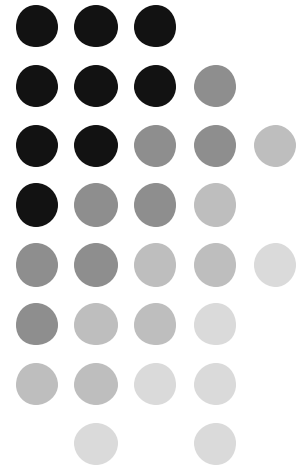


Vulnerability Assessment Using Nessus

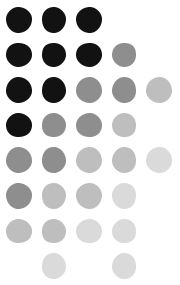


Paul Asadoorian, GCIA, GCIH
Network Security Engineer
Brown University

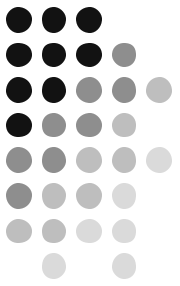
Paul_Asadoorian@brown.edu



Overview

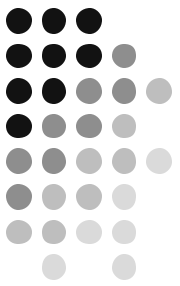


- Introduction to Nessus
- Nessus Architecture
- Nessus in Action
- Scanning Methodologies
- Reporting
- Challenges



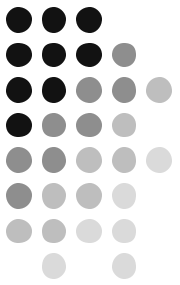
Nessus

- A “Free, Powerful, up-to-date, easy to use, remote security scanner”
- Open-Source, free to use, modify, etc..
- Vulnerability definitions, called plugins, are free as well
- Easy is a matter of perspective



Nessus - Features

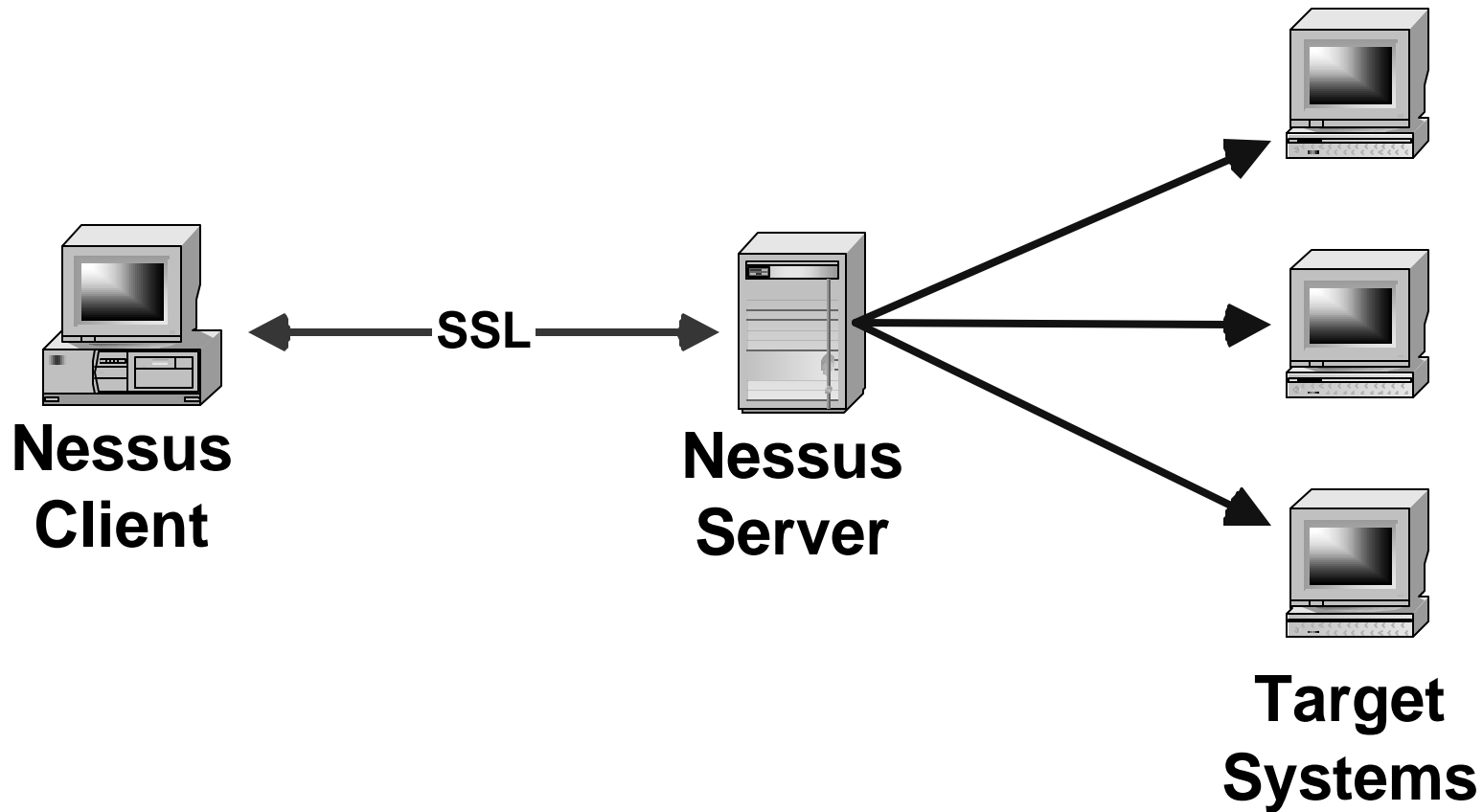
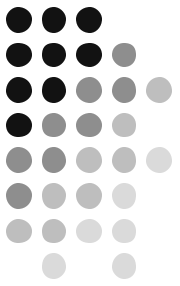
- Plugins – uses its own scripting language (NASL) to define how it tests for vulnerabilities
- Client/Server architecture – Client and server can be anywhere on the network
- Protocol aware – i.e. It will detect FTP running on port 31337
- Application Aware – Tests web servers running on the same port

