Overview

- Introductions
- Linux Usage at Tenable
- Linux Usage in our Products
- Linux Usage at our Customers
- Horror Stories !!!!
- Discussion – Linux Appliances
- Discussion – VMWARE and Linux
- Discussion – Linux/RedHat/SuSE

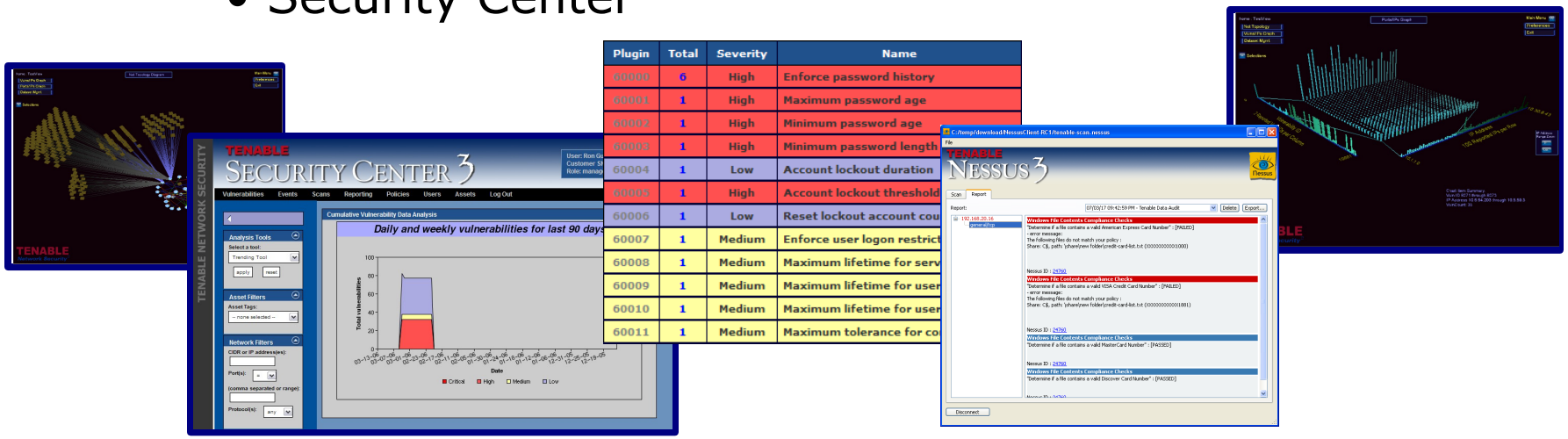
Introduction

- Ron Gula
  - CTO/CEO and Co-Founder of Tenable
  - Founder of Network Security Wizards which made the Dragon Intrusion Detection System
  - Director of Risk Mitigation at USi
  - Consultant, pen-tester & security researcher for GTE, BBN and NSA
  - Captain in USAF

Introduction

The goal of this talk is to provide you a brief glimpse into how Linux is used by Tenable and our customers.

- Tenable Network Security
  - Security and Compliance Monitoring products
    - Nessus Vulnerability Scanner
    - Passive Vulnerability Scanner
    - Log Correlation Engine
    - Security Center



Linux Usage at Tenable

- Typical "office" Stuff
  - 50 employees
  - VPNs, IP phones, .etc
  - Most employees use Windows as desktop
- Most Critical "office" Applications
  - Hosted on Linux
  - Outsourced
  - Some on Windows 2003 and OS X

Linux Usage at Tenable

- Atypical Office stuff
  - Need to build Nessus for 8+ platforms
    - Fedora 5/6, Red Hat ES3/ES4, SuSE 9/10, Debian 3.1
    - FreeBSD 5/6
    - Solaris 9/10
    - Mac OS X 10.4
    - Windows 2000, 2003 and XP
  - Need to maintain "target farm" for security research
    - Patch auditing for 10+ platforms
    - Wide variety of common applications and stuff you've never heard of

Linux Usage at Tenable

- VMWare
  - Extensively Used
    - Developers run VMs on desktops
    - Some main servers run on VMs
  - Running VMware on top of Windows
    - Better performance for VMs
    - Potentially better integration with our SAN solution
  - Linux usage
    - Pristine build targets for Fedora, ES, Debian, .etc
    - Development environments
    - QA environments
  - Evaluating ESX

Linux Usage at Tenable

- Dedicated Linux Systems (Non VMs)
  - Disk intensive applications
    - Log Correlation Engine performance
    - Passive Vulnerability Scanner Gigabit performance
  - Native OS testing
    - Using System Commander to natively boot several different OSes

Linux Usage in our Products

- Current Shipping Versions
  - Security Center – RH ES3/4
  - Log Correlation Engine – RH ES3/4
    - Linux agents for RH ES3/4 and Fedora
  - Passive Vulnerability Scanner – RH ES3/4
  - Nessus – RH ES3/4, Debian, SuSE, Fedora

