The Volgenau School of
Information Technology and Engineering

GEORGE MASON UNIVERSITY

Beyond Reactive Management of Network Intrusions

Professor Sushil Jajodia

Center for Secure Information Systems
jajodia@gmu.edu
http://csis.gmu.edu/jajodia

Center for SECURE INFORMATION SYSTEMS
CSIS

Outline

- CSIS Overview
- Selected Research Projects
- Cauldron
- Challenges

Program History

- Established in 1990 as the first academic center in Information Security at a U.S. University
- Charter Member, NSA Center of Academic Excellence in Information Assurance Education and Research

Objectives

- Focus multi-disciplinary research to solve a wide range of computer security problems
- Collaborate with leading research institutions, industry, and government partners
- Transfer solutions from academic research to commercial sector

Current Status

- A leading information security research center
- NSA Center of Academic Excellence in Information Assurance Education: 1999-2013
- NSA Center of Academic Excellence in Information Assurance Research: 2008-2013
- Committee on National Security Systems and the National Security Agency certified that our courses meet National Training Standards for academic years 2002-2013
- Selected as a participant in the DoD Information Assurance Scholarship Program, 2001-present
- Established partnership with National Defense University Information Resource Management College

Current Status (cont.)

- Produced licensed works and received 3 patents, filed for 12 patents
- Long history of sponsorship by federal agencies and the commercial sector
- Substantial scientific publication record
- Highly productive alumni
- Reputation attracts high quality students
- Visiting scholars from Canada, Italy, South Africa, Korea, India, Japan, Spain, Germany, Sweden, China, Singapore, France

Research Staff and Faculty

Sushil Jajodia
Director

Anup Ghosh
Chief Scientist

Steven Noel
Associate Director

Pramod Kalapa
Director of Software Development

Angelos Stavrou
Assistant Professor

Kun Sun
Research Professor

Yih Huang
Research Scientist

Specialized Degree Programs

- PhD in IT, CS, and EE with security concentration
- MS in Information Security and Assurance
- Graduate Certificates in Information System Security and Network Security
- BS in IT and CS with security concentration

PhD Graduates

- **Universities:** Rutgers, Penn State, North Carolina State, South Carolina at Columbia, Colorado State, Arkansas at Little Rock, North Carolina at Charlotte, James Madison, Tulsa, Howard
- **Government:** National Defense University, Naval Postgraduate School, US Military Academy, Naval Research Lab, NSA, NIST
- **Industry:** MITRE, Booz Allen, SAIC, Sparta, Computer Sciences Corporation, IDA

Current Government Sponsors

NSA

HSARPA

AFRL

DARPA

NIST

FAA

ARO

NSF

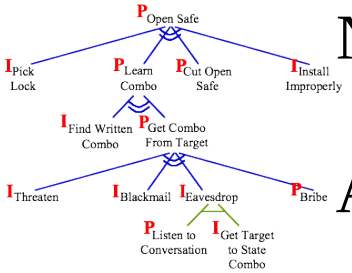
IARPA

AFOSR

Expenditures and Award Increments

FY Expenditures	
2005	1,705,559
2006	1,870,656
2007	2,176,279
2008	3,043,552
2009	3,112,101
FY Awards & Increments	
2006	3,129,389
2007	1,975,621
2008	4,137,151
2009	2,327,491

Key Research Areas

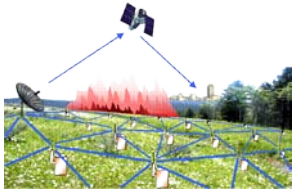


Network Attack Analysis

Cyber Situational Awareness

Virtualization For Security

Protection Against Malicious Code

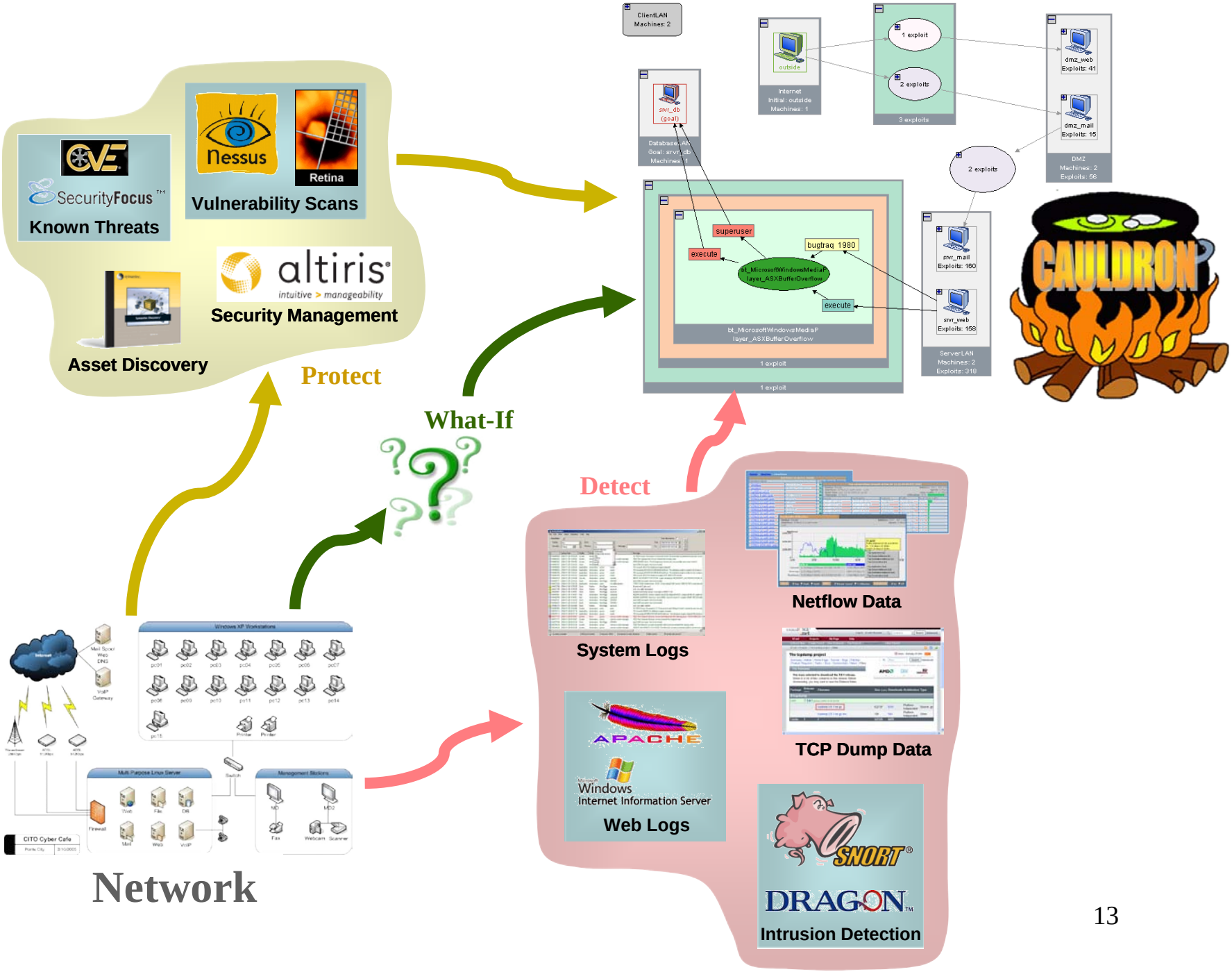


Mobile Ad Hoc And Wireless Networks

Secure Composable Systems

Secure Information Sharing

Automated Intrusion Recovery

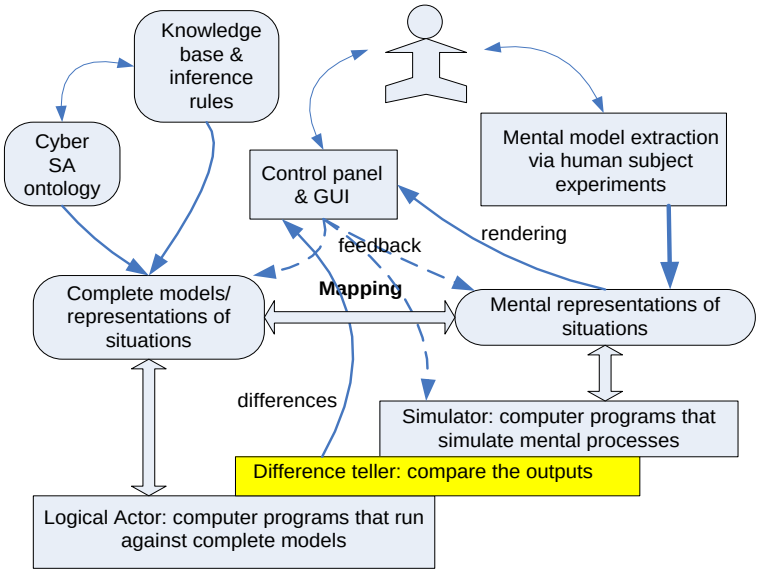

Known Threats
Vulnerability Scans
Security Management
Asset Discovery
Protect
What-If
Detect
Network
System Logs
Netflow Data
TCP Dump Data
Web Logs
Intrusion Detection
CAULDRON

Computer-aided Human Centric Cyber Situation Awareness
A MURI Project Sponsored By Army Research Office

Sushil Jajodia
Center for Secure Information Systems, George Mason University

Current Limitations

- Inaccurate and incomplete vulnerability analysis, intrusion detection, and forensics
- Lack of capability to monitor certain microscopic system/attack behavior
- Limited capability to transform/fuse/distill information into cyber intelligence
- Limited capability to handle uncertainty
- Existing system designs are not very "friendly" to Cyber Situational Awareness



Technical Approach

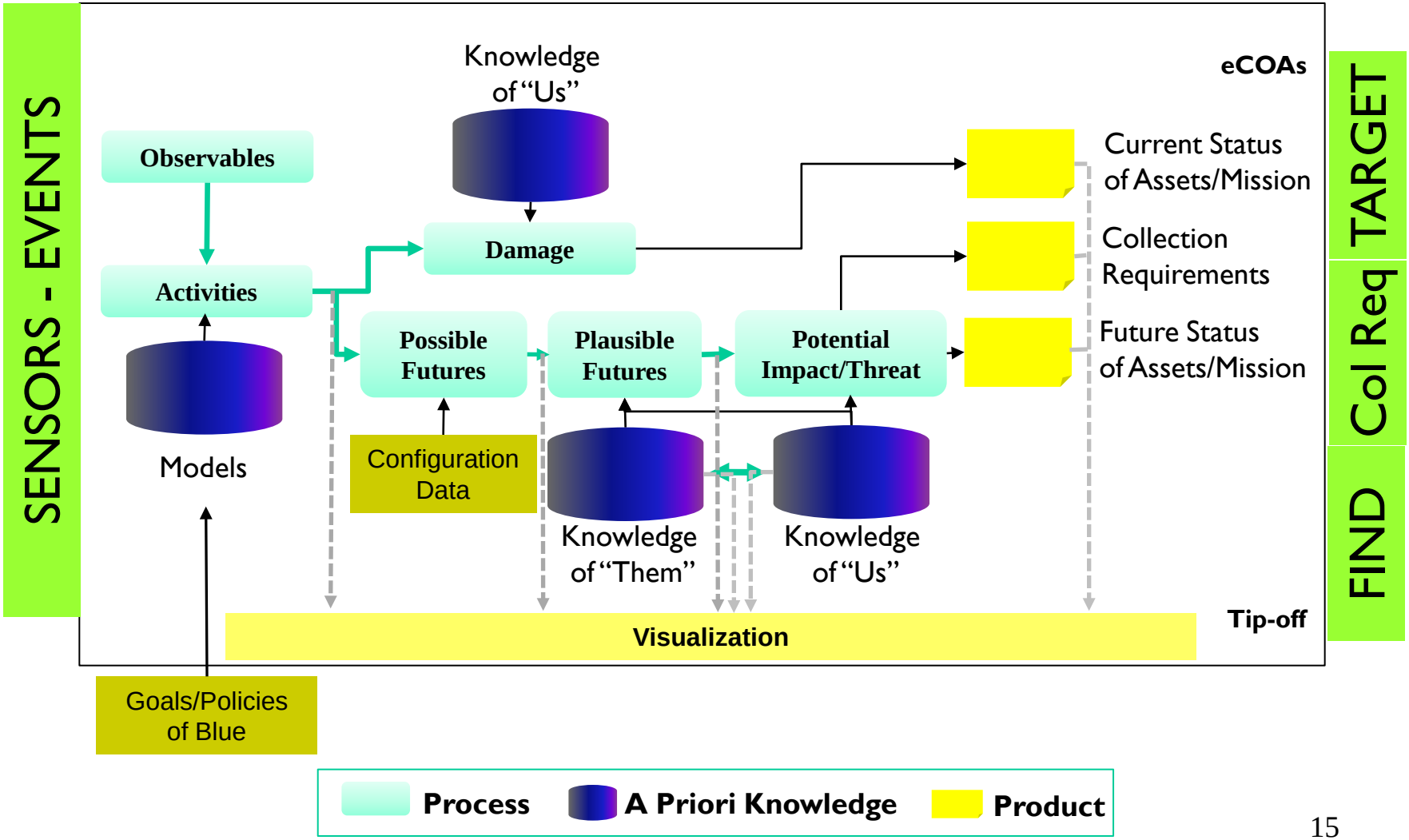
- Build the missing links through innovations in CSA specific information and knowledge fusion, cognition automation, artificial intelligence, and visual analytics
- Awareness-driven cyber defense
- Develop automatic blind spot identification and monitoring techniques

Other Team Members

- Peng Liu, John Yen, Mike McNeese, Dave Hall
  Pennsylvania State University
- Nancy Cooke
  Arizona State University
- Coty Gonzalez
  Carnegie Mellon University
- Peng Ning, Michael Young
  North Carolina State University
- V.S. Subrahmanian
  University of Maryland

