A Graph-Theoretic Visualization Approach To Network Risk Analysis

Kenneth Prole
Scott O'Hare, Ph.D.
Applied Visions, Inc., Secure Decisions division

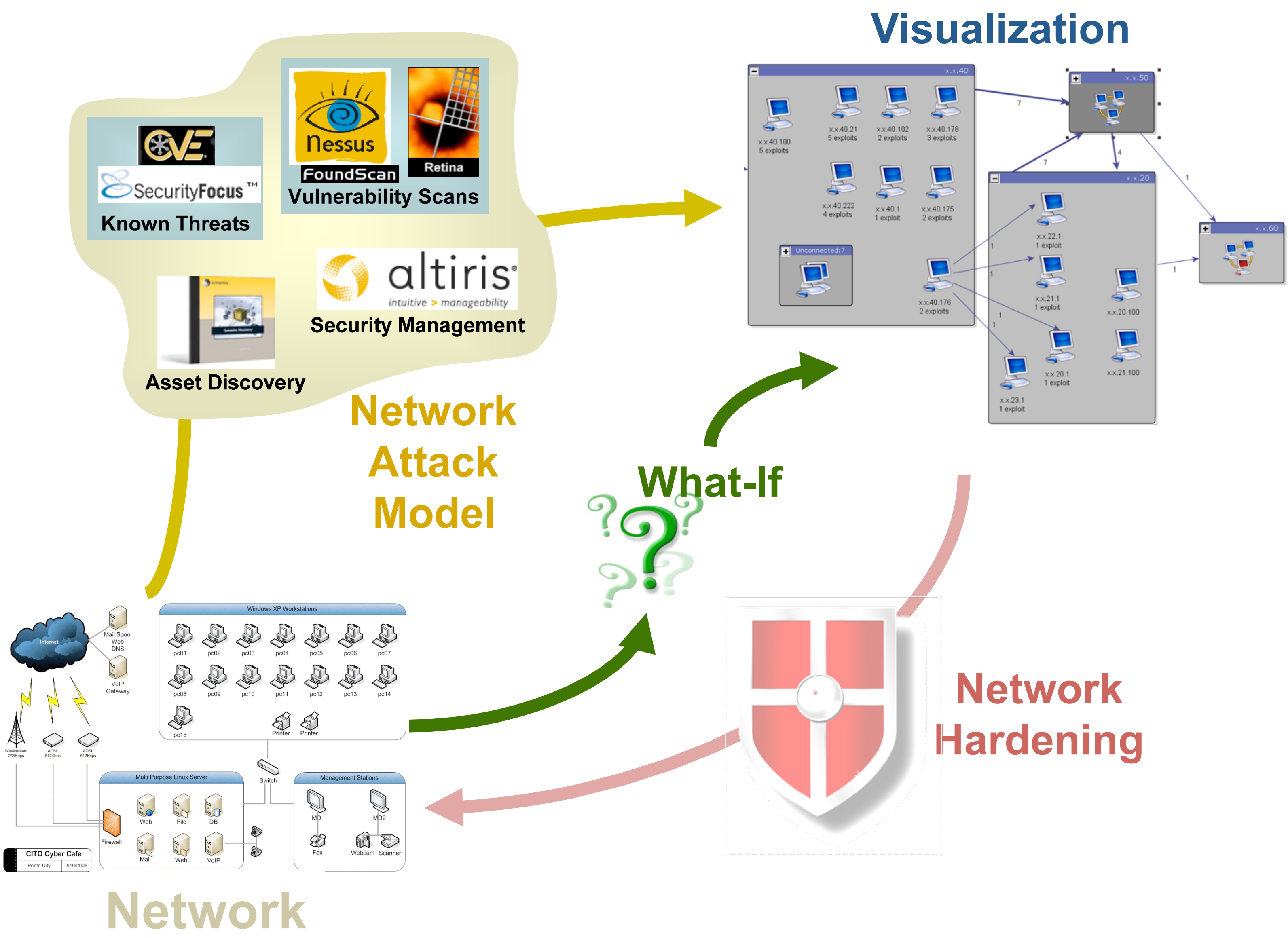
Steven Noel, Ph.D.
Center for Secure Information Systems
George Mason University

