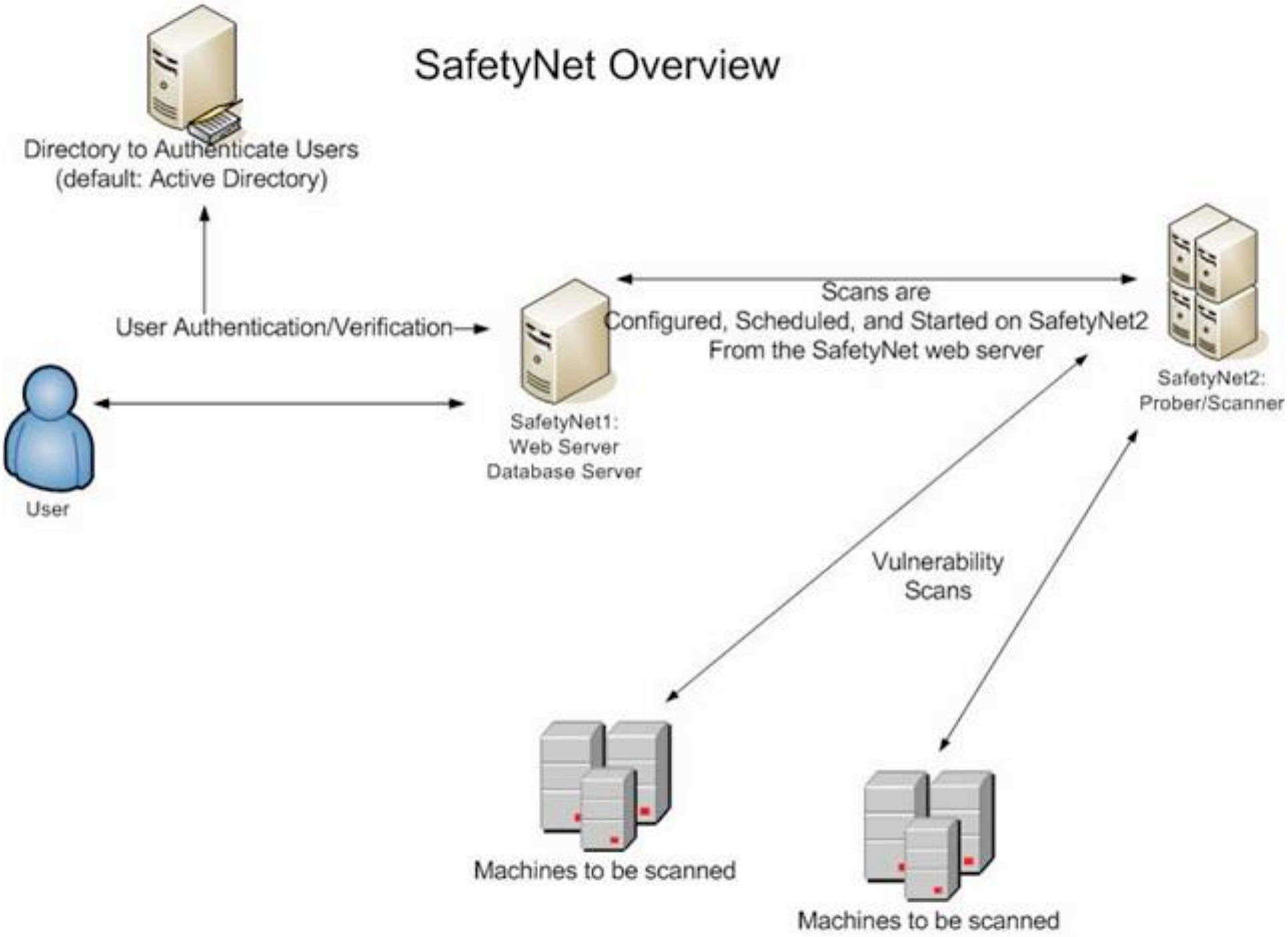
- Received funding for
  - Two Dell 2850 development systems
  - $ for Windows 2003 Server Web Edition
  - $ for Gb Ethernet lines
- It was intended that the development systems would be switched over to run as the production systems

# Development

- Open source technology for the systems
  - PHP
  - MySQL
  - C/C++
  - Cygwin
  - WinPcap
- Closed source
  - IIS
  - Winbatch
  - Active Directory

# Development

- Staffing
  - 1 full time programmer
    - Front end
      - Web development
      - DB development
      - Docs/Testing
  - 1 full time programmer
    - Back end
      - App development
      - Module development
      - Docs/Testing


SafetyNet Overview
Directory to Authenticate Users
(default: Active Directory)
User Authentication/Verification
Scans are
Configured, Scheduled, and Started on SafetyNet2
From the SafetyNet web server
SafetyNet2:
Prober/Scanner
User
SafetyNet1:
Web Server
Database Server
Vulnerability
Scans
Machines to be scanned
Machines to be scanned

## Please Log-In

SafetyNet is provided to allow computer users and systems administrators at Virginia Tech the ability to proactively perform centralized security scans of their systems.

For more information about using SafetyNet **Click Here**.

To log in simply enter your **Hokies ID** and password below.

Hokies\:

Password:

Log-In Reset

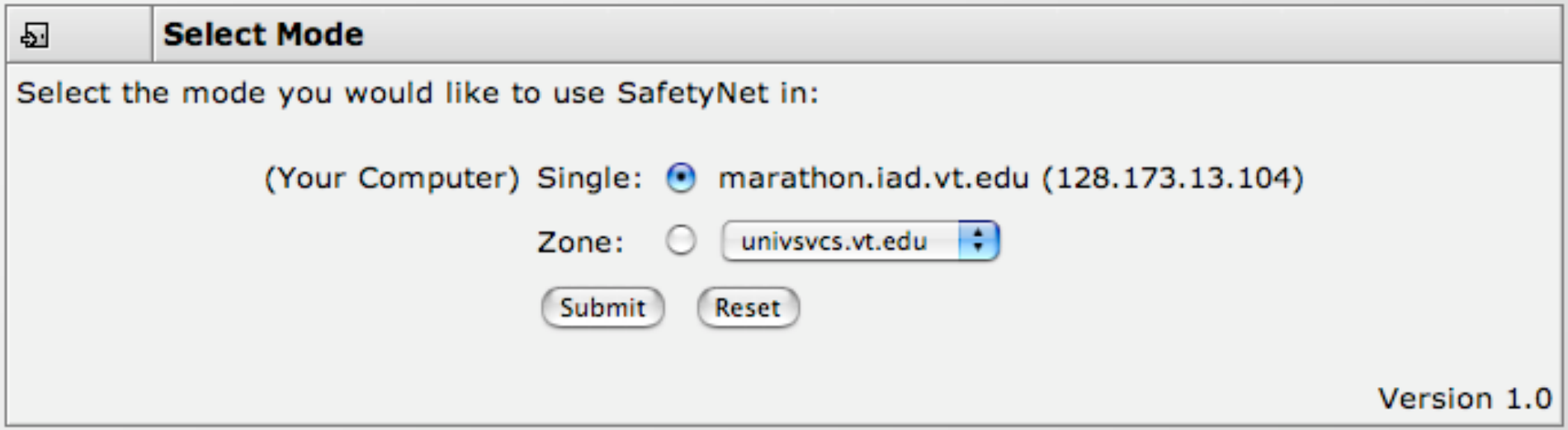
Version 1.0


*- We utilize an SSL certificate signed by the VT CA to encrypt data transmitted to and from this site. Click here for information about installing the VT Root CA Certificate.*

*The SafetyNet website was developed by VTmig (Virginia Tech Microsoft Implementation Group) and is maintained by the VT IT Security Office.*

*View our detailed Privacy Statement*

*Cookies & Javascript must be enabled to use SafetyNet.*


Select Mode
Select the mode you would like to use SafetyNet in:
(Your Computer) Single:
marathon.iad.vt.edu (128.173.13.104)
Zone:
univsvcs.vt.edu
Submit
Reset
Version 1.0