Situation Awareness Process Model

From Observables to Threats (At Time, t)



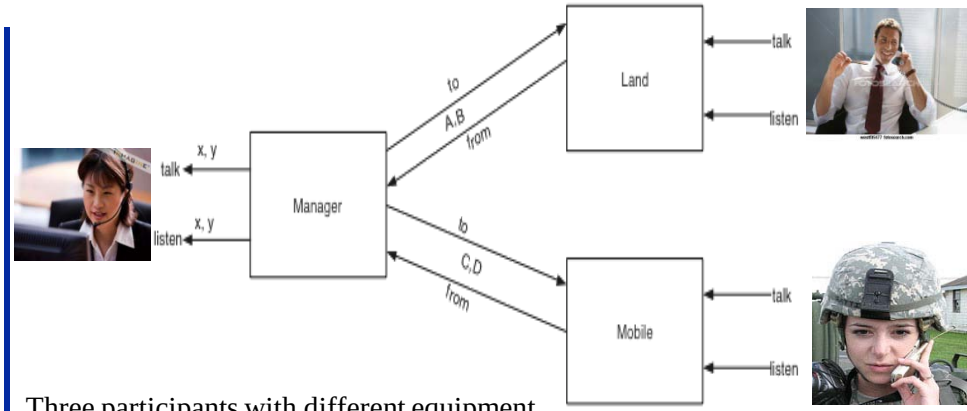
Source: George Tada and John Salerno, AFRL/Rome

Secure Composition of Networked Systems Based on User Tasks and Organizational Policy

Sushil Jajodia, Duminda Wijesekera, Angelos Stavrou
Center for Secure Information Systems, George Mason University

Objective

- Software as services are constructed using a collection of modules
- Some of these modules are constructed from other sub-modules (Referred to as components-based software engineering)
- Construction, composition, and linking of these modules can be static or dynamic
- Our objective is to make compositions and linking
  - Secure (to be able to specify security requirements)
  - Environment and resources cognizant
  - Policy based



Three participants with different equipment

- Conference manager has video-conferencing
- Soldier has secure telephone
- Engineer has a landline

Technical Approach

- Software will be deployed as sophisticated service-oriented components, with metadata describing syntax and semantics of interactions among services
- Clients can discover service providers and, when needed, multiple services will be combined to form task solutions
- Service metadata will constrain solutions so that they meet organizational policy and security requirements
- This will greatly simplify administrative burden and help guide users select secure software solutions for given tasks

Recent Progress

- Develop policy syntax and semantics
- All policies are locally stratified constraint logic programs
- Select rule syntax (system predicates) and the constraint language
- Create consistent policies for composed modules

Challenges

- Explore expressibility vs. complexity trade-offs
- Enhance policy framework beyond connecting modules

Autonomic Recovery of Enterprise-wide Systems After Attack or Failure with Forward Correction (AFOSR MURI)

Anup Ghosh, Sushil Jajodia: {aghosh1,jajodia}@gmu.edu; Angelos Keroymytis, Sal Stolfo, Jason Nieh: {angelos,sal,nieh}@cs.columbia.edu; Peng Liu :pliu@ist.psu.edu

Objective

Develop self-regenerative enterprise networks that recover and re-constitute themselves after attacks and failures

- Develop a transaction-based model for commodity operating systems to determine where an attack occurred, what data or programs were altered, and back-out all these changes without affecting unrelated data/activities.
- Automatically generate patches to make systems more robust after attack.

Technical Approach:

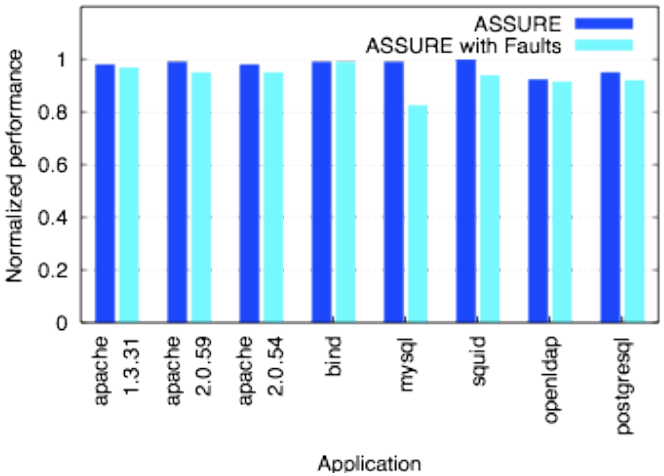
- Develop a layered approach to self-regenerative systems:
  - application-level resilience using error virtualization and rescue points
  - system-level resilience using virtualization and transaction semantics for programs to roll back system state to the last known good continuation point
  - dynamic patching of applications to improve resiliency after attack
  - roll forward with correction to quarantine tainted processes and files & back-out changes

DoD Benefit:

- Uninterruptible service for critical network centric warfare services
- Error localization and tolerance in applications
- Automatic system recovery after attack including quarantine of tainted processes and data
- Increased resiliency after attack through auto-patch generation

Accomplishments

Robustness to Network Server Exploits



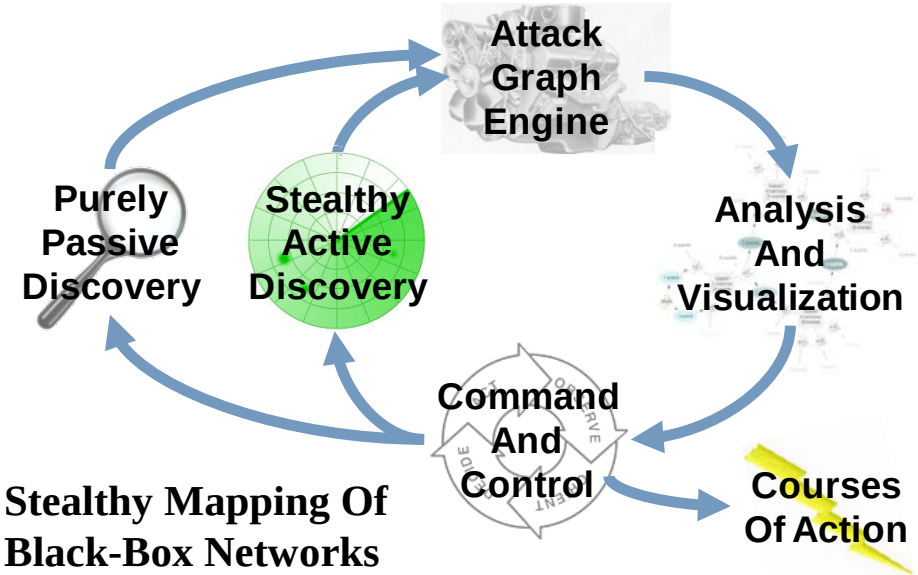
Mapping Attack Paths in Black-Box Networks Through Passive Vulnerability Inference

Anup Ghosh, Sushil Jajodia
Center for Secure Information Systems, George Mason University

Objective

Passive techniques for mapping *attack graphs* through black-box networks

- Stealthy **network reconnaissance**, when active scanning is not an option
- Hybrid techniques that supplement passive inference with **stealthy active methods**, for even more robust attack graphs
- Inference of **functional semantics** of network components, for intelligent targeting



Technical Approach

- Infer network configuration (topology, devices, services, etc.) through passive observation and stealthy active scanning
- Map discovered network elements to known vulnerabilities, and create model of network and potential attacker exploits
- Map attack graphs through network, based on attack goals and degree of network control
- Decide on best courses of action, e.g., additional information to gather, new hosts to control

Accomplishments

Purely passive observation

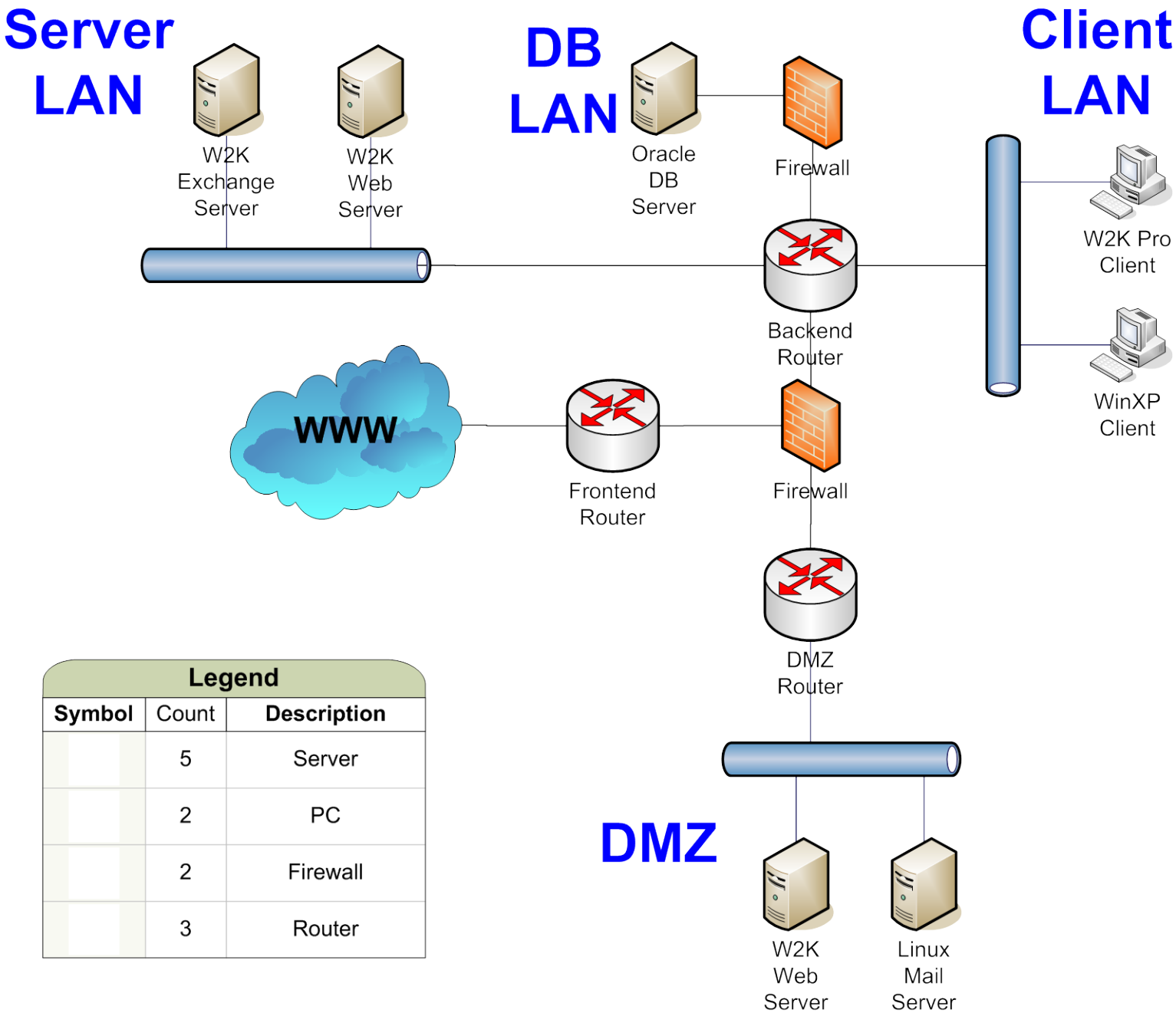
- Map network topology, protocols, and services

Cooperating outsider and stealthy insider

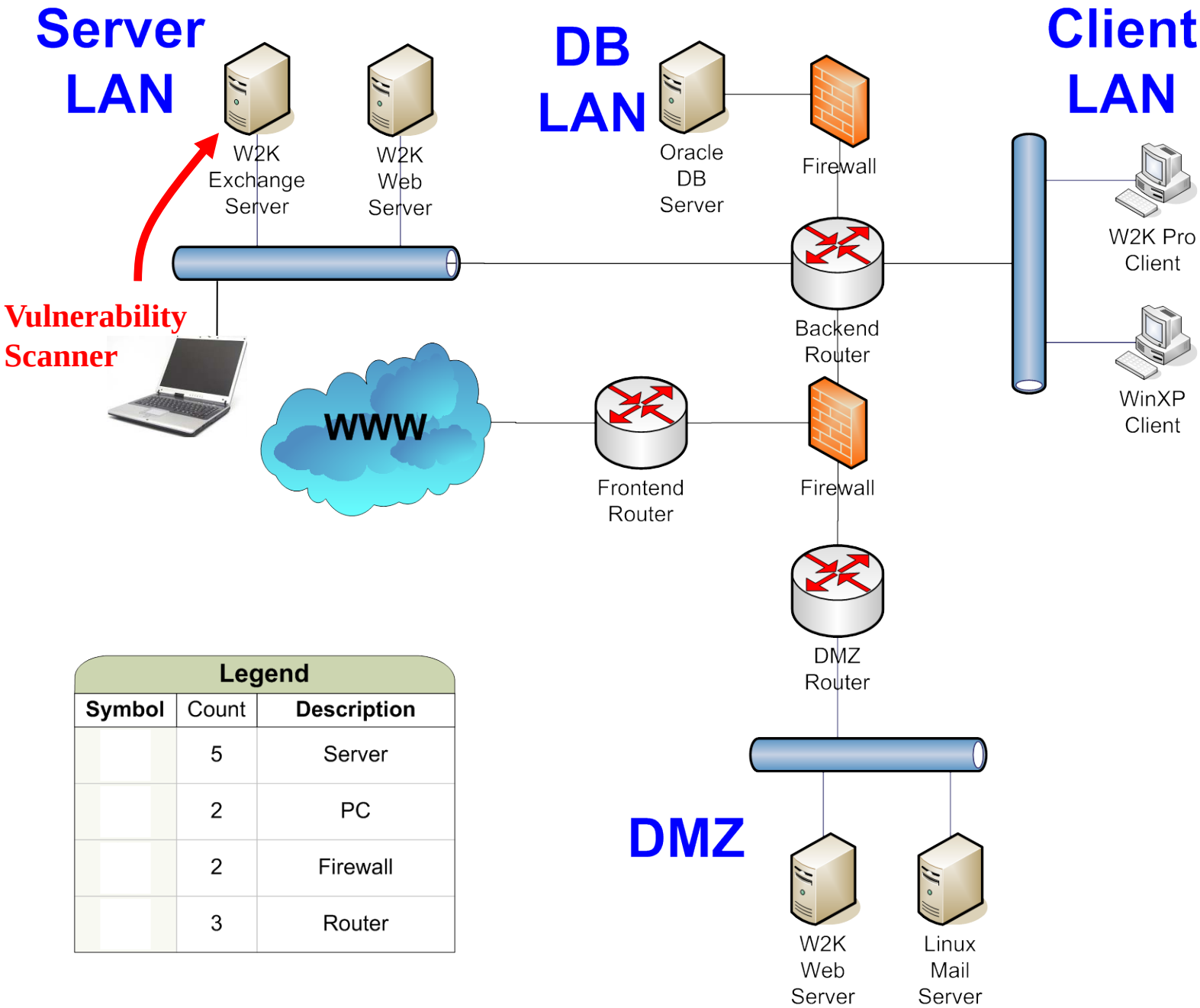
- Complete mapping of firewall holes
- Inducing new firewall holes