VizSec 2008
MIT - Cambridge, MA
September 15, 2008

Introduction

- Topological Vulnerability Analysis (TVA) attack graph technology
  - Builds comprehensive input model from network scans and database of potential attacker exploits
  - Analyzes vulnerability dependencies and models attack paths into a network
  - Discovers attack paths that convey the impact of individual and combined vulnerabilities on overall security
- New visualization approach
  - Dynamic interlinked views with high-level overview and detail drilldown

Architecture



Visualization

Known Threats

Vulnerability Scans

Security Management

Asset Discovery

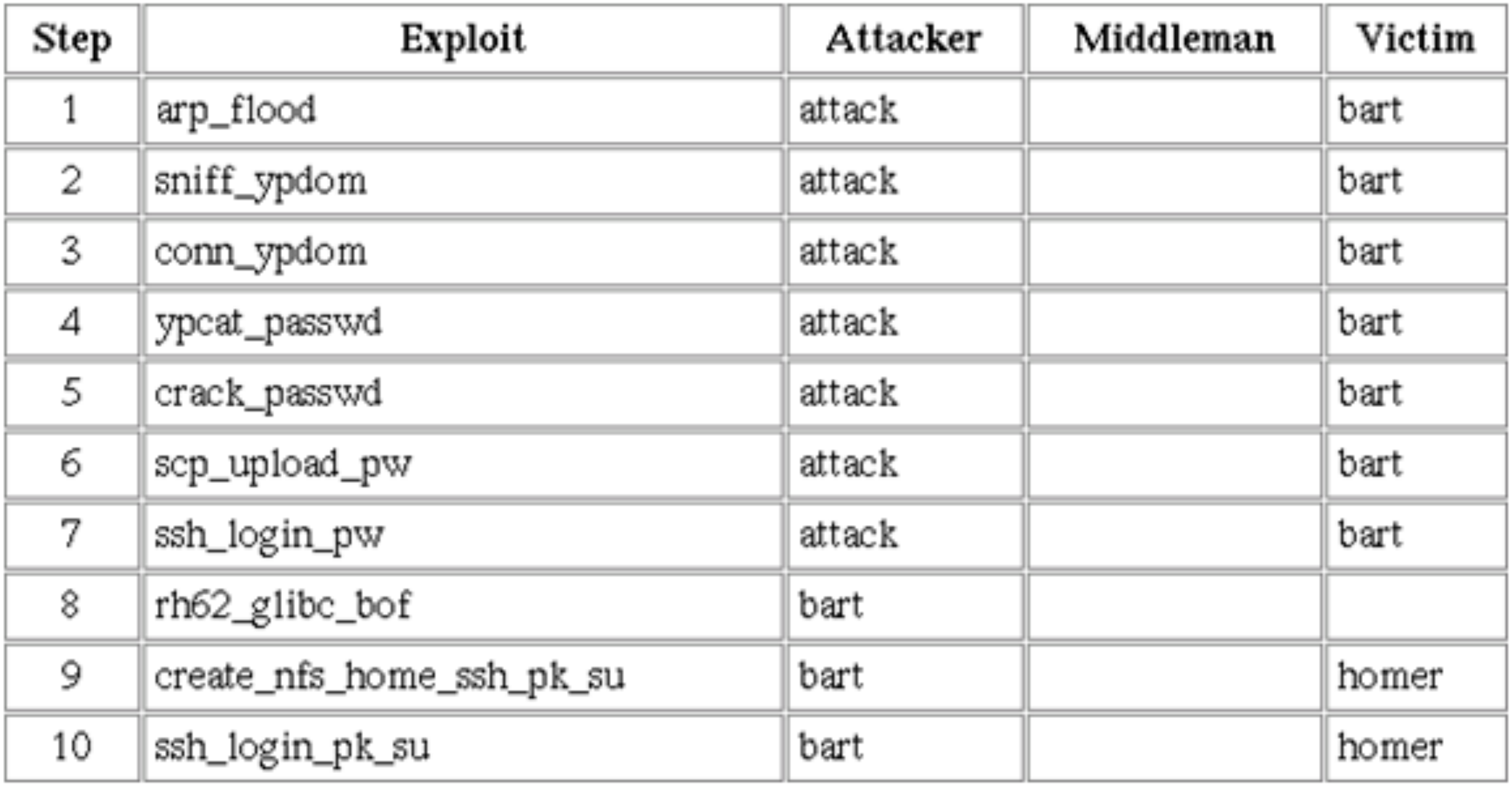
Network Attack Model

What-If

Network Hardening

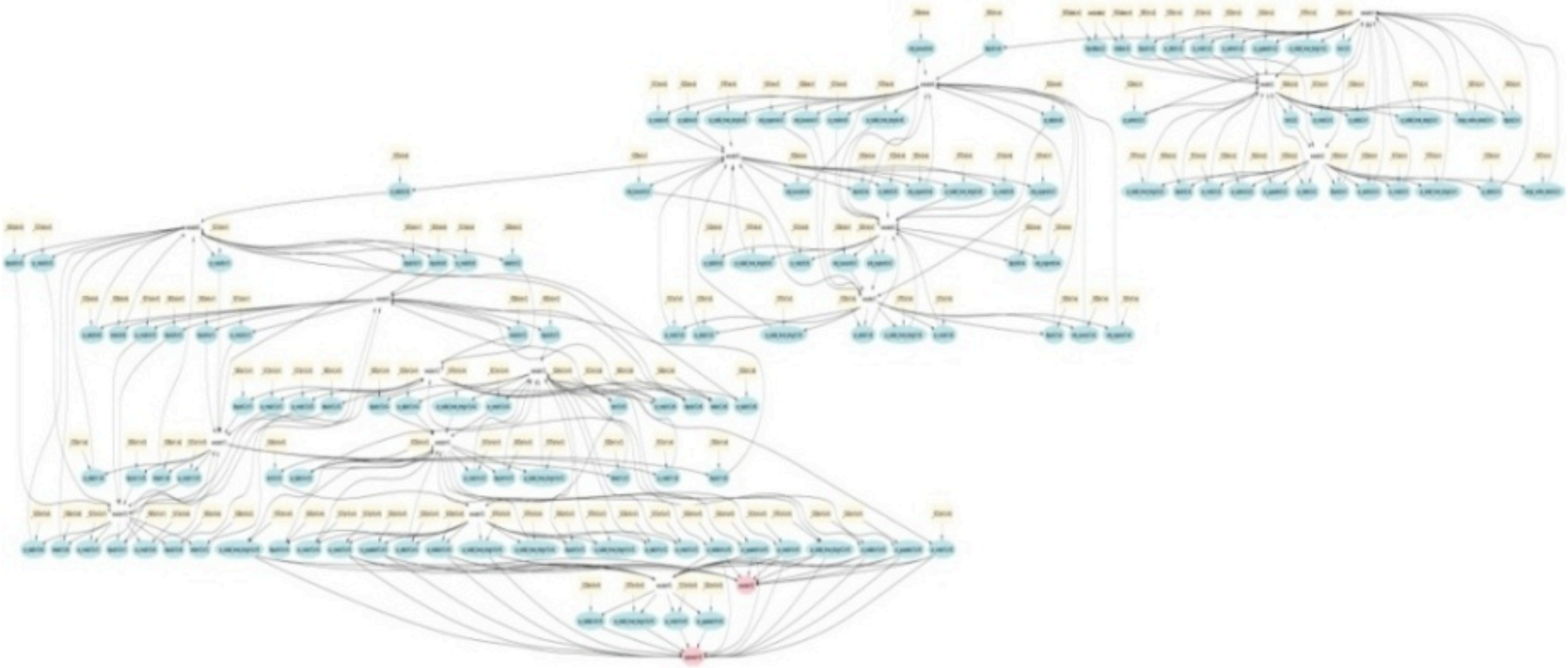
Network