Home | Access Settings | Scan History | Scan Wizard | Documentation

Questions/Comments | LOGOUT

## Welcome to SafetyNet - Security Scanning Tool

### Home
This section provides descriptions for all of the tabs in SafetyNet.

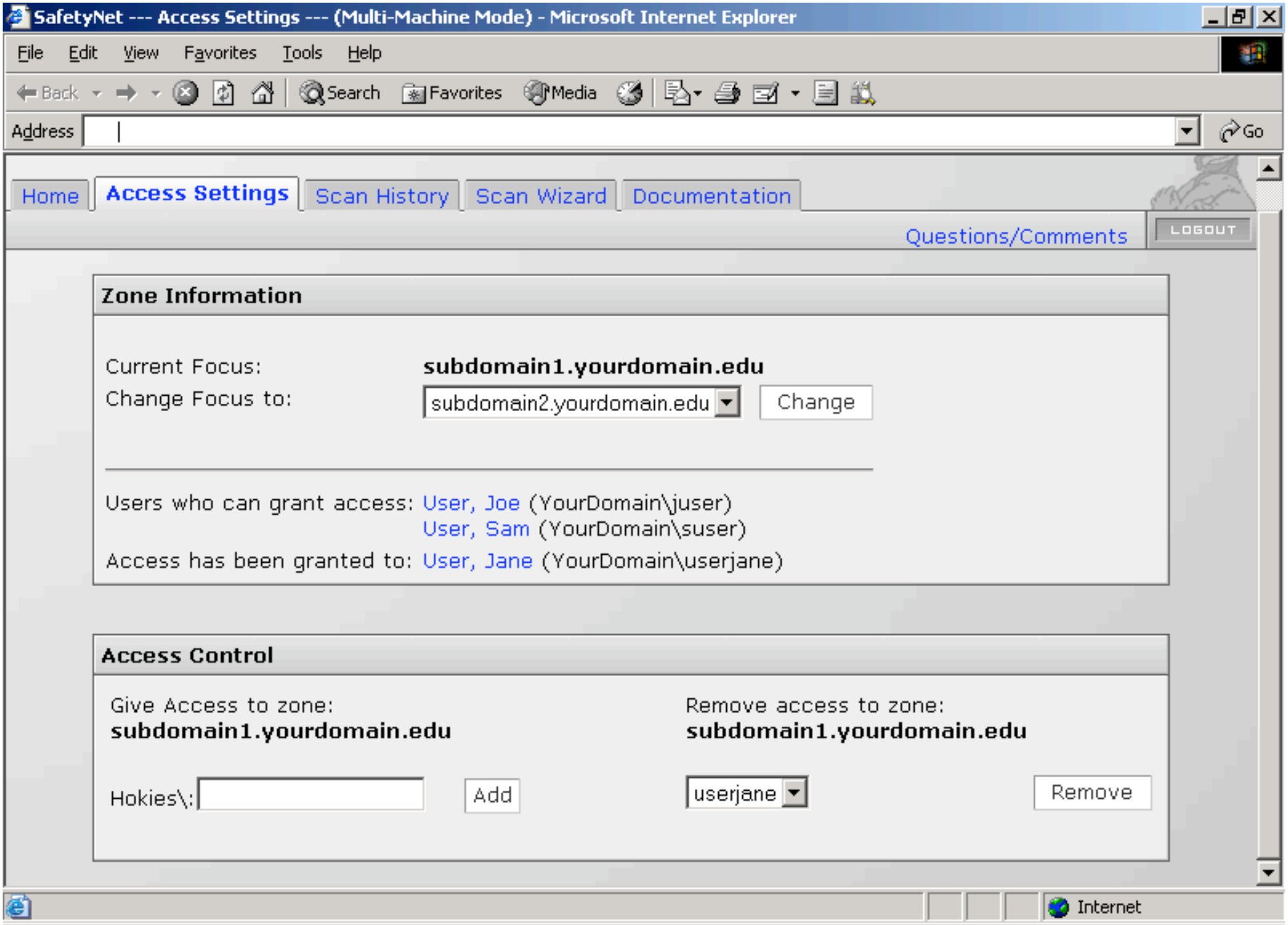
### Access Settings
This section allows network liaisons the ability to authorize other Hokies accounts to scan their DNS zone. If you are a network liaison for more than one DNS zone you may change the focus of your current DNS zone.

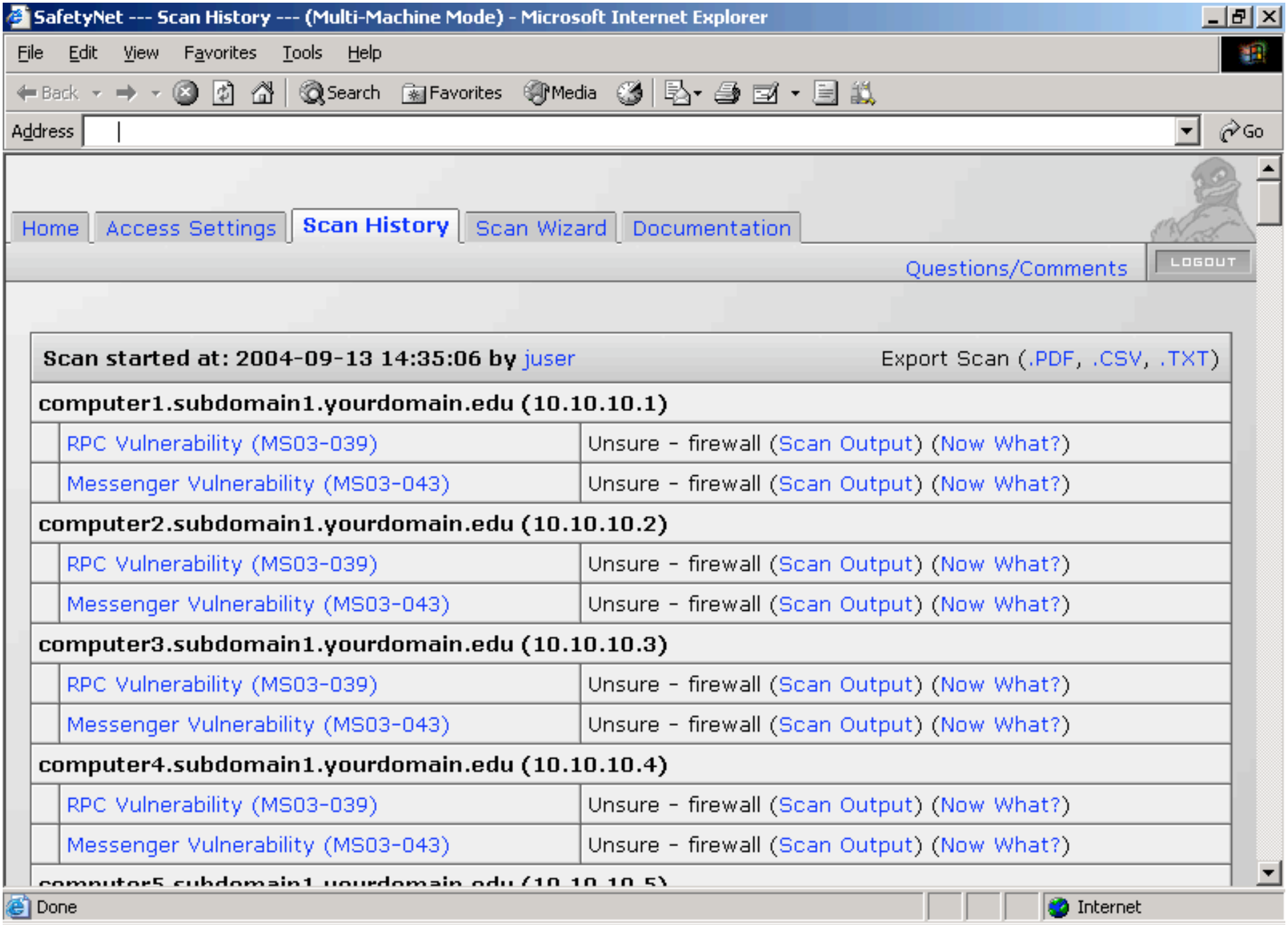
### Scan History
This section allows you to view the last 5 scans and error reports for the currently focused DNS zone(univsvcs.vt.edu). You can also export a scan history into a downloadable document (.PDF,.CSV,.TXT).

### Scan Wizard
This section is where you will setup the scans you would like to perform.

### Documentation
This section provides a more in-depth look at the function of each of the SafetyNet tabs. This section also explains each scanning module's functions, limitations, range of results, and recommended follow-up actions.