Challenges

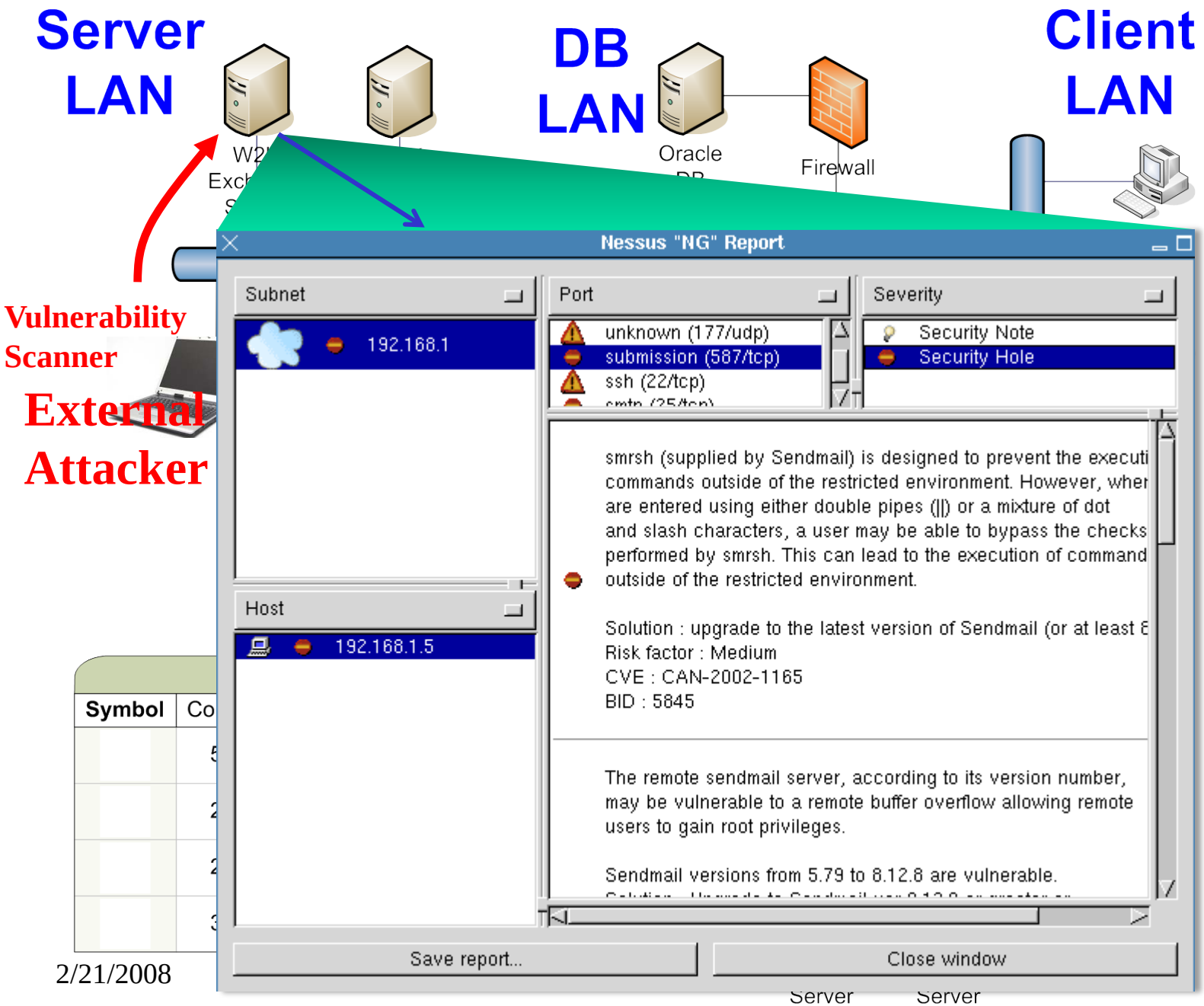
Mature from proof-of-concept code to prototype system for demonstration