Evolution Stage 1: Single Attack Paths

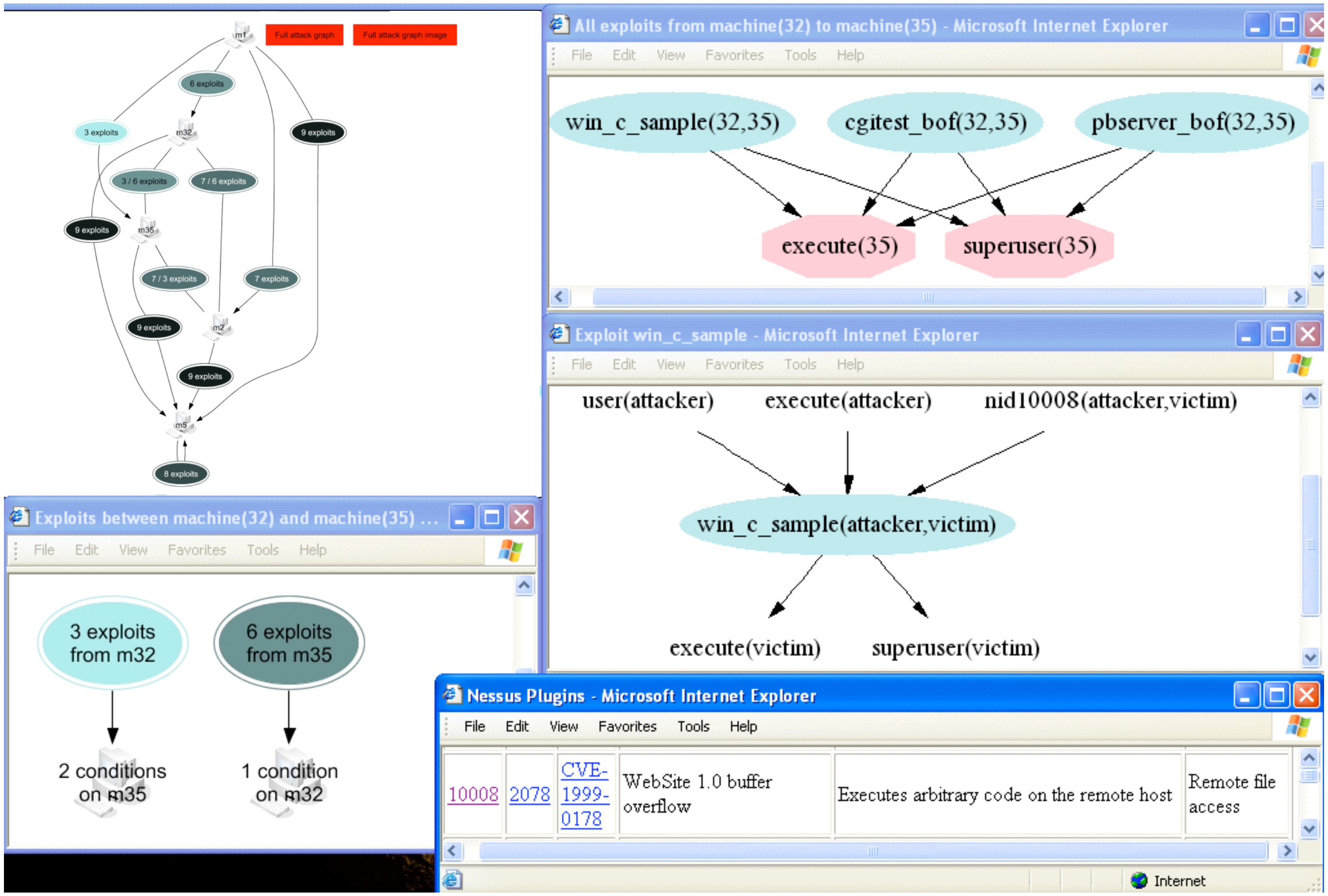


Step	Exploit	Attacker	Middleman	Victim
1	arp_flood	attack		bart
2	sniff_ypdom	attack		bart
3	conn_ypdom	attack		bart
4	ypcat_passwd	attack		bart
5	crack_passwd	attack		bart
6	scp_upload_pw	attack		bart
7	ssh_login_pw	attack		bart
8	rh62_glibc_bof	bart		
9	create_nfs_home_ssh_pk_su	bart		homer
10	ssh_login_pk_su	bart		homer