Version 1.0


SafetyNet --- Access Settings --- (Multi-Machine Mode) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Home
Access Settings
Scan History
Scan Wizard
Documentation
Questions/Comments
LOGOUT
Zone Information
Current Focus:
subdomain1.yourdomain.edu
Change Focus to:
subdomain2.yourdomain.edu
Change
Users who can grant access: User, Joe (YourDomain\juser)
User, Sam (YourDomain\suser)
Access has been granted to: User, Jane (YourDomain\userjane)
Access Control
Give Access to zone:
subdomain1.yourdomain.edu
Hokies\:
Add
Remove access to zone:
subdomain1.yourdomain.edu
userjane
Remove
Internet


SafetyNet --- Scan History --- (Multi-Machine Mode) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Home
Access Settings
Scan History
Scan Wizard
Documentation
Questions/Comments
LOGOUT
Scan started at: 2004-09-13 14:35:06 by juser
Export Scan (.PDF, .CSV, .TXT)
computer1.subdomain1.yourdomain.edu (10.10.10.1)
RPC Vulnerability (MS03-039)
Unsure - firewall (Scan Output) (Now What?)
Messenger Vulnerability (MS03-043)
Unsure - firewall (Scan Output) (Now What?)
computer2.subdomain1.yourdomain.edu (10.10.10.2)
RPC Vulnerability (MS03-039)
Unsure - firewall (Scan Output) (Now What?)
Messenger Vulnerability (MS03-043)
Unsure - firewall (Scan Output) (Now What?)
computer3.subdomain1.yourdomain.edu (10.10.10.3)
RPC Vulnerability (MS03-039)
Unsure - firewall (Scan Output) (Now What?)
Messenger Vulnerability (MS03-043)
Unsure - firewall (Scan Output) (Now What?)
computer4.subdomain1.yourdomain.edu (10.10.10.4)
RPC Vulnerability (MS03-039)
Unsure - firewall (Scan Output) (Now What?)
Messenger Vulnerability (MS03-043)
Unsure - firewall (Scan Output) (Now What?)
Done
Internet

Home | Access Settings | Scan History | Scan Wizard | **Documentation**

Questions/Comments | LOGOUT

## Documentation and Help

**Descriptions of Scans** - This article describes the scans that are offered on the SafetyNet website

**Limitations of SafetyNet** - This article explains the limitations of SafetyNet and how they might affect you as a systems administrator

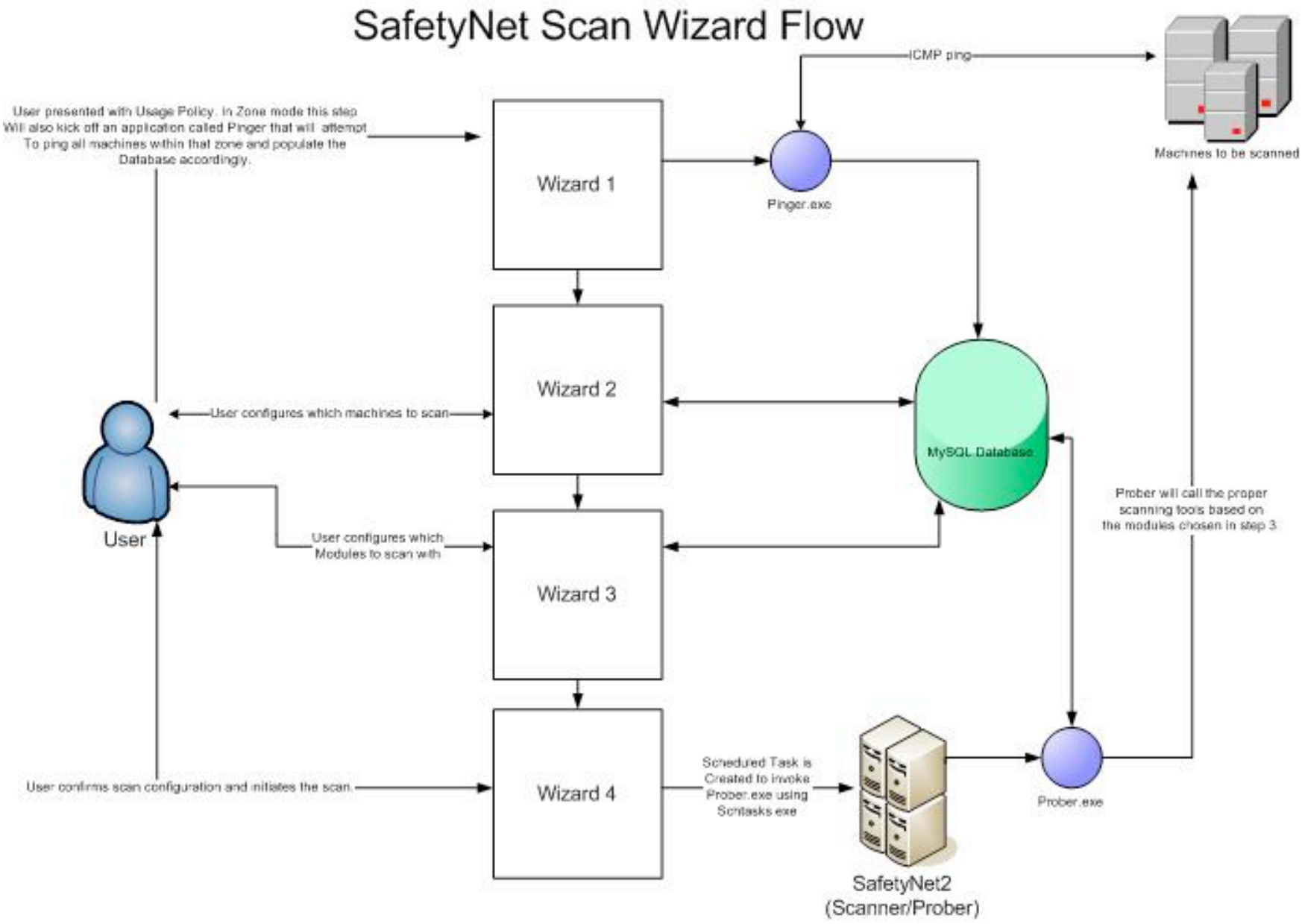
**Example Scan Results** - This article shows example results (including screen shots) produced by SafetyNet when scanning vulnerable machines.

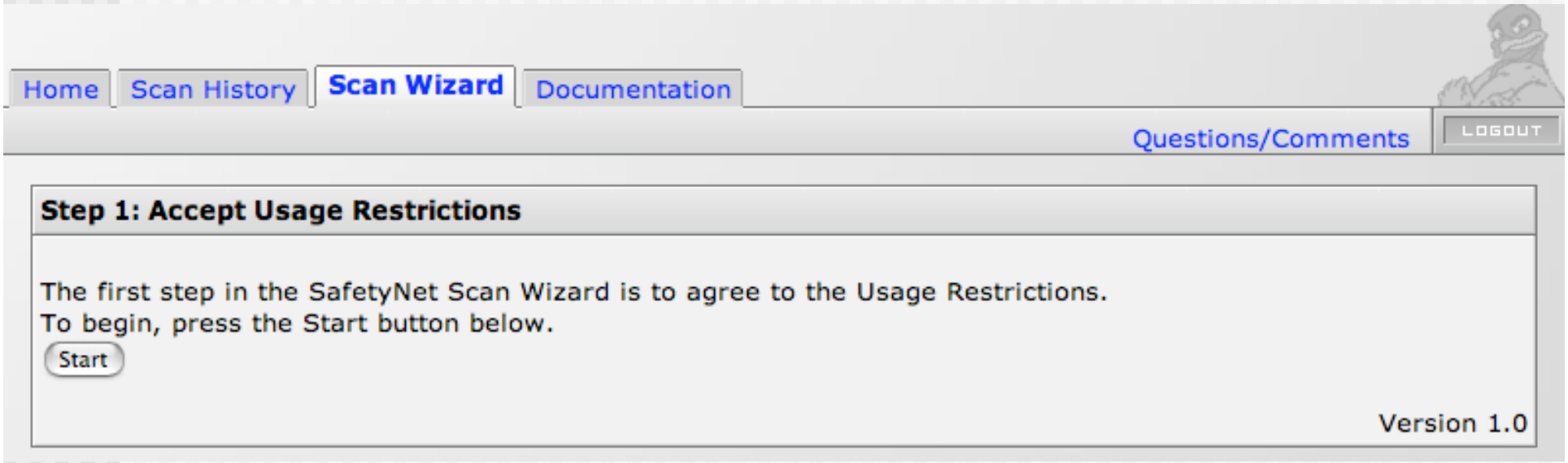
**Frequently Asked Questions (FAQ)** - Knowledge Base articles pertaining to SafetyNet that you may find useful