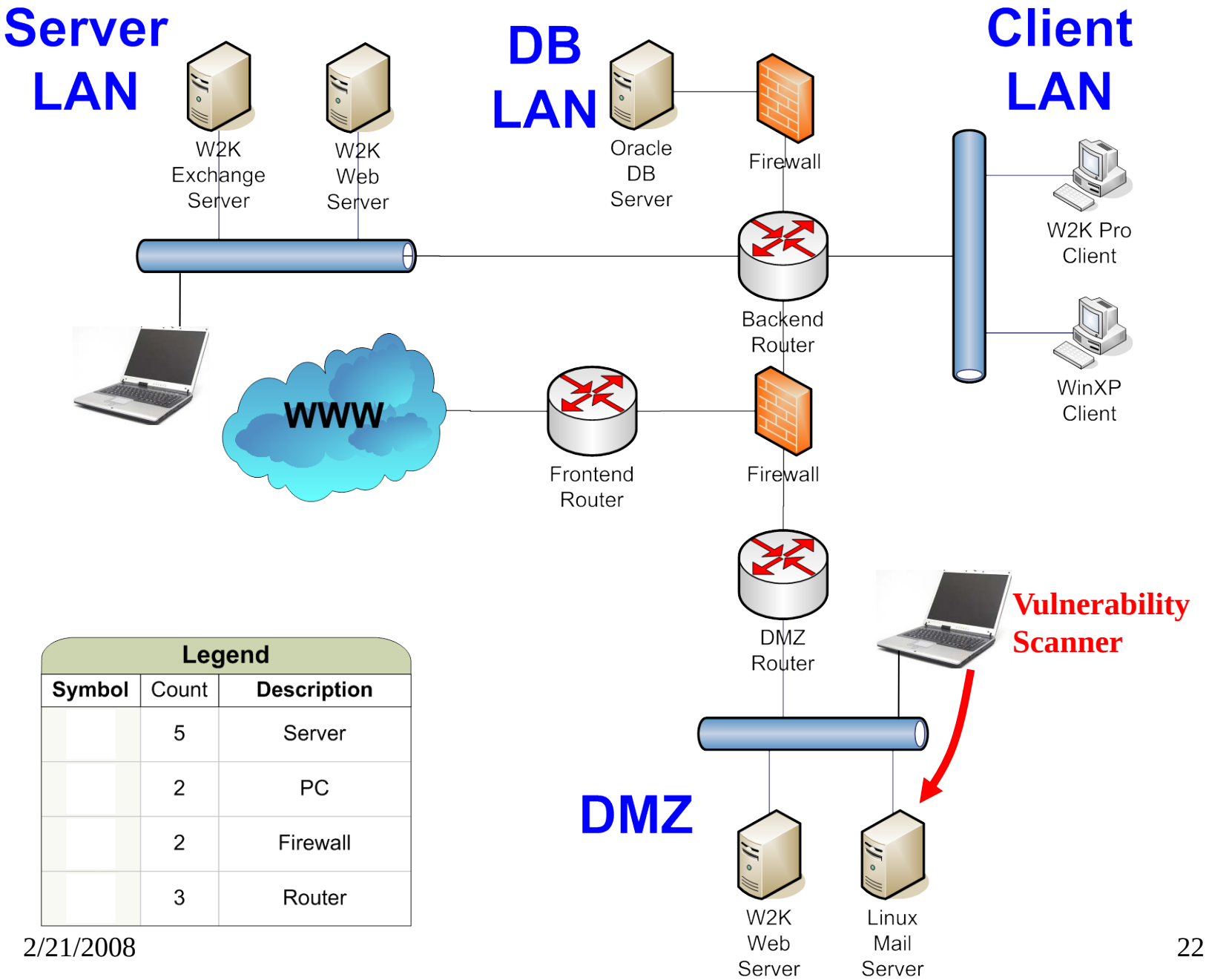


Legend		
Symbol	Count	**Description**
	5	Server
	2	PC
	2	Firewall
	3	Router

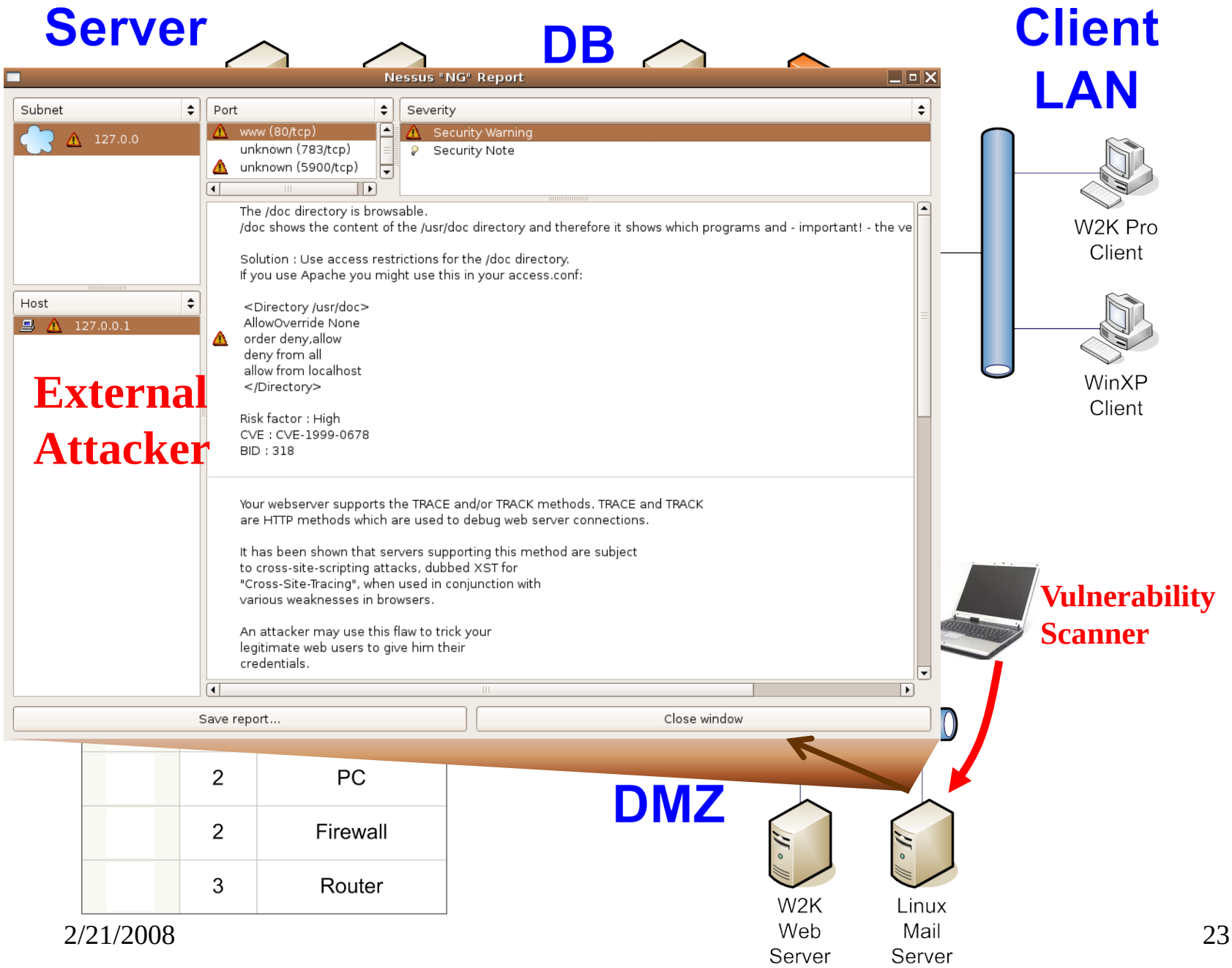


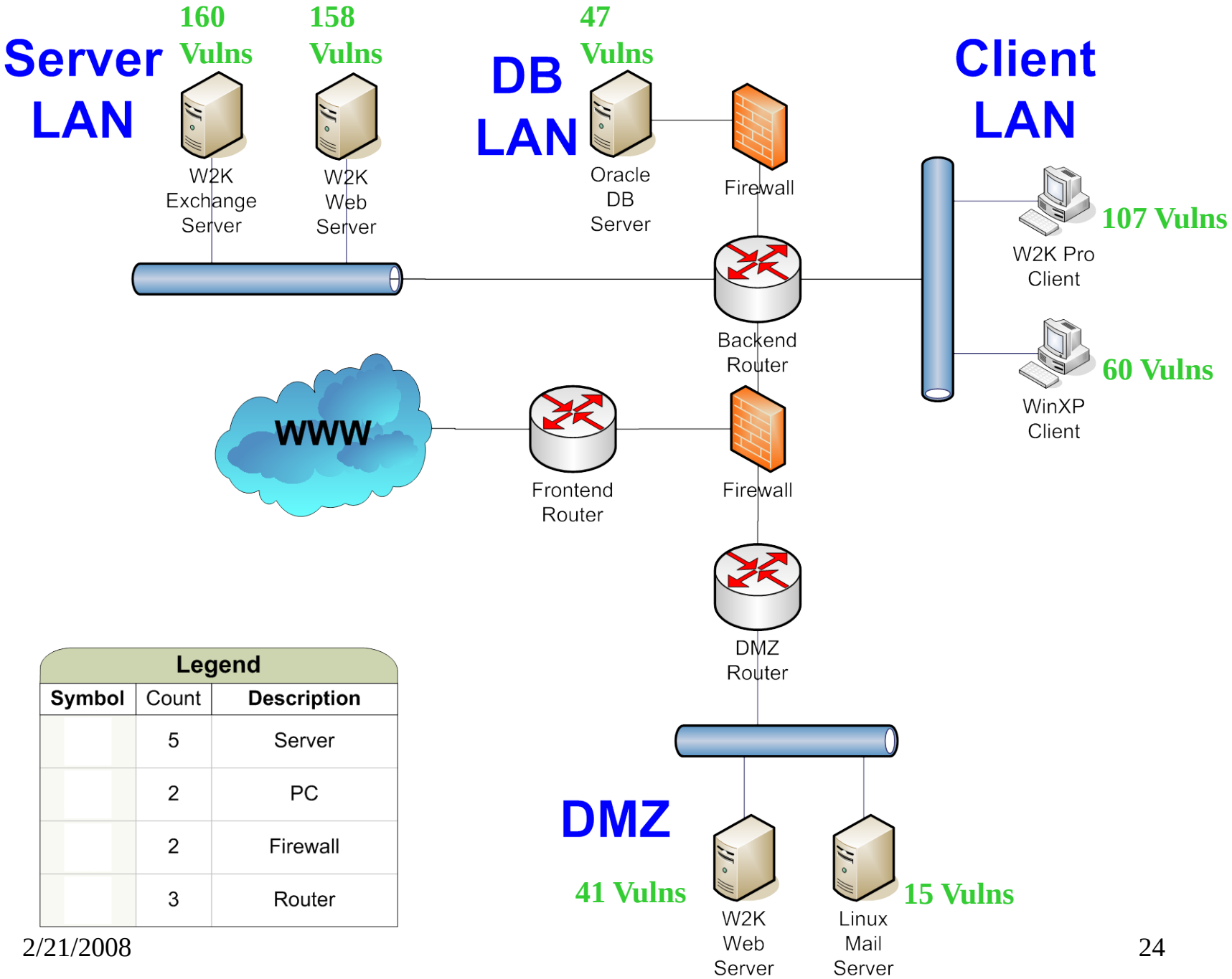
Legend		
Symbol	Count	**Description**
	5	Server
	2	PC
	2	Firewall
	3	Router


Server LAN
DB LAN
Client LAN
Oracle
Firewall
Vulnerability Scanner
External Attacker
Nessus "NG" Report
Subnet
192.168.1
Port
unknown (177/udp)
submission (587/tcp)
ssh (22/tcp)
Severity
Security Note
Security Hole
smrsh (supplied by Sendmail) is designed to prevent the executi
commands outside of the restricted environment. However, wher
are entered using either double pipes (||) or a mixture of dot
and slash characters, a user may be able to bypass the checks
performed by smrsh. This can lead to the execution of command
outside of the restricted environment.
Solution : upgrade to the latest version of Sendmail (or at least 8
Risk factor : Medium
CVE : CAN-2002-1165
BID : 5845
The remote sendmail server, according to its version number,
may be vulnerable to a remote buffer overflow allowing remote
users to gain root privileges.
Sendmail versions from 5.79 to 8.12.8 are vulnerable.
Host
192.168.1.5
Save report...
Close window
Symbol
Server
Server

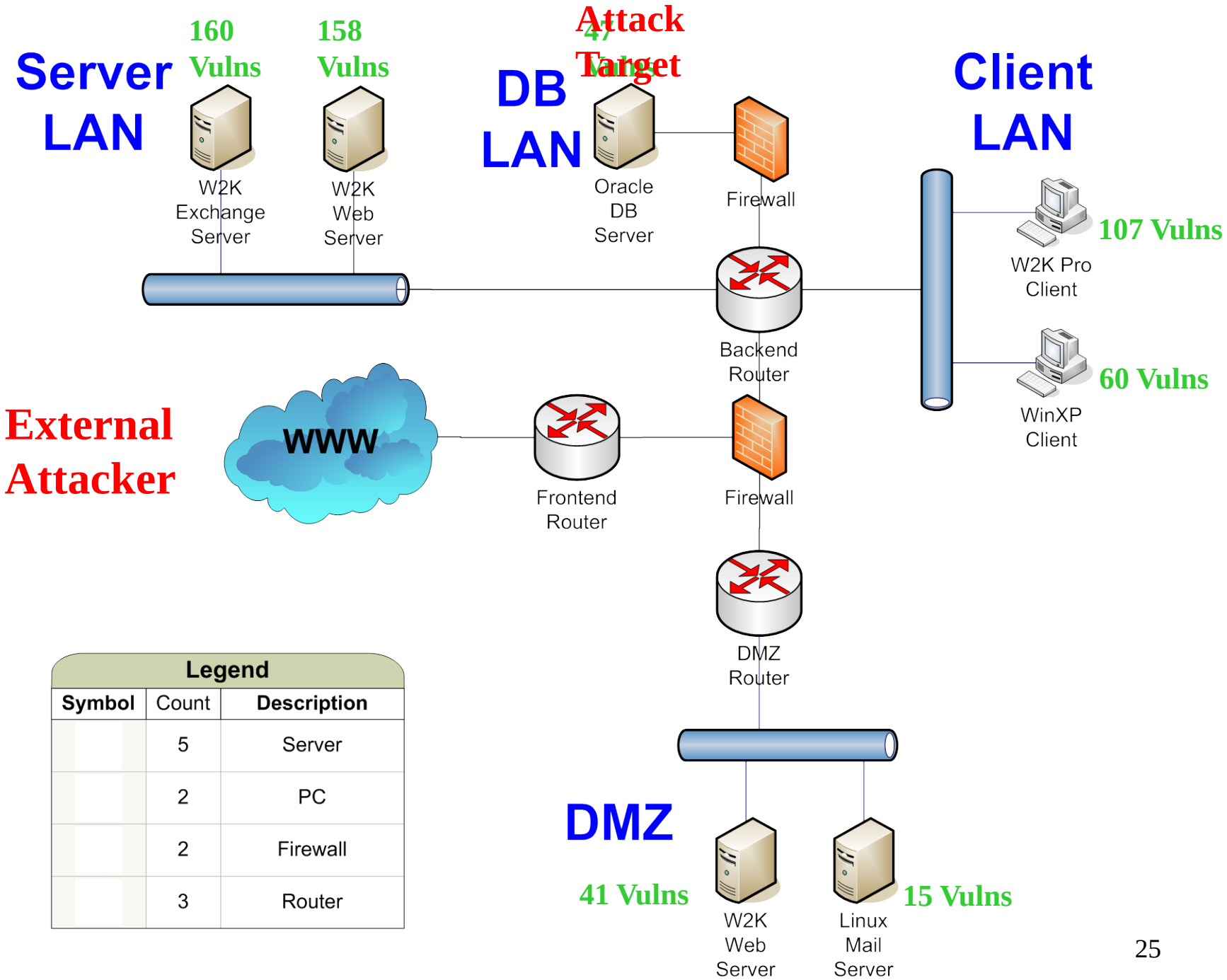


Legend		
Symbol	Count	**Description**
	5	Server
	2	PC
	2	Firewall
	3	Router


Server
DB
Client LAN
Nessus "NG" Report
Subnet
127.0.0
Port
www (80/tcp)
unknown (783/tcp)
unknown (5900/tcp)
Severity
Security Warning
Security Note
The /doc directory is browsable.
/doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the ve
Solution : Use access restrictions for the /doc directory.
If you use Apache you might use this in your access.conf:
<Directory /usr/doc>
AllowOverride None
order deny,allow
deny from all
allow from localhost
</Directory>
Risk factor : High
CVE : CVE-1999-0678
BID : 318
Your webserver supports the TRACE and/or TRACK methods. TRACE and TRACK
are HTTP methods which are used to debug web server connections.
It has been shown that servers supporting this method are subject
to cross-site-scripting attacks, dubbed XST for
"Cross-Site-Tracing", when used in conjunction with
various weaknesses in browsers.
An attacker may use this flaw to trick your
legitimate web users to give him their
credentials.
Host
127.0.0.1
External Attacker
Save report...
Close window
W2K Pro Client
WinXP Client
Vulnerability Scanner
DMZ
W2K Web Server
Linux Mail Server
2
PC
2
Firewall
3
Router



Legend		
Symbol	Count	**Description**
	5	Server
	2	PC
	2	Firewall
	3	Router



Legend		
Symbol	Count	Description
	5	Server
	2	PC
	2	Firewall
	3	Router

Limitations of Vulnerability Scanners

- Generate overwhelming amount of data
- Example Nessus scan
  - Elapsed time: 00:48:07
  - Total security holes found: 255
  - High severity: 40
  - Low severity: 117
  - Informational: 98
- No indication of how vulnerabilities can be combined
- Can an outside attacker obtain access to the Crown Jewels?
- Where does a security administrator start?

Limitations of IDSs

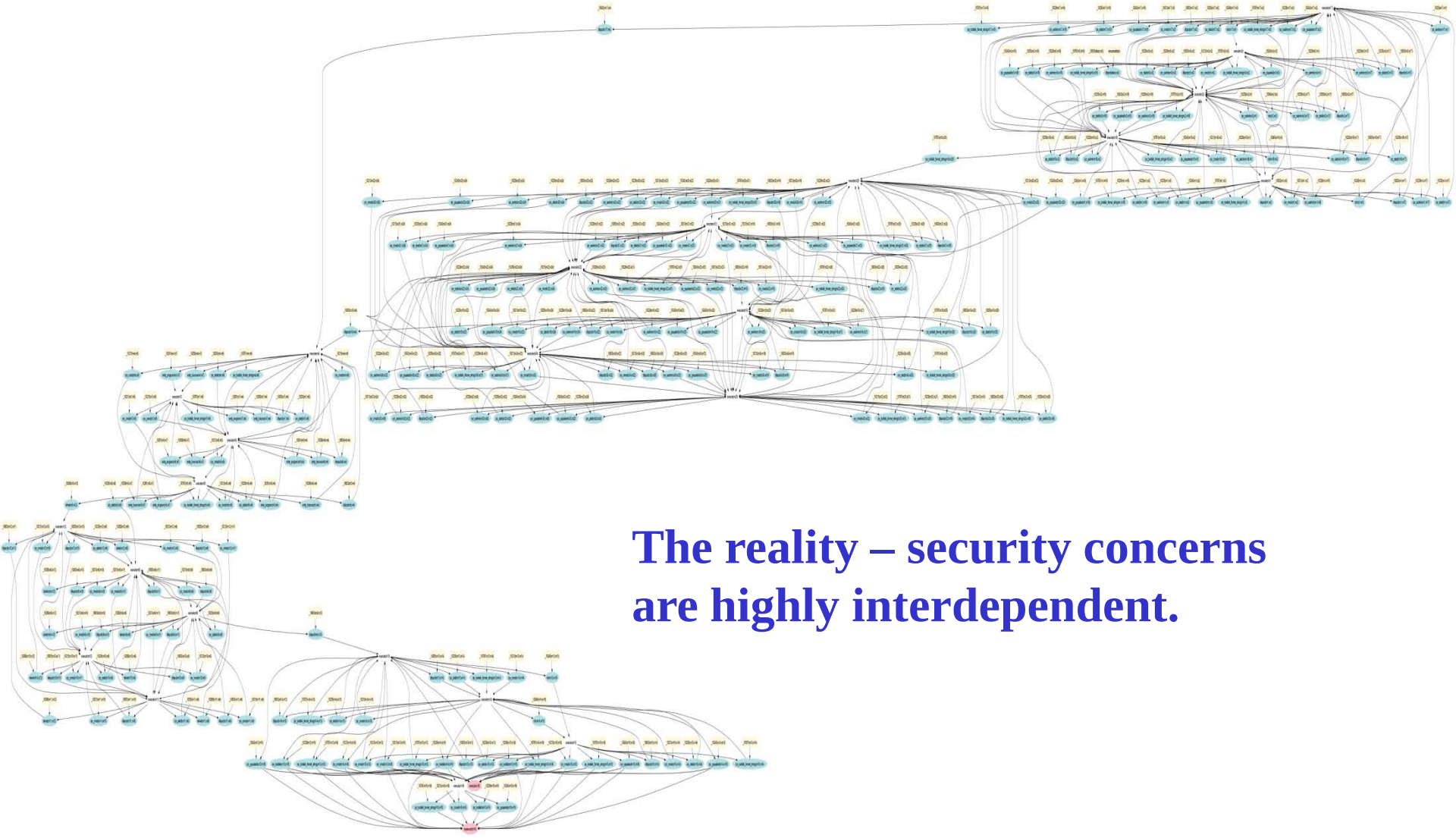
- Generate overwhelming number of alerts
- Many false alerts – normal traffic or failed attacks
- Alerts are isolated
- No indication of how alerts can be combined
- Incomplete alert information
- Where does a security administrator start?
- Is the attacker trying to obtain access to Crown Jewels?
- Require extensive human intervention