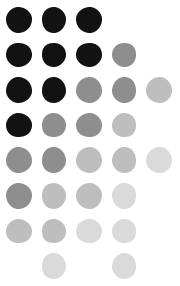


Nessus – Features

- Intelligent scanning – Anonymous FTP
- Reports provide vulnerability listings and a good number of resolutions
- Client/Server uses SSL to protect report results
- Much better about not crashing targets!

Nessus - Architecture

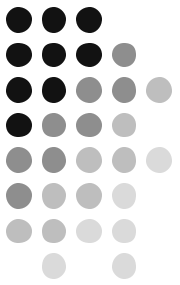




Nessus Client

- Native Unix GTK Client (Linux, Solaris, and others)
- Windows Client (NessusWX)
- Windows Client is preferred, more report options, better interface


Nessus Client - Unix




Nessus Setup

Nessusd host | Plugins | Prefs. | Scan options | Target selection | User | KB | Credits

New session setup

 Nessusd Host : localhost

Port : 1241

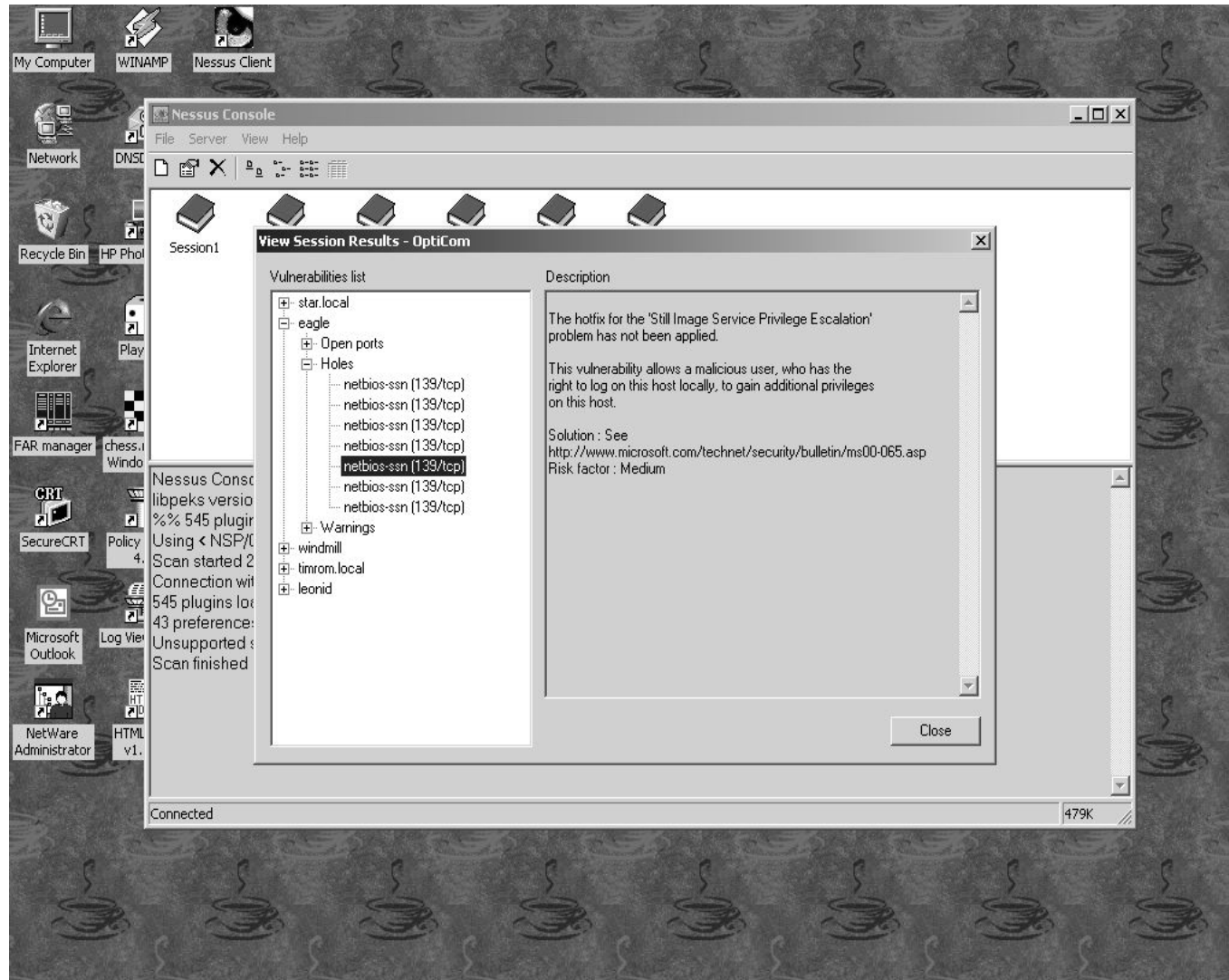
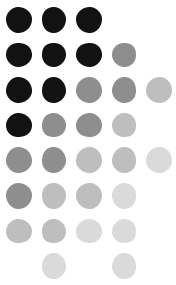
 Login : renaud