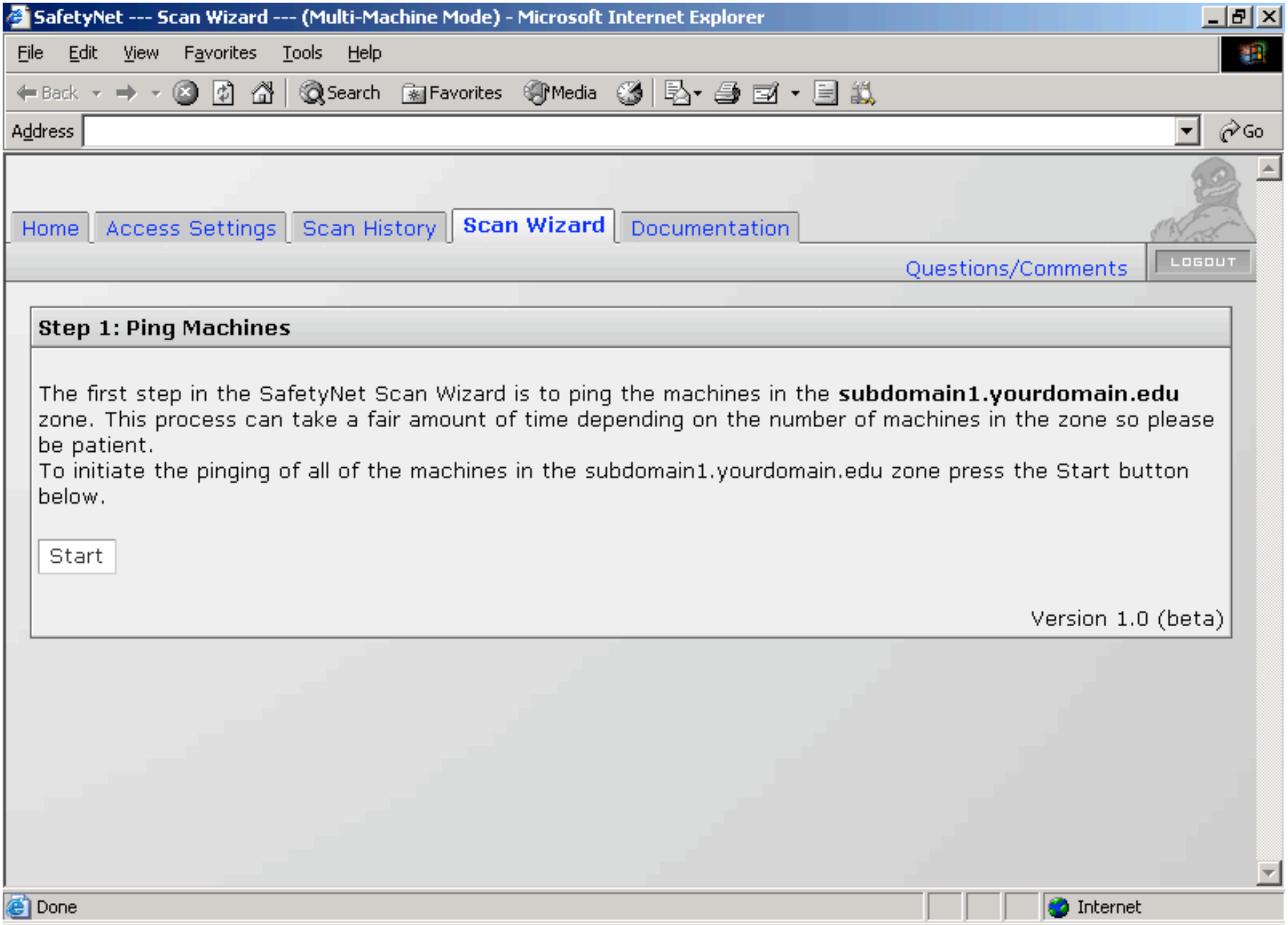
**Network Liaison List** - List of network liaisions maintained by CNS. Network liaisons responsible for a zone may scan all of the machines in that zone via SafetyNet.

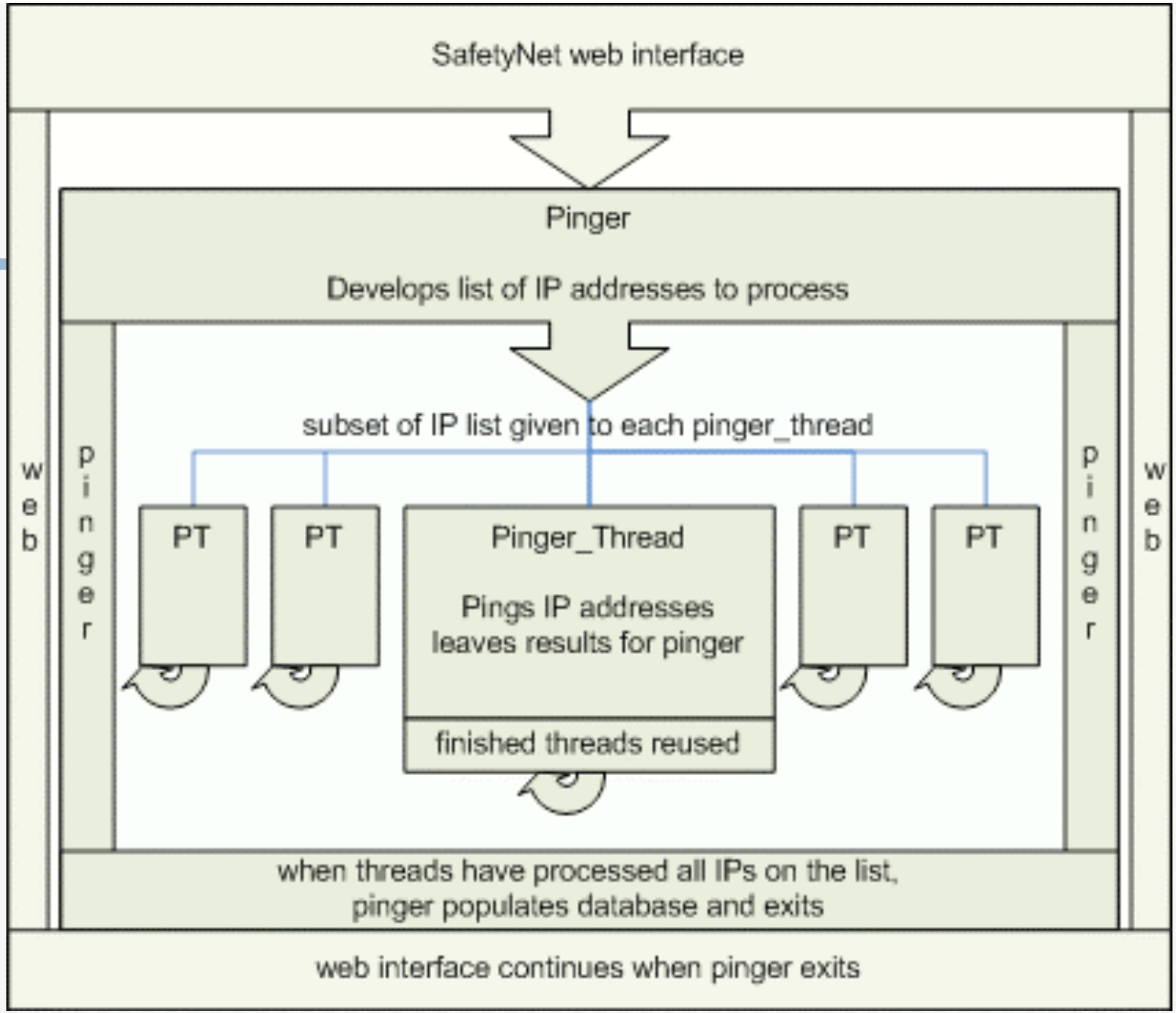
**Questions or Comments** - Send us your feedback about SafetyNet. Security related questions should be sent to 4help.