Summary

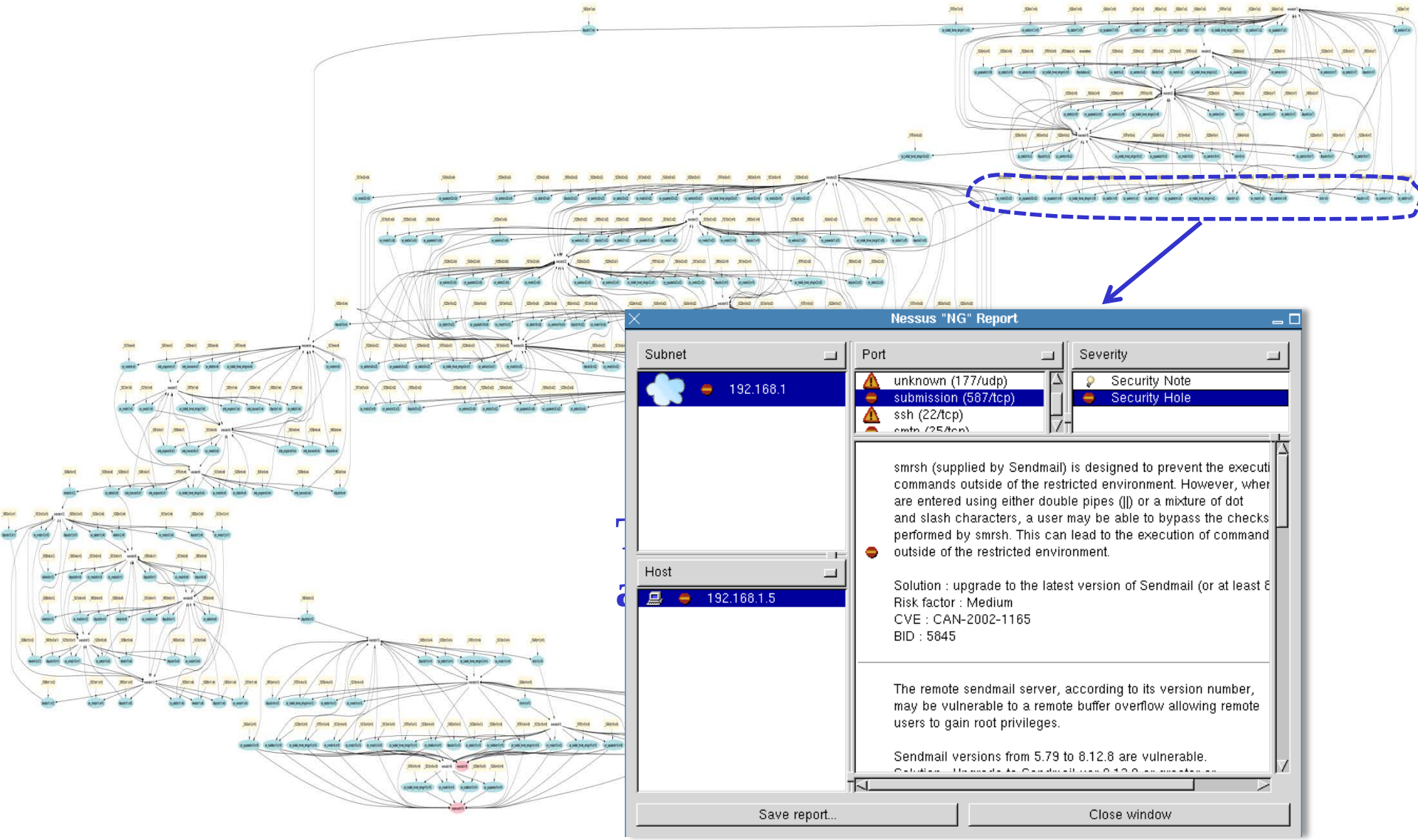
- Current security measures largely independent
- Little synergy among tools
- Vulnerabilities considered in isolation may seem acceptable risks, but attackers can combine them to produce devastating results

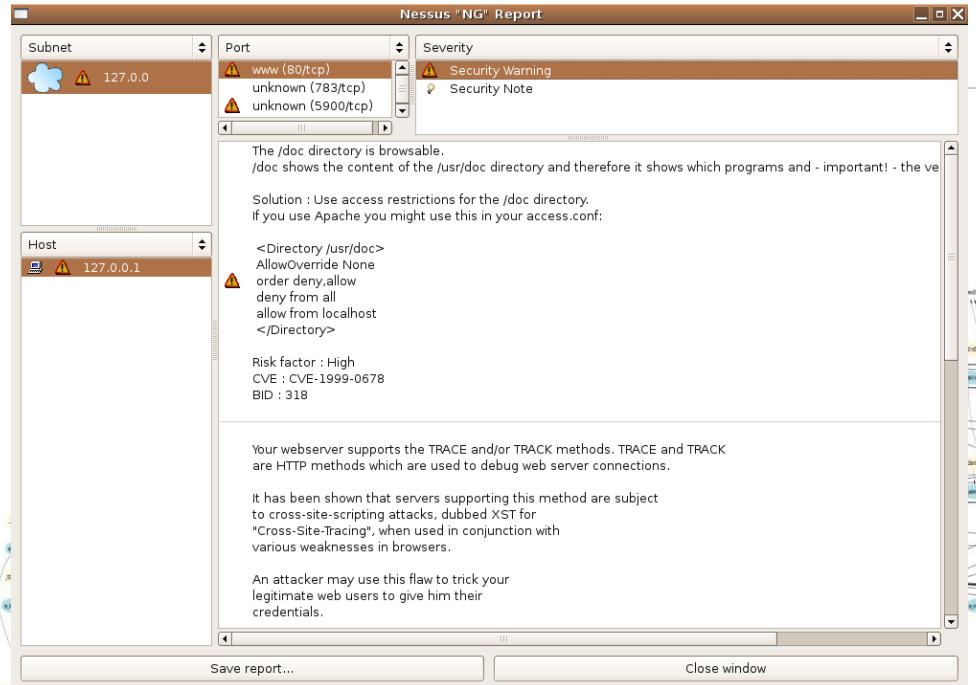
What is lacking?

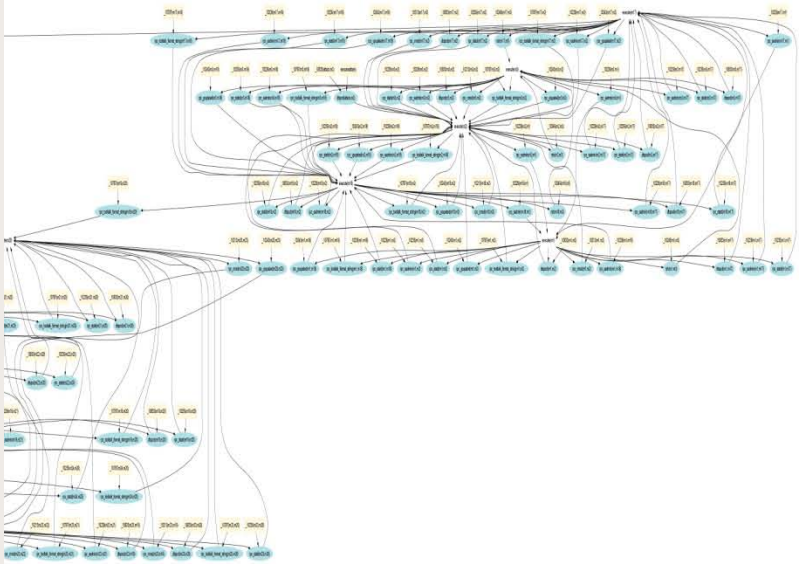
- Context for total network security
- How outsiders penetrate firewalls and launch attacks from compromised hosts
- Insider attacks

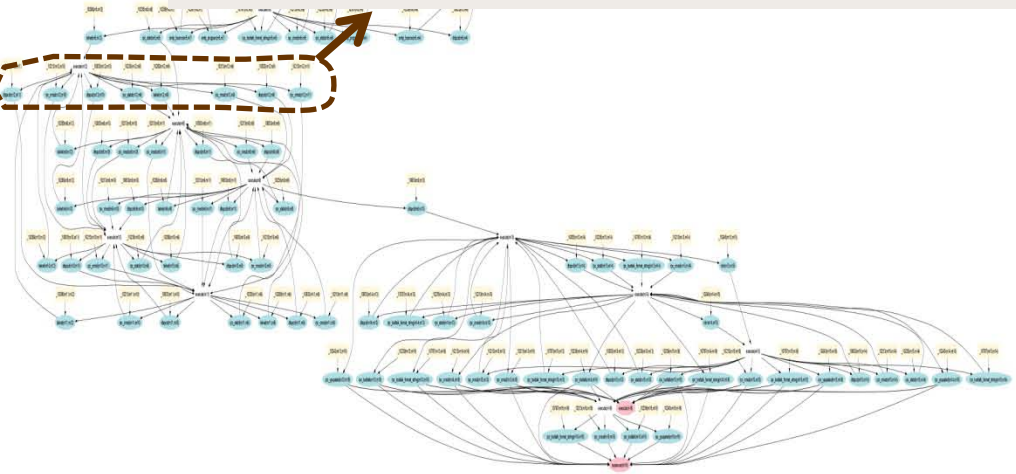


The reality – security concerns are highly interdependent.


Nessus "NG" Report
Subnet
192.168.1
Port
unknown (177/udp)
submission (587/tcp)
ssh (22/tcp)
Severity
Security Note
Security Hole
smrsh (supplied by Sendmail) is designed to prevent the executi
commands outside of the restricted environment. However, wher
are entered using either double pipes (||) or a mixture of dot
and slash characters, a user may be able to bypass the checks
performed by smrsh. This can lead to the execution of command
outside of the restricted environment.
Solution : upgrade to the latest version of Sendmail (or at least 8
Risk factor : Medium
CVE : CAN-2002-1165
BID : 5845
The remote sendmail server, according to its version number,
may be vulnerable to a remote buffer overflow allowing remote
users to gain root privileges.
Sendmail versions from 5.79 to 8.12.8 are vulnerable.
Host
192.168.1.5
Save report...
Close window







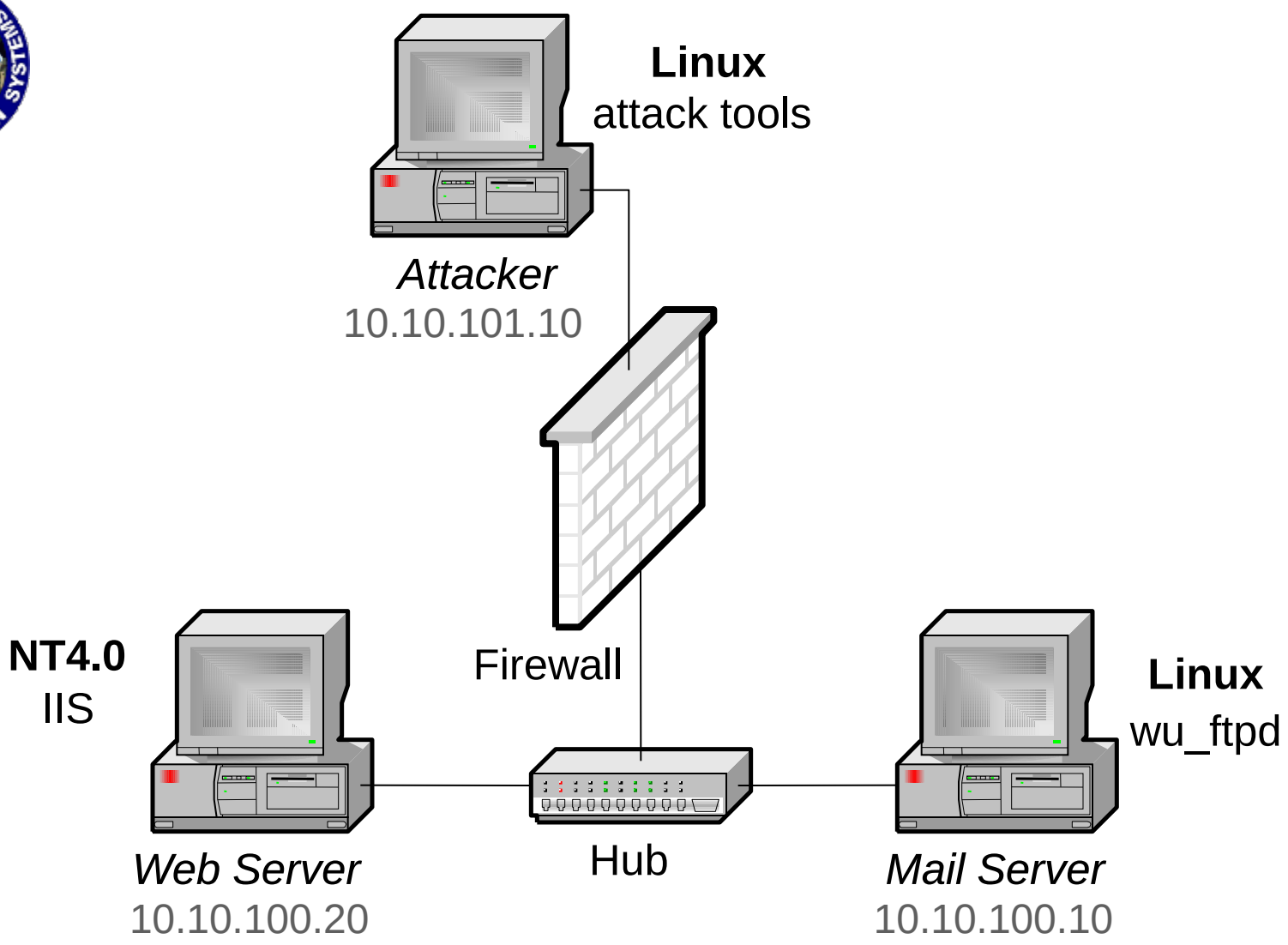
Simply Listing Problems
Misses the Big Picture!