Evolution Stage 2: All Paths

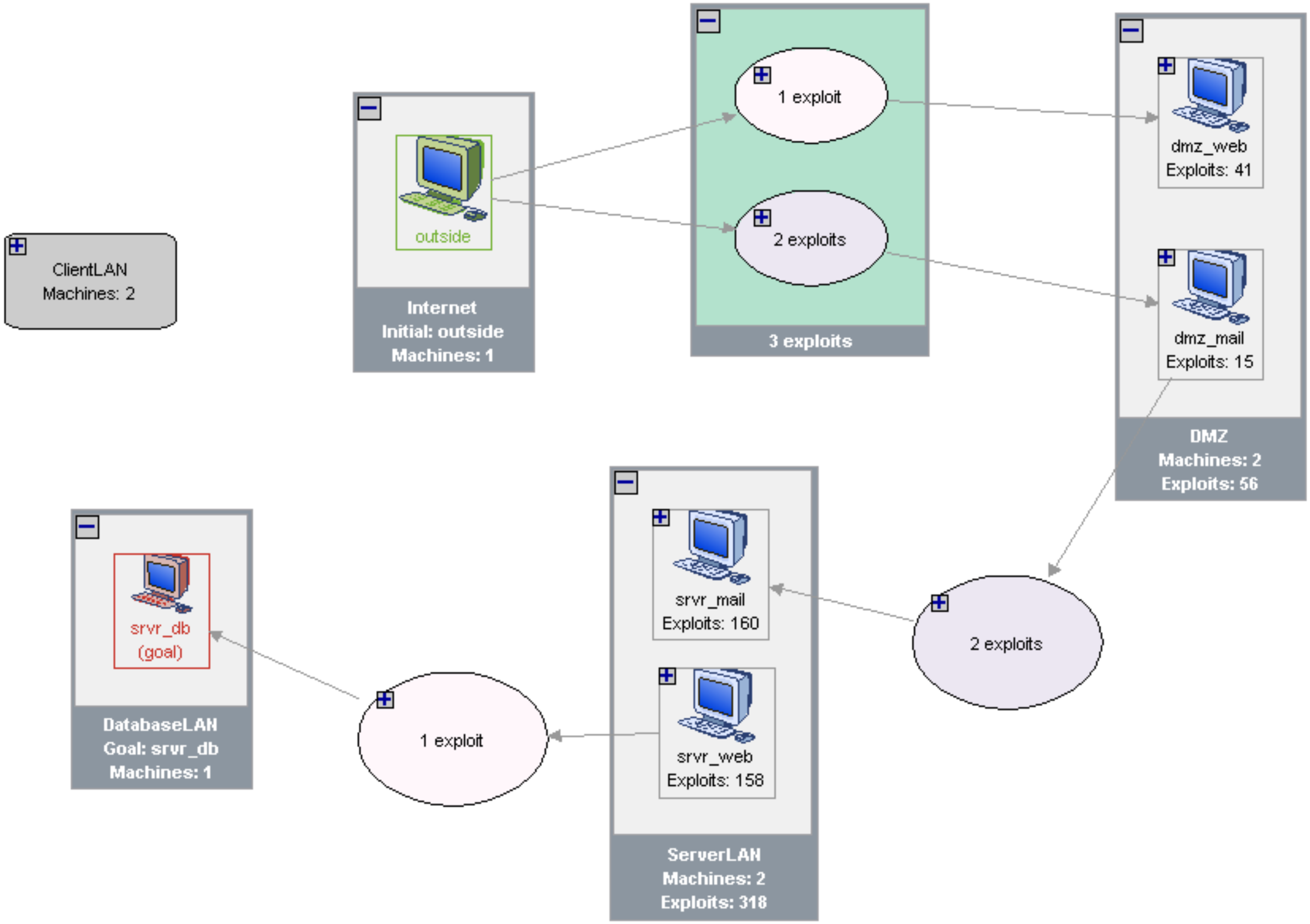


Evolution Stage 3: Graph Aggregation

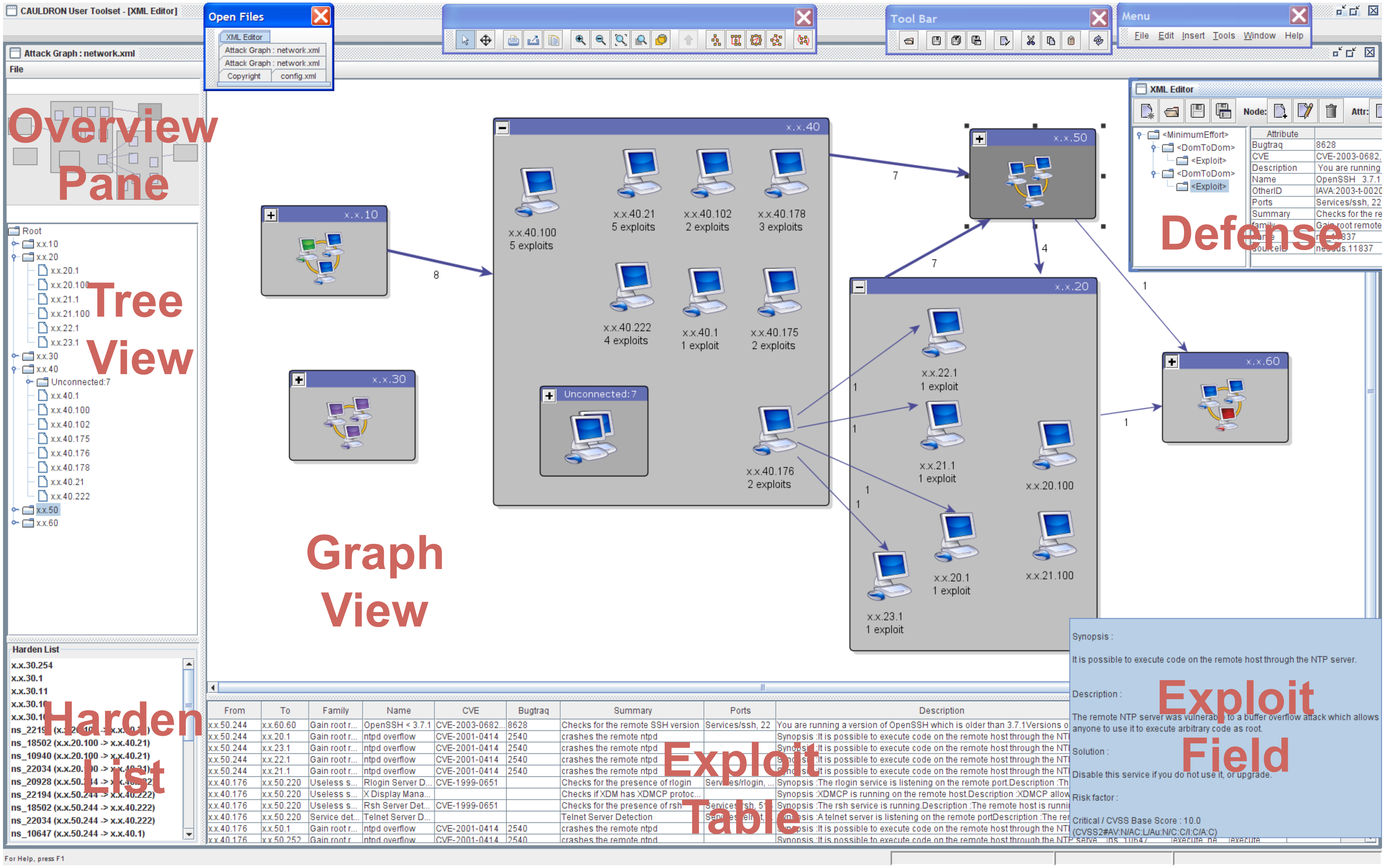

m1
Full attack graph
Full attack graph image
6 exploits
3 exploits
m32
9 exploits
3 / 6 exploits
7 / 6 exploits
9 exploits
m35
7 / 3 exploits
7 exploits
9 exploits
m2
9 exploits
m5
8 exploits
All exploits from machine(32) to machine(35) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
win_c_sample(32,35)
cgitest_bof(32,35)
pbserver_bof(32,35)
execute(35)
superuser(35)
Exploit win_c_sample - Microsoft Internet Explorer
File Edit View Favorites Tools Help
user(attacker)
execute(attacker)
nid10008(attacker,victim)
win_c_sample(attacker,victim)
execute(victim)
superuser(victim)
Exploits between machine(32) and machine(35) ...
File Edit View Favorites Tools Help
3 exploits from m32
6 exploits from m35
2 conditions on m35
1 condition on m32
Nessus Plugins - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Internet