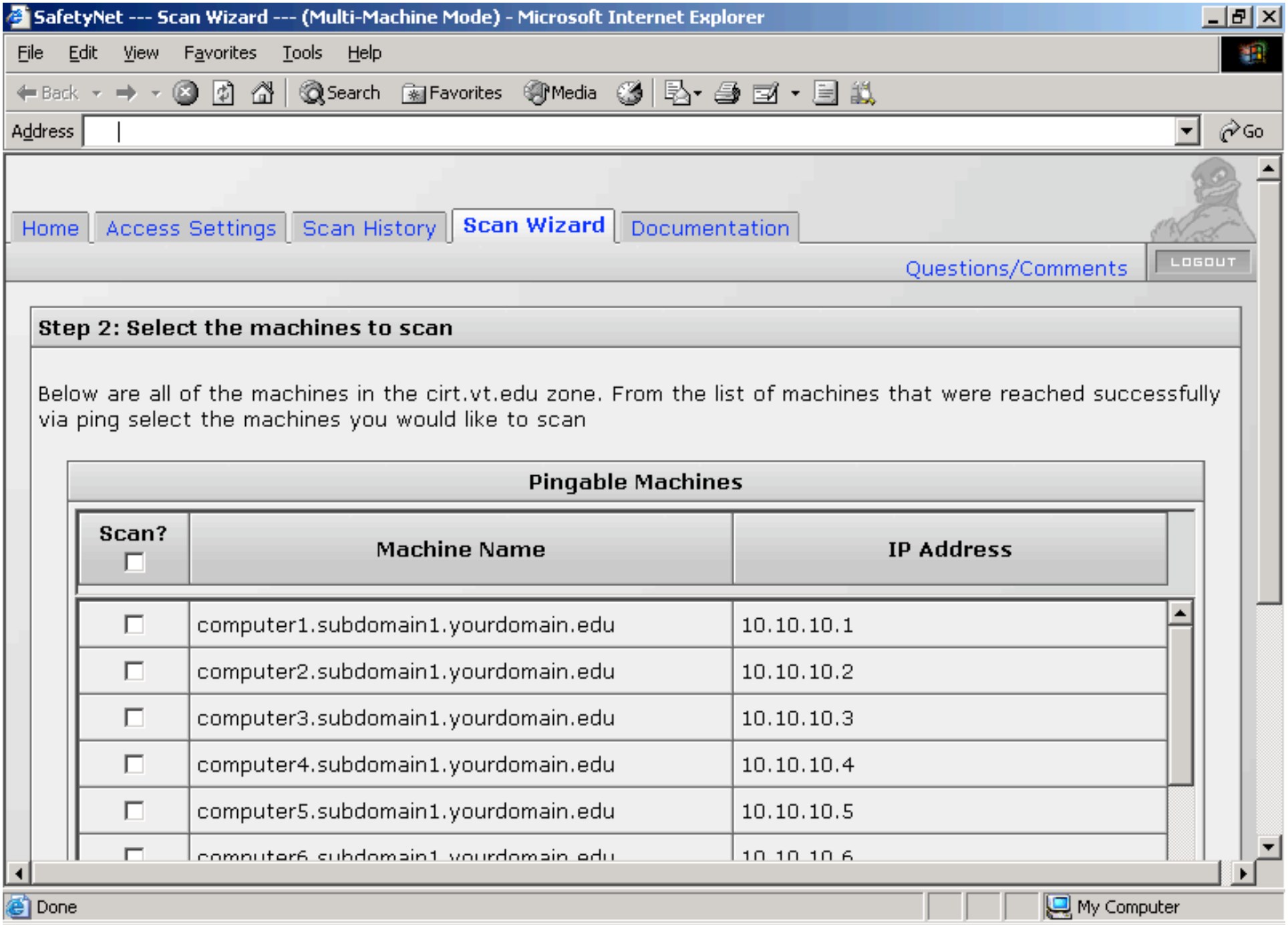
Version 1.0

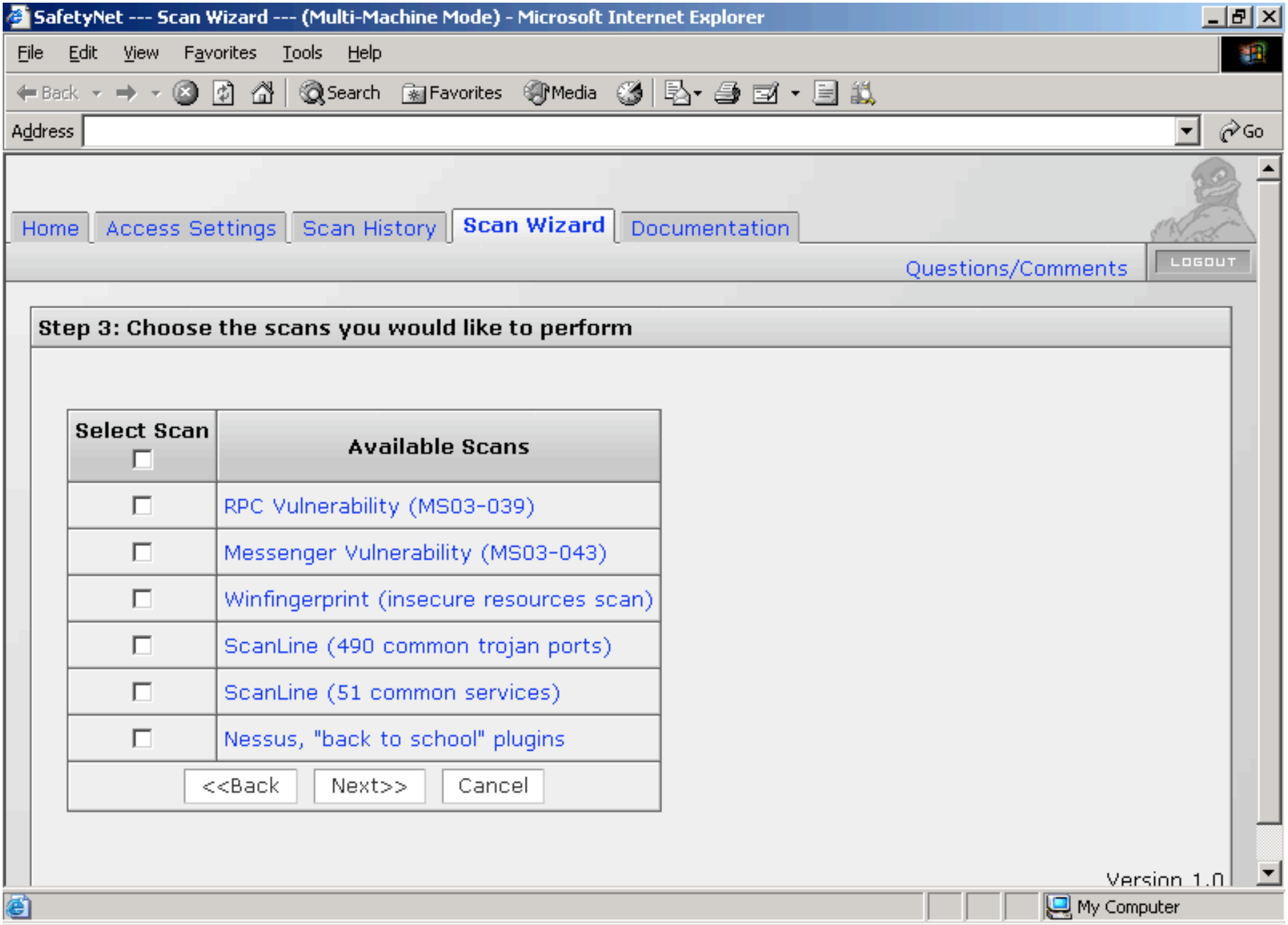

SafetyNet Scan Wizard Flow
ICMP ping
Machines to be scanned
User presented with Usage Policy. In Zone mode this step
Will also kick off an application called Pinger that will attempt
To ping all machines within that zone and populate the
Database accordingly.
Wizard 1
Pinger.exe
Wizard 2
MySQL Database
User configures which machines to scan
User
User configures which
Modules to scan with
Wizard 3
Prober will call the proper
scanning tools based on
the modules chosen in step 3
User confirms scan configuration and initiates the scan.
Wizard 4
Scheduled Task is
Created to invoke
Prober.exe using
Schtasks.exe
Prober.exe
SafetyNet2
(Scanner/Prober)