Linux Usage in our Products

- Audited Forms of Linux
  - Patch audits for …
    - RH ES3/4; Fedora; Debian; CentOS; Gentoo; Mandrake; Slackware; Ubuntu
  - Vulnerability Scans for …
    - Common "LAMP" services
    - Stuff you've never heard of ("Joe's PHP Bulletin Board")
    - Basically everything that runs on Linux
  - TCP/IP Fingerprinting
    - Active scans for Linux
    - Passive (sniffing) scans for Linux

Linux Usage in our Products

- Supported Logging Sources
  - OS level Syslog events
    - Adding users
    - Placing NICs into promiscuous mode
    - Logs from SE Linux
  - Application logs
    - ipfilter; SSH; Apache; My SQL; Snort; .etc
  - Direct Network Monitoring
    - Sniffing network sessions through ***libpcap***
    - Obtaining network "flows" with netflow

Linux Usage in our Products

- Security Center applications
  - Embed Apache and PHP
  - Not using MySQL (or any other DB)
    - Very common question we get from our customers
    - SQL generally used for record locking while we tend to just shove data in there all the time
  - Using SSH
    - Public/private keys used to run "rsh" style commands between the Security Center and Log Correlation Engine
  - Distributed as an RPM
  - Managed with "rc" scripts

Linux Usage at our Customers

- Several different environments
  - Linux generally accepted and supported
    - Which OS? (Usually RedHat, but have run into SuSE)
  - Windows is the official OS
    - Need waivers or the illusion of an appliance
  - VMWare leveraged environment
  - Sometimes the underlying OS is maintained by the IT group and the security group runs our products as an application
  - Occasional oddities
    - "We base all of our builds on Fedora Core 2" – 2007 quote
    - "We hand build our servers with Gentoo"

Linux Usage at our Customers

- Variety of Linux experience
  - Some organizations have multiple RHCEs
  - Most organizations have a core of Linux people, but doing things like installing an RPM is beyond anyone except those in the core
  - We've had situations where our entire product line was purchased by one person who had Linux expertise, but then got promoted and the new guy was a pure Windows guy

Linux Usage at our Customers

- Enterprise OS Detection
  - One of the cool things you can do with our product is to detect what is on your network
  - Detecting un-authorized copies of certain OSes (including Linux) is a very popular feature
    - i.e. The researcher who boots up an unhardened copy of Fedora

Horror Stories

- Security Center Debug Script
  - Support conversation
    - Customer: “Your product isn’t working.”
    - Support: “Can you send us your debug?”
    - Customer: “Here you go!”
  - What have we seen:
    - Unhardened boxes
    - Un-patched boxes
    - The wrong OS
    - Competitor’s products running along side ours
    - Attempts to void our licensing

Horror Stories

- Linux Anti-Virus
  - Several leading AV solutions for Linux seem to really prevent our products from working
    - Scanners can't scan – duh!
    - Sniffers can't sniff – duh!
    - Things that write Gigabytes of data to the disk get throttled too
    - Also impacts installation and upgrades

Horror Stories

- Lack of Linux experience
  - Not to uncommon support call
  - Customer: "I need help with the upgrade"
  - Support: "You need to run rpm –Uvh"
  - Customer types "rpm dashudh"
  - Variations of this theme
  - Webex and GotoMeeting are very useful in these cases

Horror Stories

- Lack of understanding of concepts such as GPL, Open Source, Free, .etc
  - Have had customers remove scripts from our products and use them for other applications
  - Still have customers request source code from us for commercial products
    - I love this one because I always ask if we can get the changes to the code and the answer always is that the "lawyers" claim that any code written by that organization is their own intellectual property
  - Routinely have some anti-open-source purchasing groups and legal groups rake Tenable over the coals

Discussion – Linux Appliances

- Demand for an "instant on" version of the product
- Would like to avoid SSH access or even the need to provision IP addresses
- Some customers still want to be able to "get in there" and "run MySQL" or "harden it with my own kernel"

Discussion – Linux and VMWare

- VMWare is VERY popular
- We have performance concerns with
  - CPU power
  - Disk I/O bandwidth
  - Memory usage
- We have licensing concerns
  - Very easy to copy fully licensed images around
- Starting to get requests for non-VMWare
  - Xen; Parrellels

Discussion – RedHat vs. SuSE

- Have only run into one real large customer who standardized their UNIXes on SuSE
- RedHat seems to be the "normal exception"
- Have not seen any increase in adoption of SuSE in the US; Europe uses SuSE a lot though
- Most enterprises still running Solaris for mission critical stuff
- OS X is still on the rise

Conclusion/Questions

- Thanks for your attention!
- Please feel free to email me at
  - rgula AT tenablesecurity.com