10008	2078	CVE-1999-0178	WebSite 1.0 buffer overflow	Executes arbitrary code on the remote host	Remote file access

Evolution Stage 4: Interactive Visualization



Next Evolution in Attack Graph Visual Analysis



Toolbars

Overview Pane

Tree View

Graph View

Defense

Harden List

Exploit Table

Exploit Field

Attribute	
Bugtraq	8628
CVE	CVE-2003-0682,
Description	You are running
Name	OpenSSH 3.7.1
OtherID	IAVA:2003-t-0020
Ports	Services/ssh, 22
Summary	Checks for the re
family	Gain root remote
name	ns_11837
sourceID	nessus.11837

Harden List

x.x.30.254
x.x.30.1
x.x.30.11
x.x.30.10
x.x.30.10
ns_22194 (x.x.20.100 -> x.x.40.21)
ns_18502 (x.x.20.100 -> x.x.40.21)
ns_10940 (x.x.20.100 -> x.x.40.21)
ns_22034 (x.x.20.100 -> x.x.40.21)
ns_20928 (x.x.50.244 -> x.x.40.222)
ns_22194 (x.x.50.244 -> x.x.40.222)
ns_18502 (x.x.50.244 -> x.x.40.222)
ns_22034 (x.x.50.244 -> x.x.40.222)
ns_10647 (x.x.50.244 -> x.x.40.1)

From	To	Family	Name	CVE	Bugtraq	Summary	Ports	Description
x.x.50.244	x.x.60.60	Gain root r...	OpenSSH < 3.7.1	CVE-2003-0682...	8628	Checks for the remote SSH version	Services/ssh, 22	You are running a version of OpenSSH which is older than 3.7.1Versions o
x.x.50.244	x.x.20.1	Gain root r...	ntpd overflow	CVE-2001-0414	2540	crashes the remote ntpd		Synopsis :It is possible to execute code on the remote host through the NT
x.x.50.244	x.x.23.1	Gain root r...	ntpd overflow	CVE-2001-0414	2540	crashes the remote ntpd		Synopsis :It is possible to execute code on the remote host through the NT
x.x.50.244	x.x.22.1	Gain root r...	ntpd overflow	CVE-2001-0414	2540	crashes the remote ntpd		Synopsis :It is possible to execute code on the remote host through the NT
x.x.50.244	x.x.21.1	Gain root r...	ntpd overflow	CVE-2001-0414	2540	crashes the remote ntpd		Synopsis :It is possible to execute code on the remote host through the NT
x.x.40.176	x.x.50.220	Useless s...	Rlogin Server D...	CVE-1999-0651		Checks for the presence of rlogin	Services/rlogin, ...	Synopsis :The rlogin service is listening on the remote port.Description :Th
x.x.40.176	x.x.50.220	Useless s...	X Display Mana...			Checks if XDM has XDMCP protoc...		Synopsis :XDMCP is running on the remote host.Description :XDMCP allow
x.x.40.176	x.x.50.220	Useless s...	Rsh Server Det...	CVE-1999-0651		Checks for the presence of rsh	Services/rsh, 51	Synopsis :The rsh service is running.Description :The remote host is runni
x.x.40.176	x.x.50.220	Service det...	Telnet Server D...			Telnet Server Detection	Services/telnet, ...	Synopsis :A telnet server is listening on the remote portDescription :The rer
x.x.40.176	x.x.50.1	Gain root r...	ntpd overflow	CVE-2001-0414	2540	crashes the remote ntpd		Synopsis :It is possible to execute code on the remote host through the NT
x.x.40.176	x.x.50.252	Gain root r...	ntpd overflow	CVE-2001-0414	2540	crashes the remote ntpd		Synopsis :It is possible to execute code on the remote host through the NTP serve

Synopsis :

It is possible to execute code on the remote host through the NTP server.

Description :

The remote NTP server was vulnerable to a buffer overflow attack which allows anyone to use it to execute arbitrary code as root.

Solution :

Disable this service if you do not use it, or upgrade.

Risk factor :

Critical / CVSS Base Score : 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)