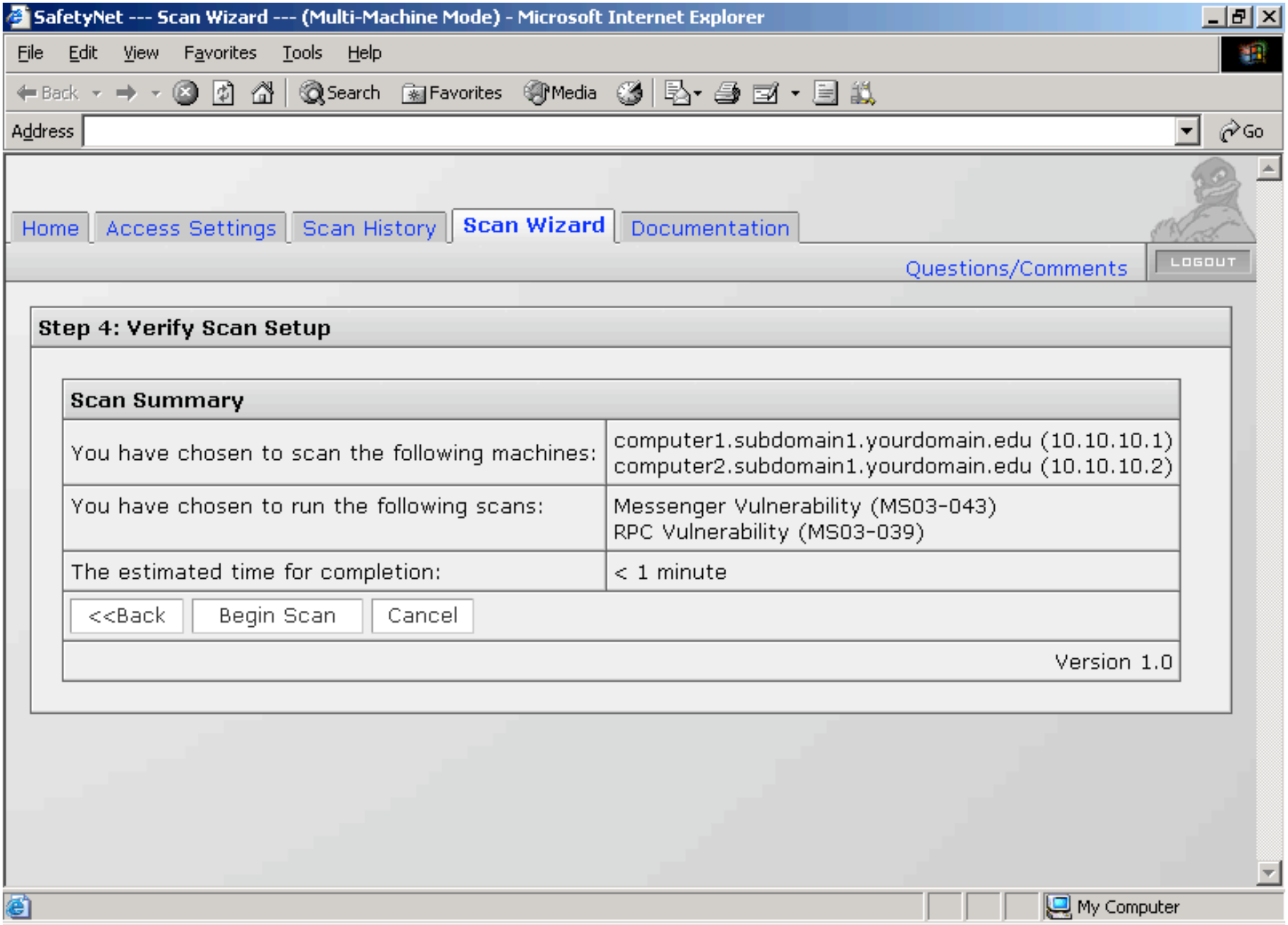

Home
Scan History
Scan Wizard
Documentation
Questions/Comments
LOGOUT
Step 1: Accept Usage Restrictions
The first step in the SafetyNet Scan Wizard is to agree to the Usage Restrictions.
To begin, press the Start button below.
Start
Version 1.0

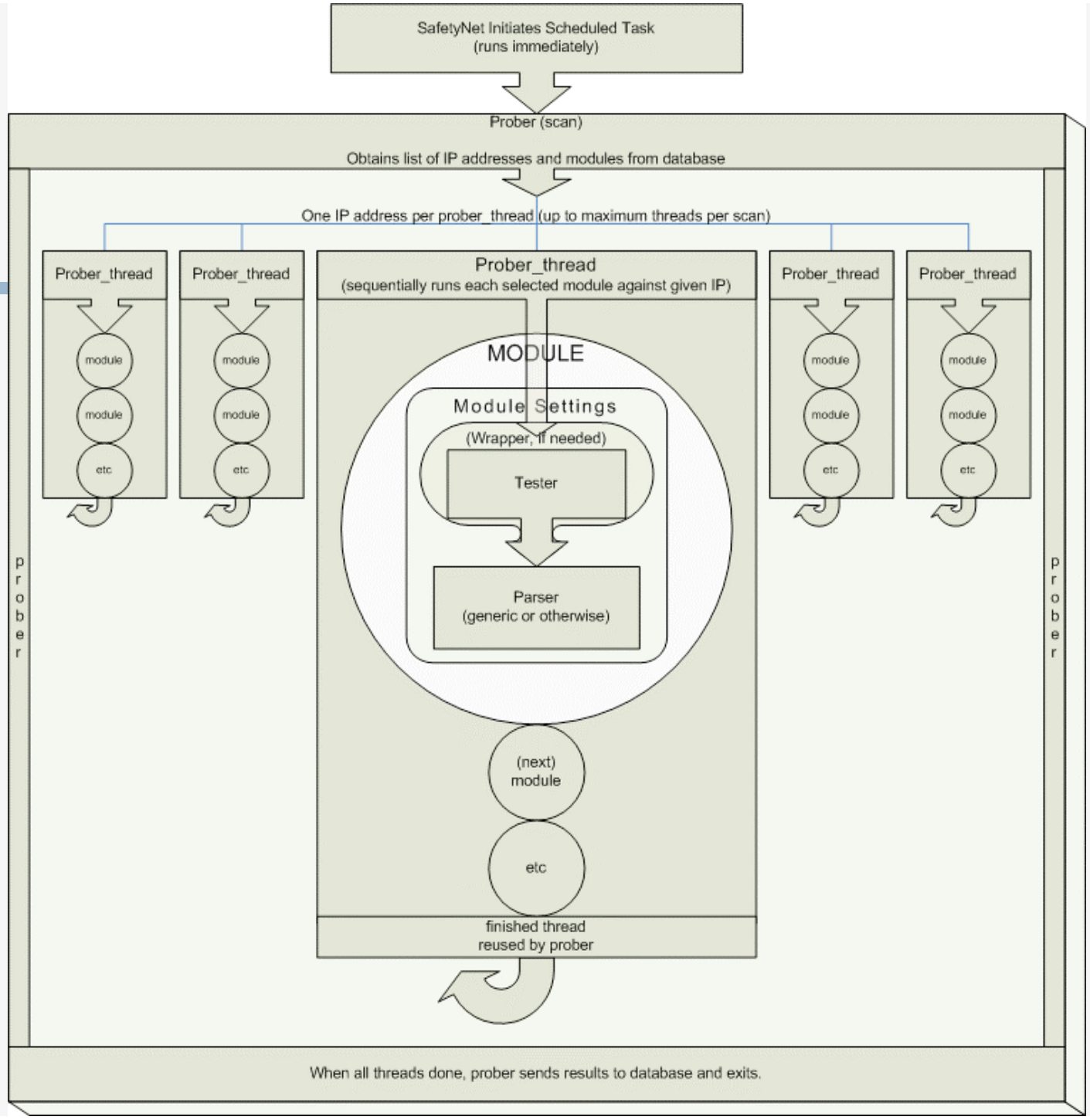

SafetyNet --- Scan Wizard --- (Multi-Machine Mode) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Home
Access Settings
Scan History
Scan Wizard
Documentation
Questions/Comments
LOGOUT
Step 1: Ping Machines
The first step in the SafetyNet Scan Wizard is to ping the machines in the subdomain1.yourdomain.edu zone. This process can take a fair amount of time depending on the number of machines in the zone so please be patient.
To initiate the pinging of all of the machines in the subdomain1.yourdomain.edu zone press the Start button below.
Start
Version 1.0 (beta)
Done
Internet