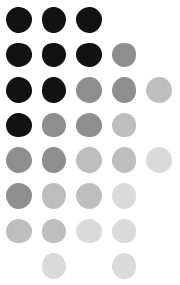
Password : ***

Log in

Start the scan | Load report | Quit

Nessus Client - Windows

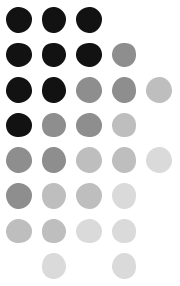




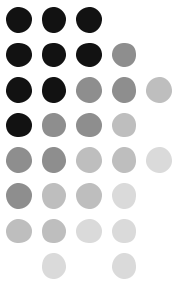
Nessus Server

- Runs on most Unix flavors (Unix, Linux, *BSD)
 - I find it runs best on Linux, your mileage may vary
- Performs all scanning functions, sends results back to client
- Includes a plugin update facility

Nessus Example



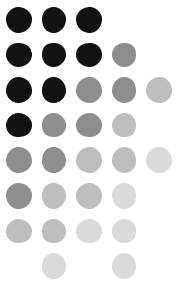
- Creating a Nessus Session
- Performing a scan
- Analyzing the results



Nessus Reports

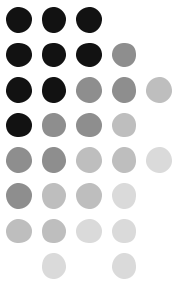
- Numerous different formats
- Problem – How to get the reports to the user securely
- Answers include:
 - Commercial Products
 - Write your own Perl or PHP application