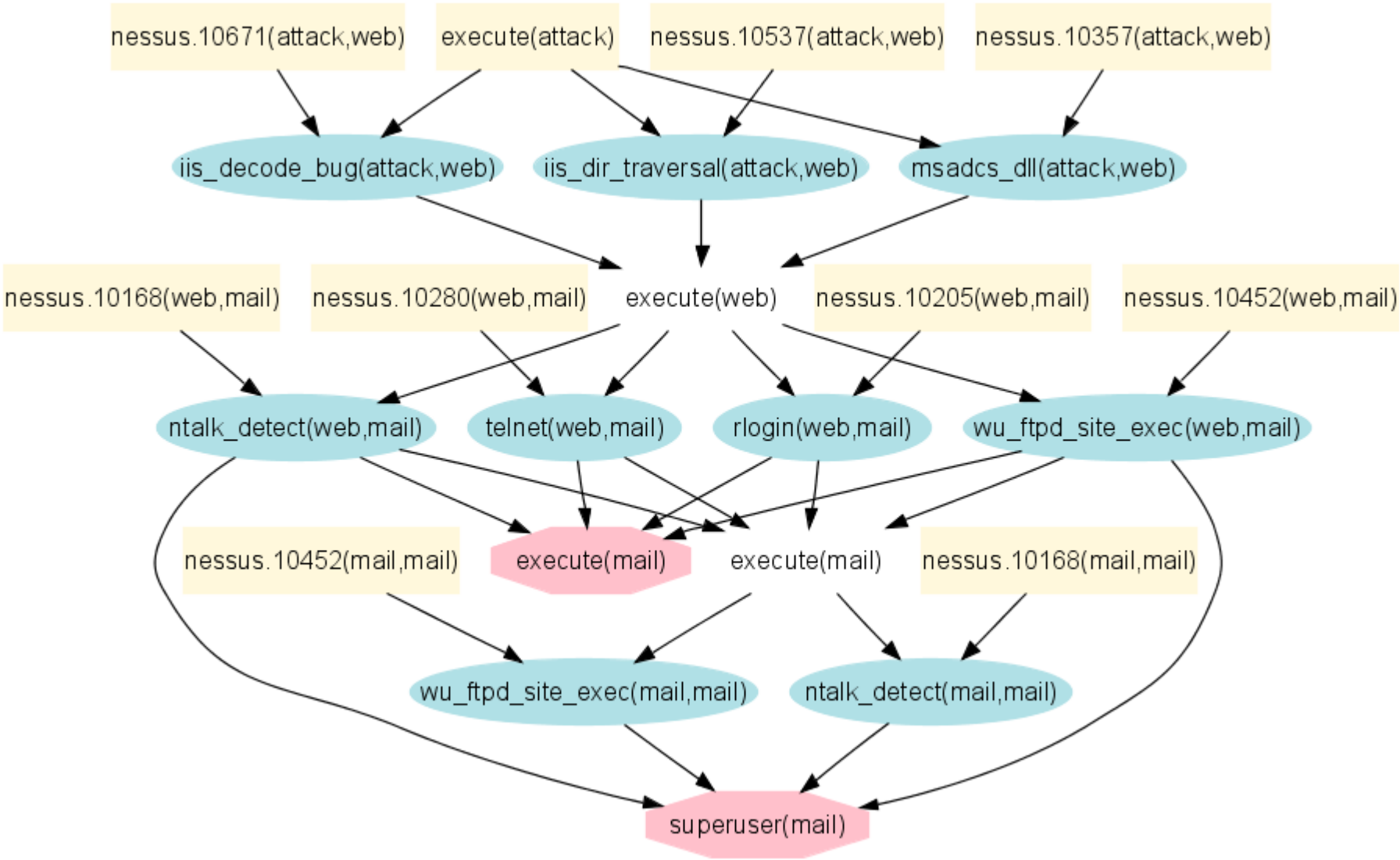
Penetration Testing

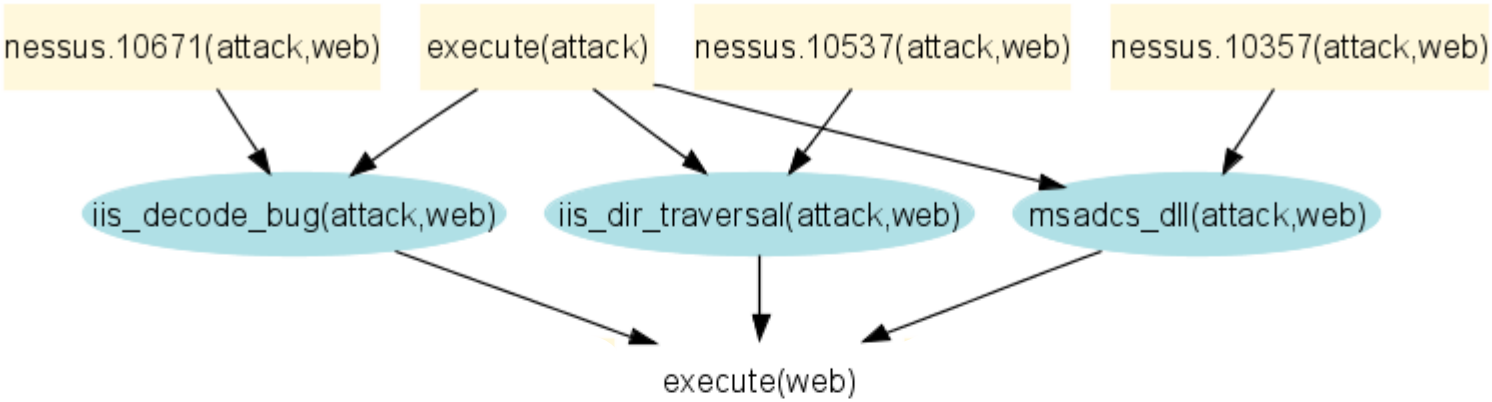
- Few experts available
- Red teams can be expensive
- Tedious
- Error-prone
- Impractical for large networks
- No formal claims

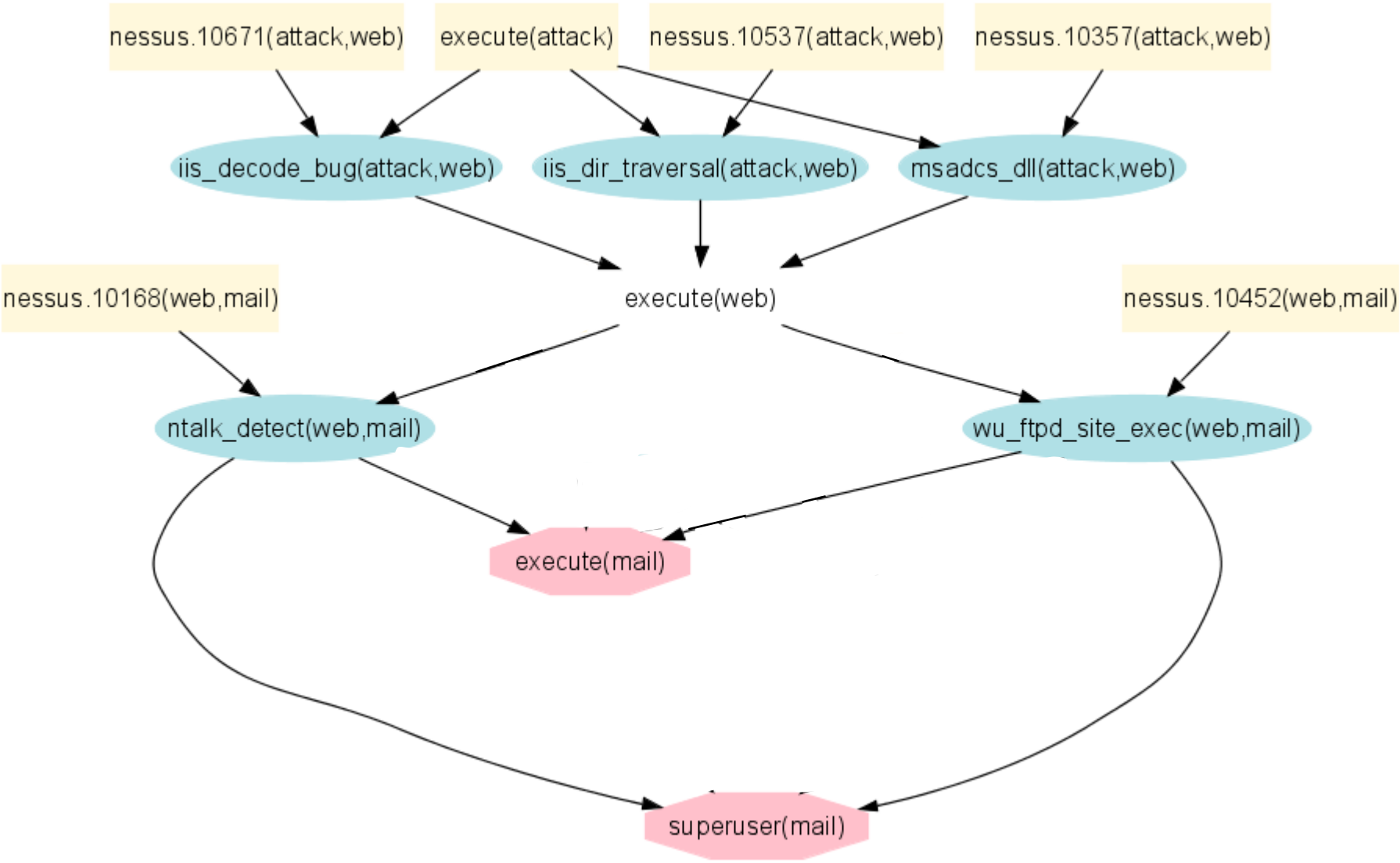
Attack Graphs

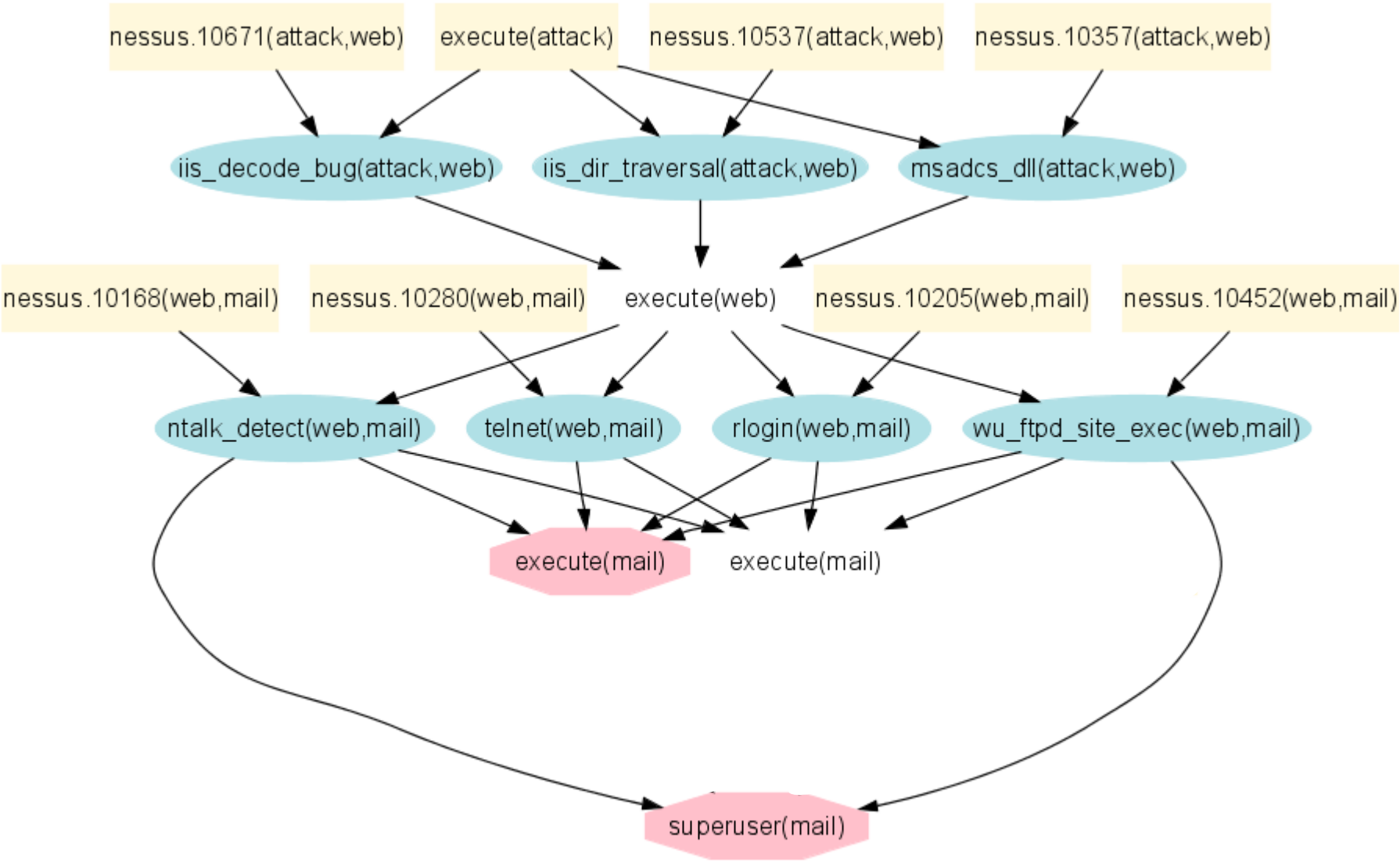
- An attacker breaks into a network through a chain of exploits where each exploit lays the groundwork for subsequent exploits
- Chain is called an attack path
- Set of all possible attack paths form an attack graph
- Generate attack graphs to mission critical resources
- Report only those vulnerabilities associated with the attack graphs