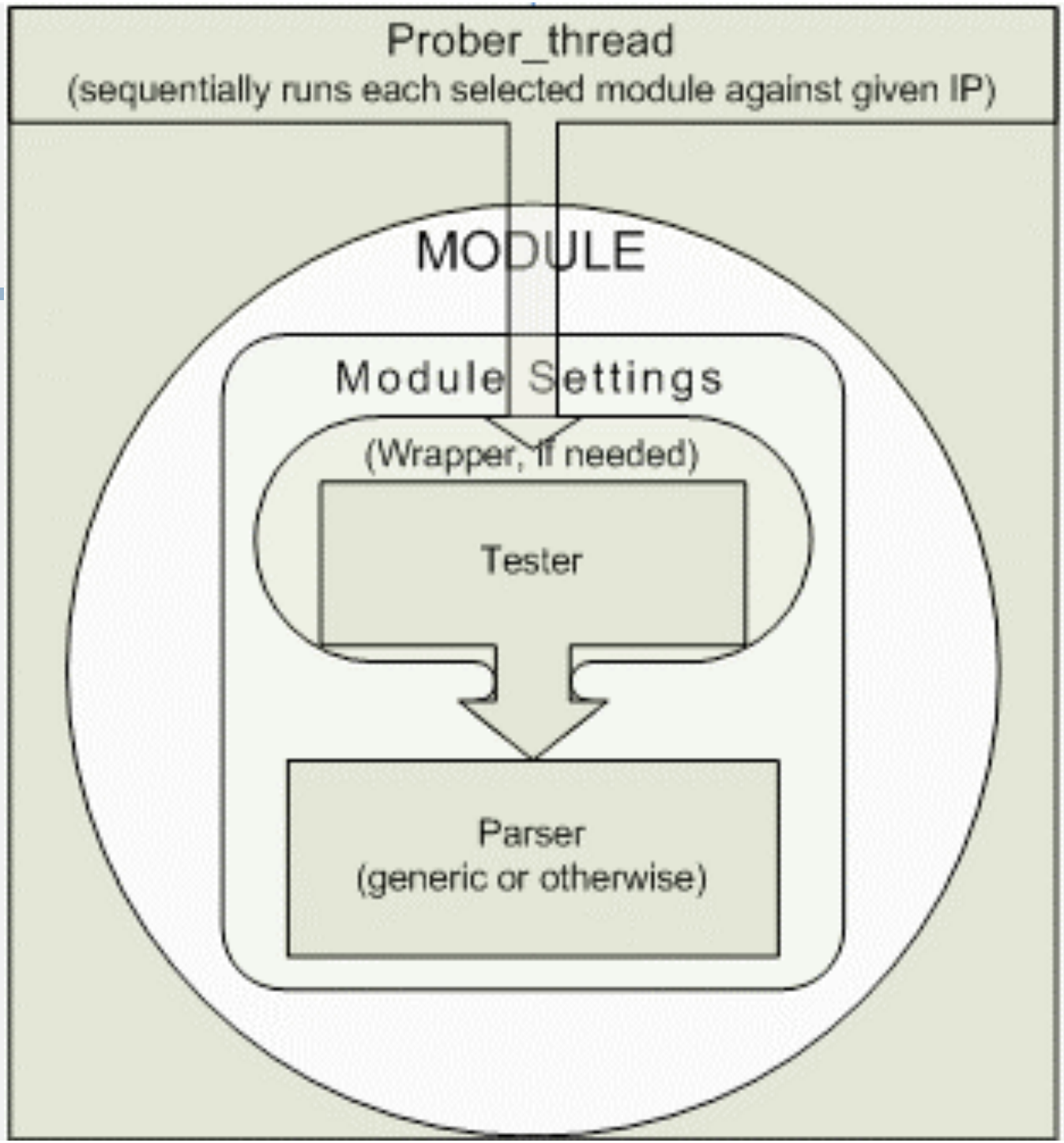

SafetyNet web interface
Pinger
Develops list of IP addresses to process
subset of IP list given to each pinger_thread
web
pinger
PT
PT
Pinger_Thread
Pings IP addresses
leaves results for pinger
PT
PT
finished threads reused
pinger
web
when threads have processed all IPs on the list,
pinger populates database and exits
web interface continues when pinger exits

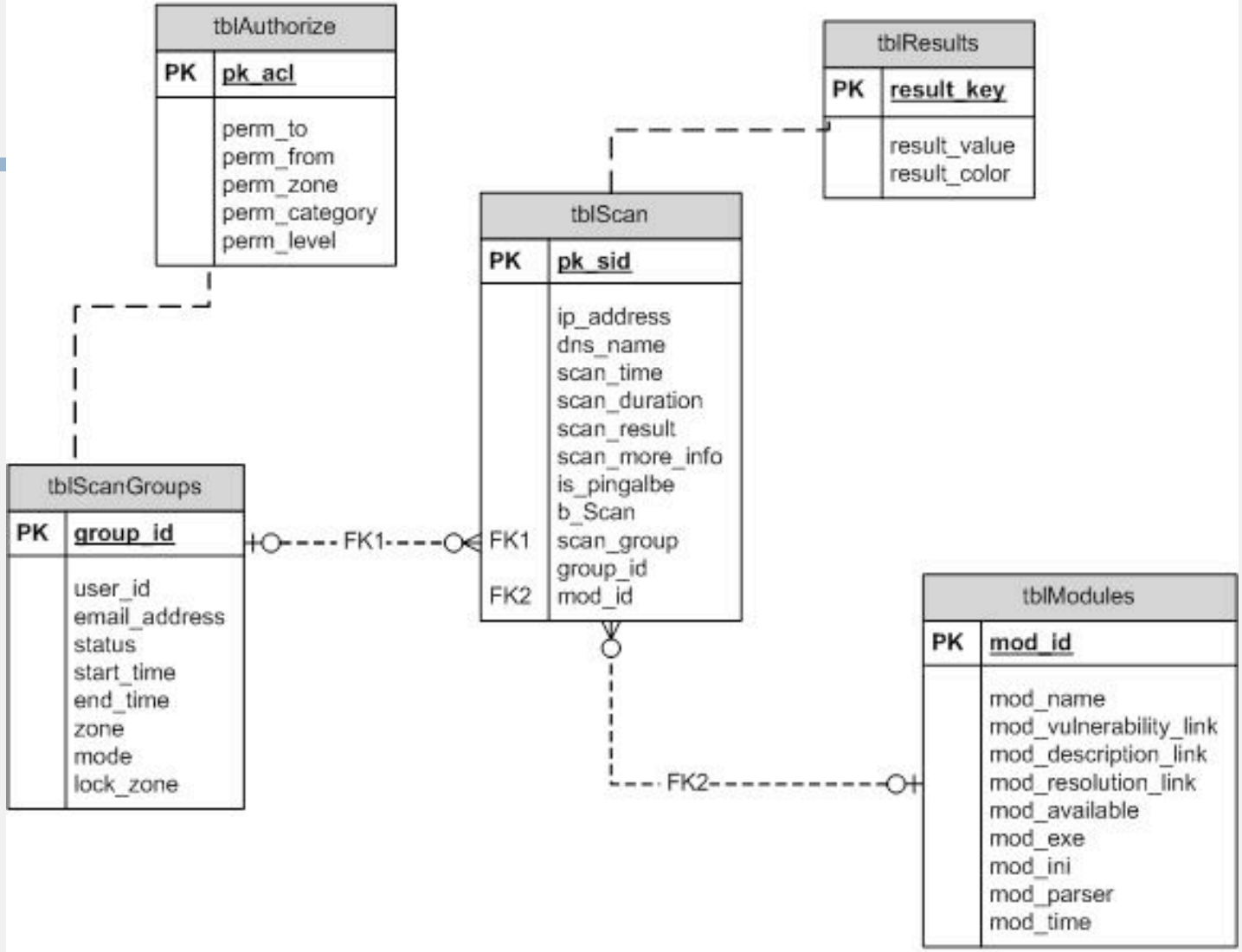

SafetyNet --- Scan Wizard --- (Multi-Machine Mode) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Home
Access Settings
Scan History
Scan Wizard
Documentation
Questions/Comments
LOGOUT
Step 2: Select the machines to scan
Below are all of the machines in the cirt.vt.edu zone. From the list of machines that were reached successfully via ping select the machines you would like to scan
Pingable Machines
Scan?
Machine Name
IP Address
computer1.subdomain1.yourdomain.edu
10.10.10.1
computer2.subdomain1.yourdomain.edu
10.10.10.2
computer3.subdomain1.yourdomain.edu
10.10.10.3
computer4.subdomain1.yourdomain.edu
10.10.10.4
computer5.subdomain1.yourdomain.edu
10.10.10.5
Done
My Computer