Commercial Nessus



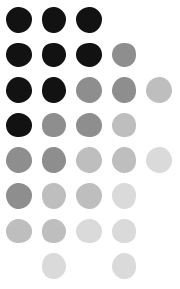
- <http://www.tenablesecurity.com/> - Complete Nessus Systems
- Renaud Deraison - Director of Research
- Ron Gula - Chief Technology Officer
- Nessus Consoles, Proxies, and Appliances

Do-It-Yourself Nessus



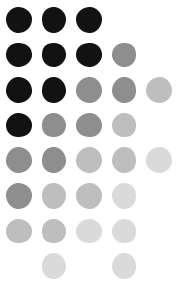
- Scan results are posted to a database server
- Web server displays reports, reading from the database server
- Accounts are created for users so they can only see their reports

Scanning Methodologies



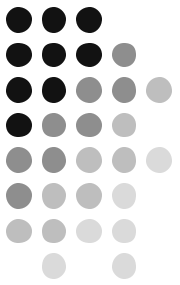
- Someone scans your system(s) and makes the report available to you
- The end user requests a scan directly from the server, the machine is scanned, and report is sent automatically
- When the user connects to the network the system is scanned automatically (Popular with wireless and VPN)

Scanning Methodologies



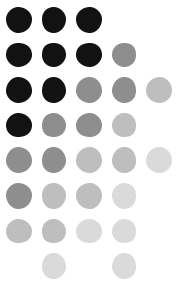
- Servers are scanned on a regular basis (maybe weekly) and results are compared
- Network Perimeter is scanned on a regular basis
- Which ones should I do?

Challenges – False Positives



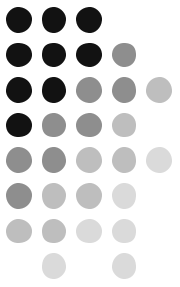
- Must verify to some degree the vulnerabilities Nessus has found
- This is time consuming and sometimes quite difficult
- Nessus is getting better, but still a ways to go

Challenges – Crash and Burn



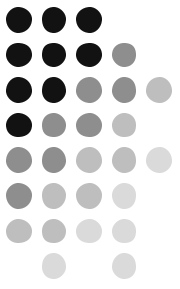
- Nessus will crash systems, routers, firewalls, and any other devices on the network!
- Happens no matter how careful you are
- Monitor your configuration closely, test new plugins first
- Prepare for the worst

Challenges – What about the application?



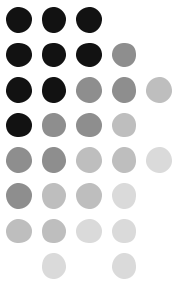
- Nessus does some application level vulnerability assessment
- Tools from SPI Dynamics, EEye, and ISS are better
- Make sure you have at least one other tool to test the application!

Challenges – Scan What? When?



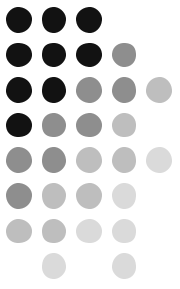
- Getting permission to scan is half the battle
- There is no guarantee that it will not crash the system
- As you know, people don't like it when you find things wrong with their systems

Challenges – How long will it take?

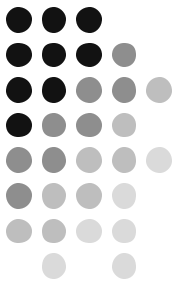


- Depends!
 - Number of hosts
 - Number of open ports
 - Number of services running on those ports
 - What kind of host (Windows, Unix, Mac)
 - How many hosts have firewalls
 - Speed of the network
 - Other network traffic
 - How many vulnerabilities are found
 - If the host crashes after the first plugin or just before the last

Challenges – How long does it usually take?



- One host = A morning or afternoon
- More than one host = 1 Day
- Entire Class C subnet = 2-3 Days
- Entire Class B = Weeks



Conclusion

- Questions?
- Email: Paul_Asadoorian@brown.edu
- Nessus Web Site:
<http://www.nessus.org>
- Presentation:
<http://pauldotcom.com/presentations.htm>