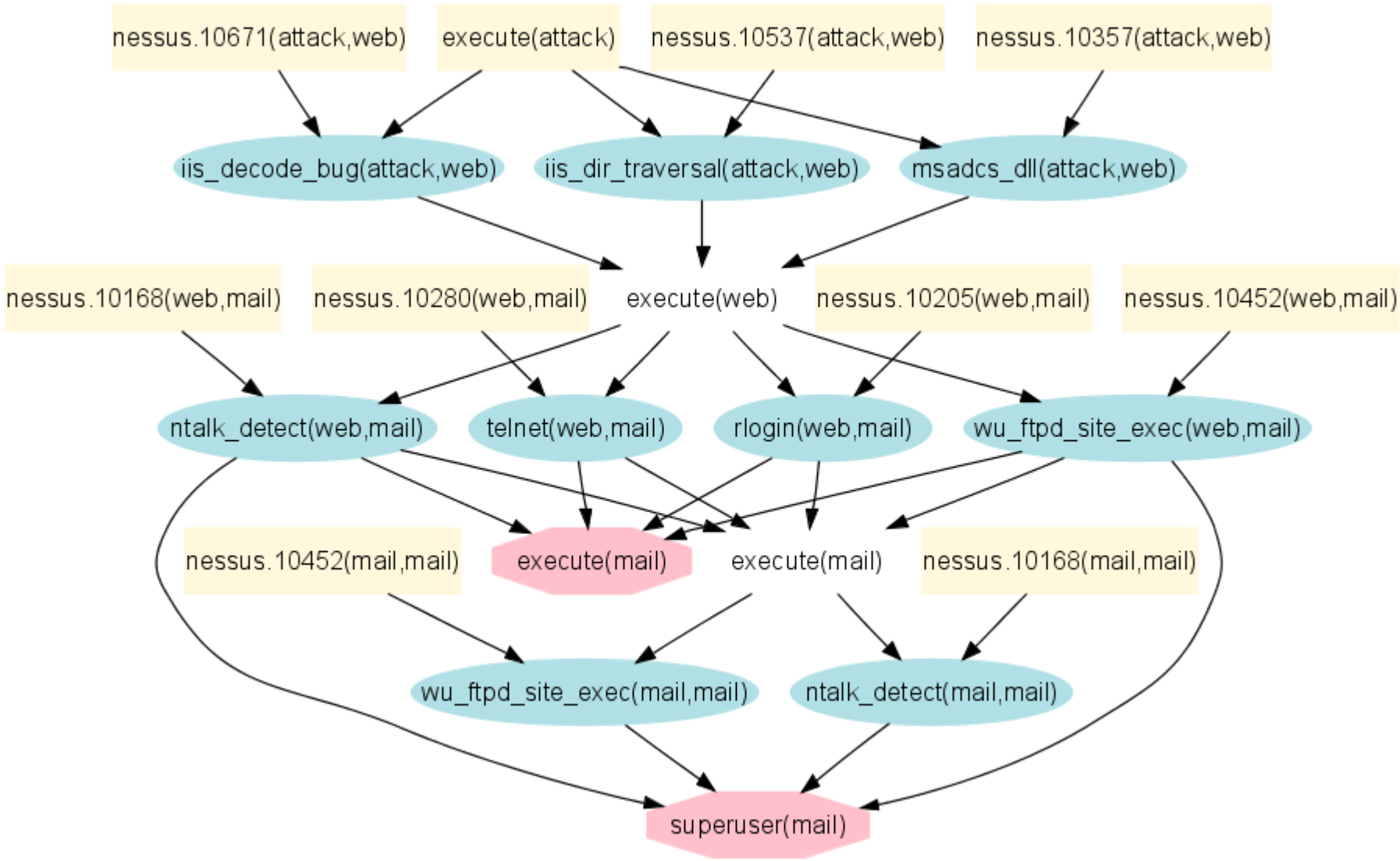

Linux
attack tools
Attacker
10.10.101.10
Firewall
NT4.0
IIS
Web Server
10.10.100.20
Hub
Linux
wu_ftpd
Mail Server
10.10.100.10

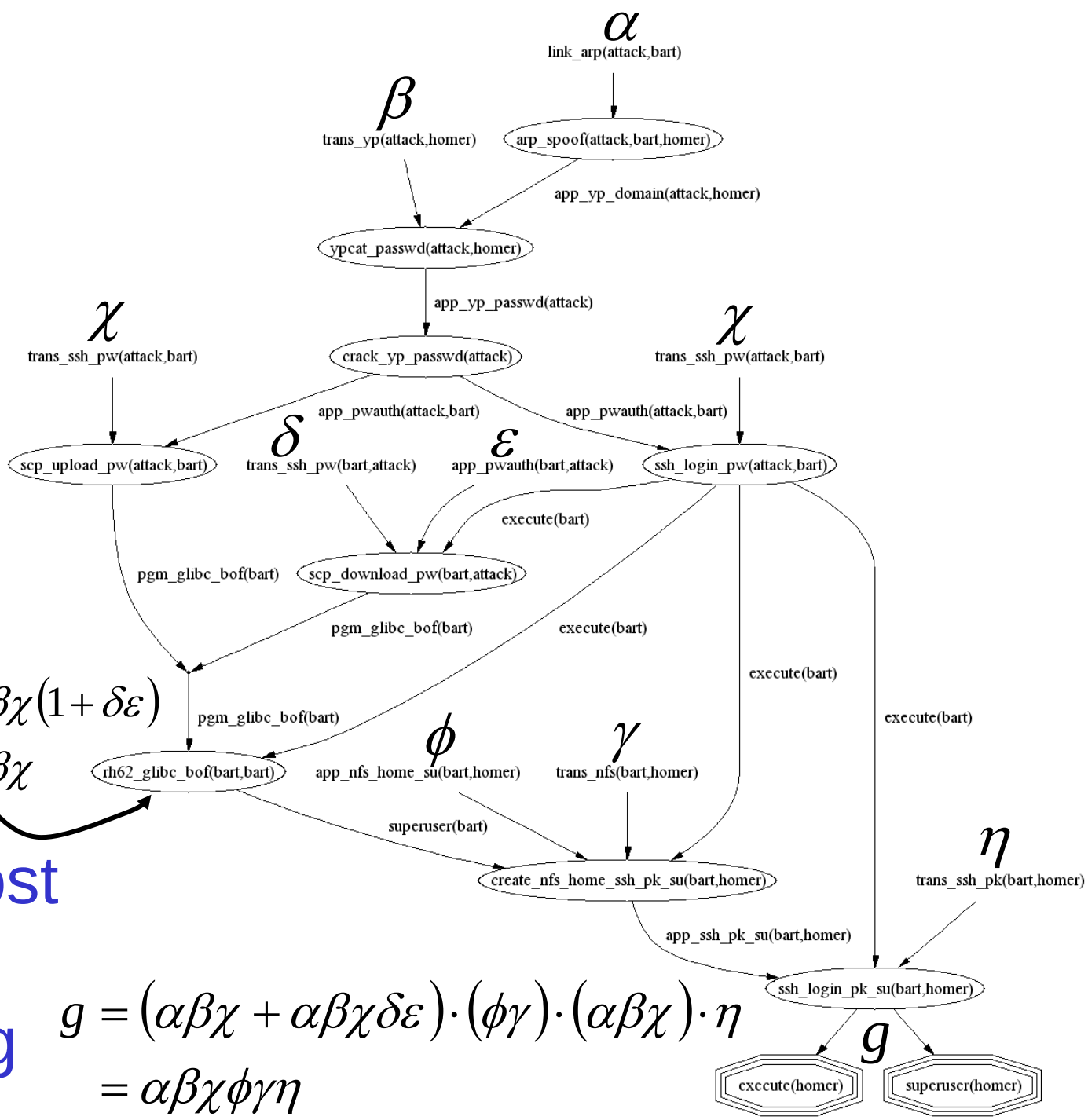

nessus.10671(attack,web)
execute(attack)
nessus.10537(attack,web)
nessus.10357(attack,web)
iis_decode_bug(attack,web)
iis_dir_traversal(attack,web)
msadcs_dll(attack,web)
nessus.10168(web,mail)
nessus.10280(web,mail)
execute(web)
nessus.10205(web,mail)
nessus.10452(web,mail)
ntalk_detect(web,mail)
telnet(web,mail)
rlogin(web,mail)
wu_ftpd_site_exec(web,mail)
nessus.10452(mail,mail)
execute(mail)
execute(mail)
nessus.10168(mail,mail)
wu_ftpd_site_exec(mail,mail)
ntalk_detect(mail,mail)
superuser(mail)


nessus.10671(attack,web)
execute(attack)
nessus.10537(attack,web)
nessus.10357(attack,web)
iis_decode_bug(attack,web)
iis_dir_traversal(attack,web)
msadcs_dll(attack,web)
execute(web)


nessus.10671(attack,web)
execute(attack)
nessus.10537(attack,web)
nessus.10357(attack,web)
iis_decode_bug(attack,web)
iis_dir_traversal(attack,web)
msadcs_dll(attack,web)
nessus.10168(web,mail)
execute(web)
nessus.10452(web,mail)
ntalk_detect(web,mail)
wu_ftpd_site_exec(web,mail)
execute(mail)
superuser(mail)


nessus.10671(attack,web)
execute(attack)
nessus.10537(attack,web)
nessus.10357(attack,web)
iis_decode_bug(attack,web)
iis_dir_traversal(attack,web)
msadcs_dll(attack,web)
nessus.10168(web,mail)
nessus.10280(web,mail)
execute(web)
nessus.10205(web,mail)
nessus.10452(web,mail)
ntalk_detect(web,mail)
telnet(web,mail)
rlogin(web,mail)
wu_ftpd_site_exec(web,mail)
execute(mail)
execute(mail)
superuser(mail)

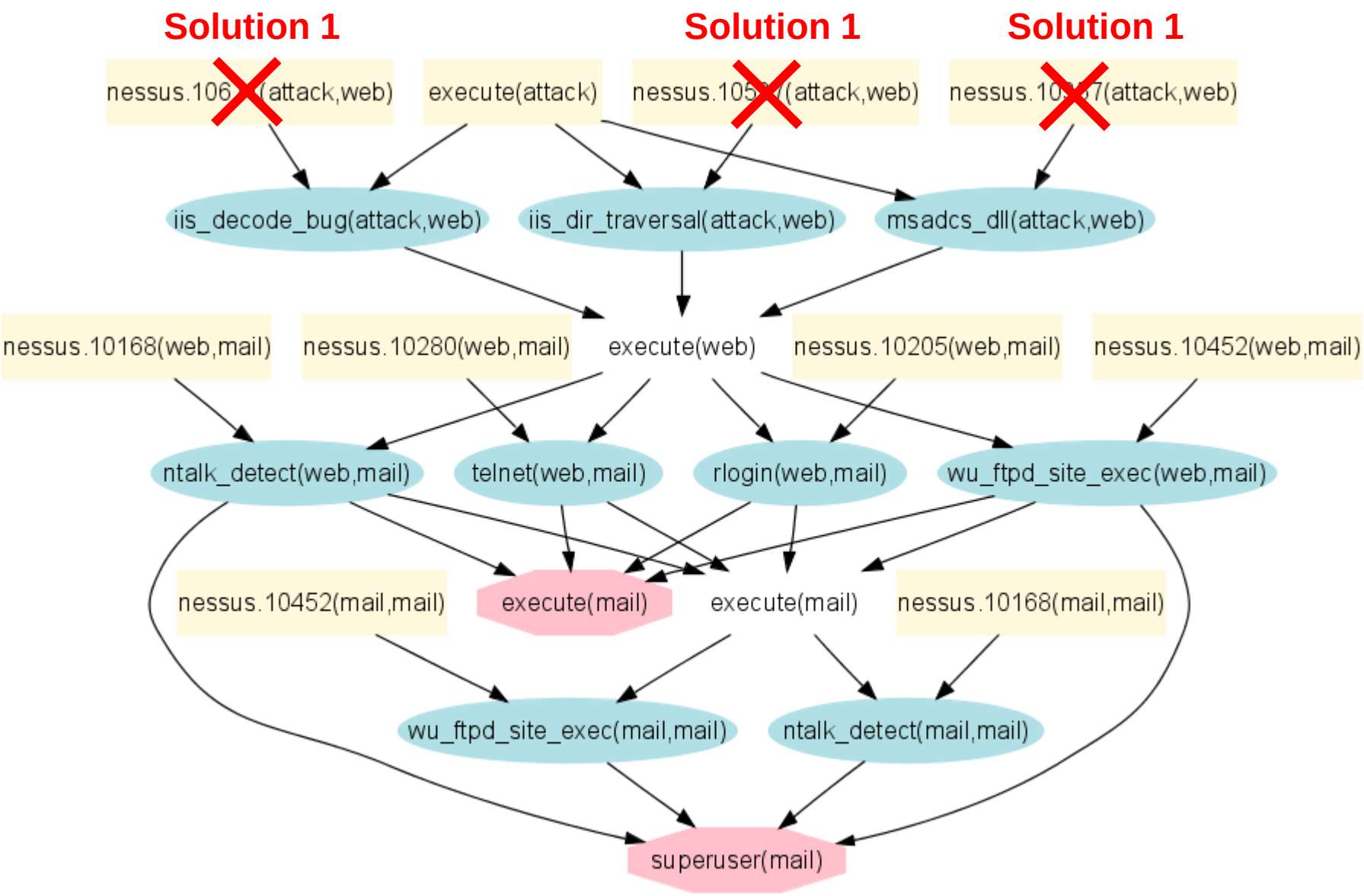

nessus.10671(attack,web)
execute(attack)
nessus.10537(attack,web)
nessus.10357(attack,web)
iis_decode_bug(attack,web)
iis_dir_traversal(attack,web)
msadcs_dll(attack,web)
nessus.10168(web,mail)
nessus.10280(web,mail)
execute(web)
nessus.10205(web,mail)
nessus.10452(web,mail)
ntalk_detect(web,mail)
telnet(web,mail)
rlogin(web,mail)
wu_ftpd_site_exec(web,mail)
nessus.10452(mail,mail)
execute(mail)
execute(mail)
nessus.10168(mail,mail)
wu_ftpd_site_exec(mail,mail)
ntalk_detect(mail,mail)
superuser(mail)