SafetyNet --- Scan Wizard --- (Multi-Machine Mode) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Home
Access Settings
Scan History
Scan Wizard
Documentation
Questions/Comments
LOGOUT
Step 3: Choose the scans you would like to perform
Select Scan
Available Scans
RPC Vulnerability (MS03-039)
Messenger Vulnerability (MS03-043)
Winfingerprint (insecure resources scan)
ScanLine (490 common trojan ports)
ScanLine (51 common services)
Nessus, "back to school" plugins
<<Back
Next>>
Cancel
Version 1.0
My Computer


SafetyNet --- Scan Wizard --- (Multi-Machine Mode) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Home
Access Settings
Scan History
Scan Wizard
Documentation
Questions/Comments
LOGOUT
Step 4: Verify Scan Setup
Scan Summary
You have chosen to scan the following machines:
computer1.subdomain1.yourdomain.edu (10.10.10.1)
computer2.subdomain1.yourdomain.edu (10.10.10.2)
You have chosen to run the following scans:
Messenger Vulnerability (MS03-043)
RPC Vulnerability (MS03-039)
The estimated time for completion:
< 1 minute
<<Back
Begin Scan
Cancel
Version 1.0
My Computer


SafetyNet Initiates Scheduled Task
(runs immediately)
Prober (scan)
Obtains list of IP addresses and modules from database
One IP address per prober_thread (up to maximum threads per scan)
Prober_thread
Prober_thread
Prober_thread
(sequentially runs each selected module against given IP)
Prober_thread
Prober_thread
module
module
etc
MODULE
Module Settings
(Wrapper, if needed)
Tester
Parser
(generic or otherwise)
(next)
module
etc
finished thread
reused by prober
prober
prober
When all threads done, prober sends results to database and exits.


Prober_thread
(sequentially runs each selected module against given IP)
MODULE
Module Settings
(Wrapper, if needed)
Tester
Parser
(generic or otherwise)


tblAuthorize
PK
pk_acl
perm_to
perm_from
perm_zone
perm_category
perm_level
tblResults
PK
result_key
result_value
result_color
tblScan
PK
pk_sid
ip_address
dns_name
scan_time
scan_duration
scan_result
scan_more_info
is_pingalbe
b_Scan
FK1
scan_group
group_id
FK2
mod_id
tblScanGroups
PK
group_id
user_id
email_address
status
start_time
end_time
zone
mode
lock_zone
FK1
tblModules
PK
mod_id
mod_name
mod_vulnerability_link
mod_description_link
mod_resolution_link
mod_available
mod_exe
mod_ini
mod_parser
mod_time
FK2

# Development

- Once a scan is initiated
  - Notice is given that an email will be sent to the initiator of the scan when the scan is completed
- Locking
  - In Single Mode a user can only have one machine being scanned at a time
  - In Zone Mode a zone can only have one scan being run on it at a time

# Development

- Modules / Utilities
  - 01 - RPC Vulnerability (MS03-039)
    - Written by ISS - worked well
  - 02 - Messenger Vulnerability (MS03-043)
    - Written by ISS - worked well
  - 03 - SQL Slammer (MS02-039) - NR
    - Written by ISS - never seemed to work properly
  - 04 - ScanLine (8 trojan ports)
    - Written by Foundstone - worked ok, had some issues
  - 05 - GNIT (multiple services) - NR
    - Written by Glitch of ellicit.org
    - Would occasional hang or give conflicting results

# Development

- Modules
  - 06 - GFI LANGuard (alerts) - NR
    - Freeware version 3.3 from GFI
    - Unstable at large loads, fail or lockup
  - 07 - Winfingerprint (insecure resources)
    - Written by Kirby Kuehl
    - Cli would lockup on disabled netbios systems
    - Had to use the -ad switch with reduced info
  - 08 - 11 - Scanline (with different options/ports)
  - 12 - Nmap (informational) - NR
    - Written by Fyodor, tested version 3.50
    - Required WinPcap v3.0, bad interaction with driver caused crashes and reboots of the system

# Development

- Modules
  - 13 - Winfingerprint (insecure resource scan) - NR
    - Without the -ad switch its unstable
  - 14 - ScanLine (common services)
  - 15 - Winfingerprint - NR
    - Used in place of Nmap - not enough info
  - 16 - Newt (all safe scans) - NR
    - Written by Tenable Network Security - version 2.0
    - Product in such a way as to not allow test wrapper
    - Unstable under large loads, lack of pre-sales support

# Development

- Modules
  - 17 - LANguard v5.0 - NR
    - Written by GFI
    - Still unstable under large loads
  - 18 -19 - Nessus (“back to school plugins”)
    - Used Windows client v2.0.12 and Cygwin v1.5.10
    - Cygwin libraries may cause a thread forking issue which causes very slow response to/from Nessus server
    - Used Linux NST distro v1.0.5 for Nessus server testing

# Development

- Utility requirements for inclusion in modules:
  - Must be able to be invoked by another exe
  - Multiple copies must be able to be run at the same time
  - Accept input in the form of switches
  - Stay running until test is finished, never stop for user input and then must actually exit when finished
  - Provide computer parsable output
  - Output must be uniquely identifiable from other output of other running threads
  - Output must be displayable to the user

# Development

- Programming a module
  - Find a utility the meets the requirements
  - Create a row in the DB table “tblModules”
  - Program module’s INI file
    - Module settings
    - Parsing settings
    - Prober settings
  - Test module
    - “Out-of-loop” testing
    - Administrator preview mode
  - Resolve errors
  - Extensive documentation available for this process

# Development

- Running and maintenance
  - Database care and feeding
  - Module runtimes and module_time_avg
  - Backend OS patching, etc
  - Module cleanup/updating
  - Nessus special concerns
    - Updating plugins
    - Plugin set is assumed inclusive
    - Default inclusion state of EVERY plugin is YES!
    - Unix related issues / uptime for module

# Development

- Q&A?

# Production

- Timeline
  - Incident – July 16th, 2003
  - PRF – Sep 9th, 2003
  - Req doc – Jan 27th, 2004
  - Sponsorship – March 3rd, 2004
  - Development – April thru July 2004 (~ 3 mth)
  - Open beta – July thru Sep (~3 mth)
  - Production – Sep forward

# Production

- Closed alpha during development
  - Sponsors
  - MIG
  - Testing group (2 people)
- Open beta during testing
  - Open to CIT/DIT
  - Restricted to F/S

# Production

- Statistics (since July 6th, 2004)
  - 1337 Successful logins
  - 757 total scans initiated
    - 641 were individual
    - 116 zones
      - Two zones scanned over 30+ times
  - 1646 machines scanned
    - 1142 failed at least one module test
  - Most frequent users are our Internal Audit staff!

# Production

- Open Source downloads
  - SafetyNet package has been downloaded over 490 times since its release
  - Second most popular download item from our download site

# Production

- Q&A?

# Post mortem

- Awkward delineation of support
  - Sponsors maintain application
  - Systems Administration group maintains hardware and OS
  - Support of system restricted to 8-5 M-F
- Application changes sponsor initiated?
  - Change authentication to include students
  - New modules
    - MBSA
    - MetaSploit framework
    - MS tools discontinued…

# Post mortem

- Lack of separate concurrent development environment hinders flexibility
- MS Windows 2003 Web Edition Server not the appropriate environment for hosting
- Difficult finding free and unrestricted use modules from “reputable” sources that meet module requirements
- Would re-write system without using proprietary WinBatch language
- Requirement for external Nessus server is a key dependency

- Most difficult component is developing the remediation KBs for vulnerable/exploited systems

# Post mortem

- SafetyNet is powerful web-based framework for harnessing your vulnerability and exploit testing code
- Designed to be stable and scalable to large numbers of target systems
- Provides historical and metrics base data for auditable analysis
- Allows for individuals and departmental IT to provide self-auditing and reporting
- Provides your security group with another arrow in the vulnerability assessment and remediation quiver

# Post mortem

- Q&A?

# Resources

- http://opensource.w2k.vt.edu
- http://vtmig.w2k.vt.edu
- http://www.w2k.vt.edu
- http://www.windowware.com