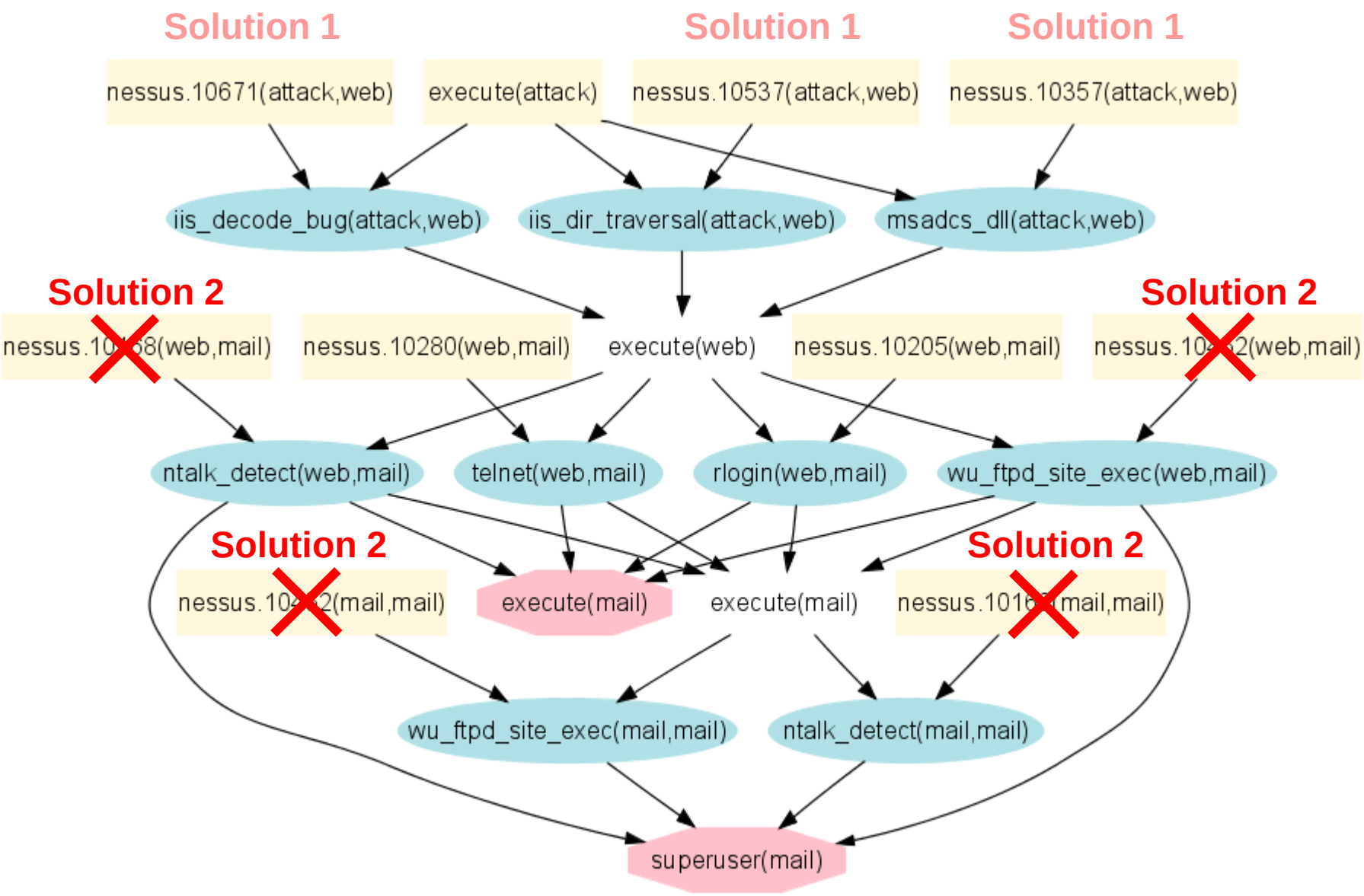


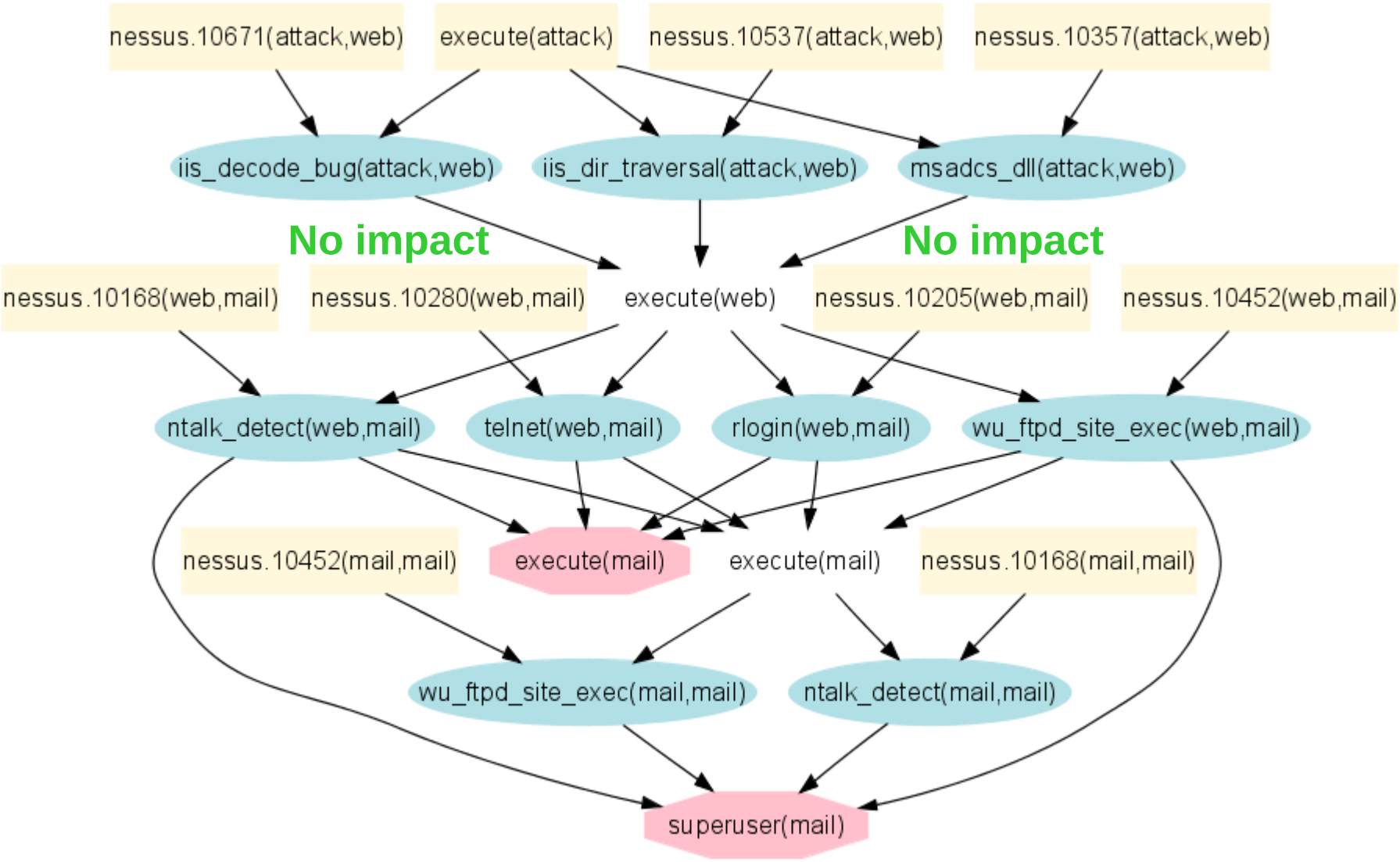
$$\alpha\beta\chi + \alpha\beta\chi\delta\varepsilon = \alpha\beta\chi(1+\delta\varepsilon)$$
$$= \alpha\beta\chi$$

Minimal-Cost Network Hardening

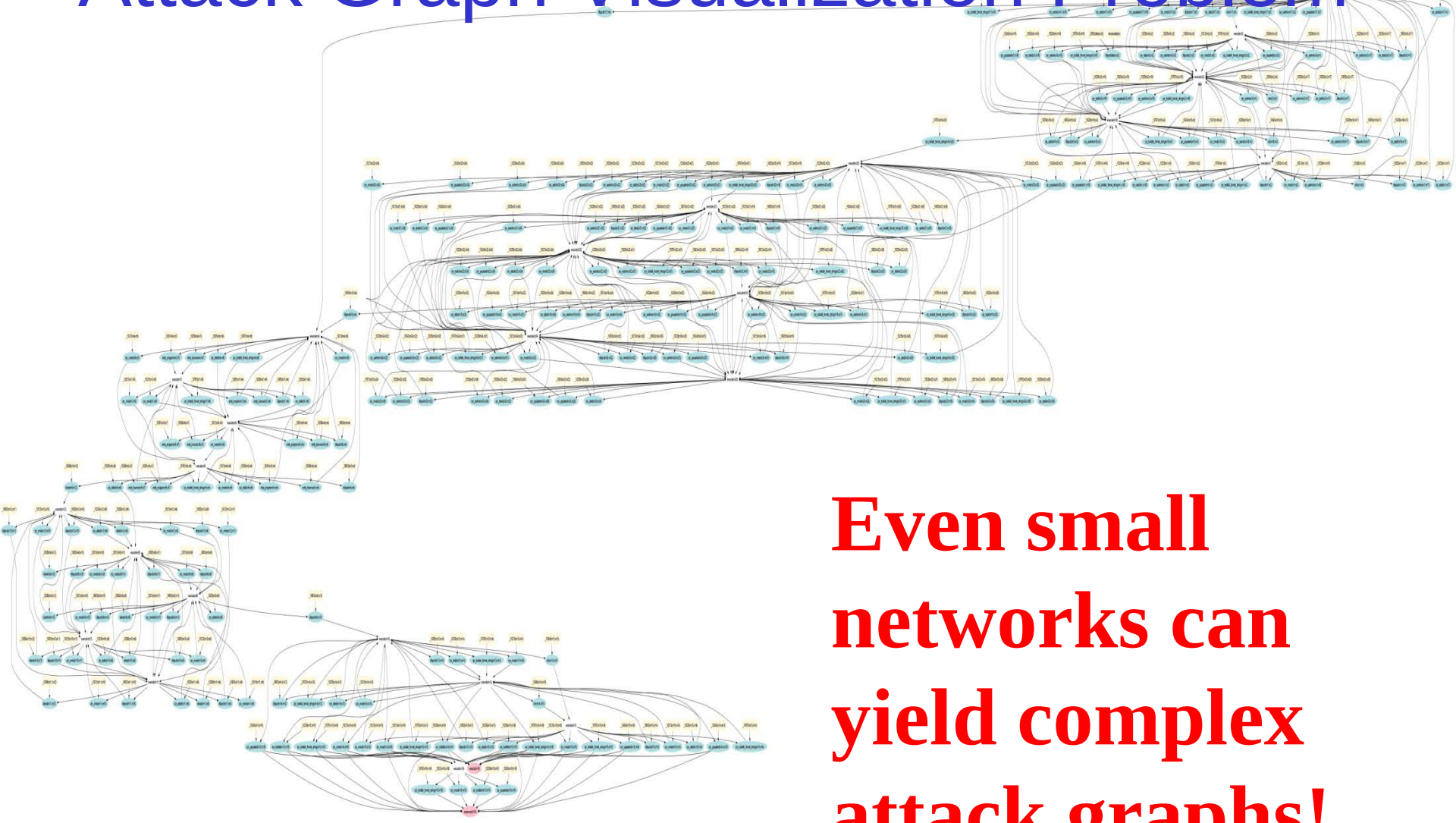
$$g = (\alpha\beta\chi + \alpha\beta\chi\delta\varepsilon)\cdot(\phi\gamma)\cdot(\alpha\beta\chi)\cdot\eta$$
$$= \alpha\beta\chi\phi\gamma\eta$$


Solution 1
Solution 1
Solution 1
nessus.106 (attack,web)
execute(attack)
nessus.105 (attack,web)
nessus.10 7(attack,web)
iis_decode_bug(attack,web)
iis_dir_traversal(attack,web)
msadcs_dll(attack,web)
nessus.10168(web,mail)
nessus.10280(web,mail)
execute(web)
nessus.10205(web,mail)
nessus.10452(web,mail)
ntalk_detect(web,mail)
telnet(web,mail)
rlogin(web,mail)
wu_ftpd_site_exec(web,mail)
nessus.10452(mail,mail)
execute(mail)
execute(mail)
nessus.10168(mail,mail)
wu_ftpd_site_exec(mail,mail)
ntalk_detect(mail,mail)
superuser(mail)

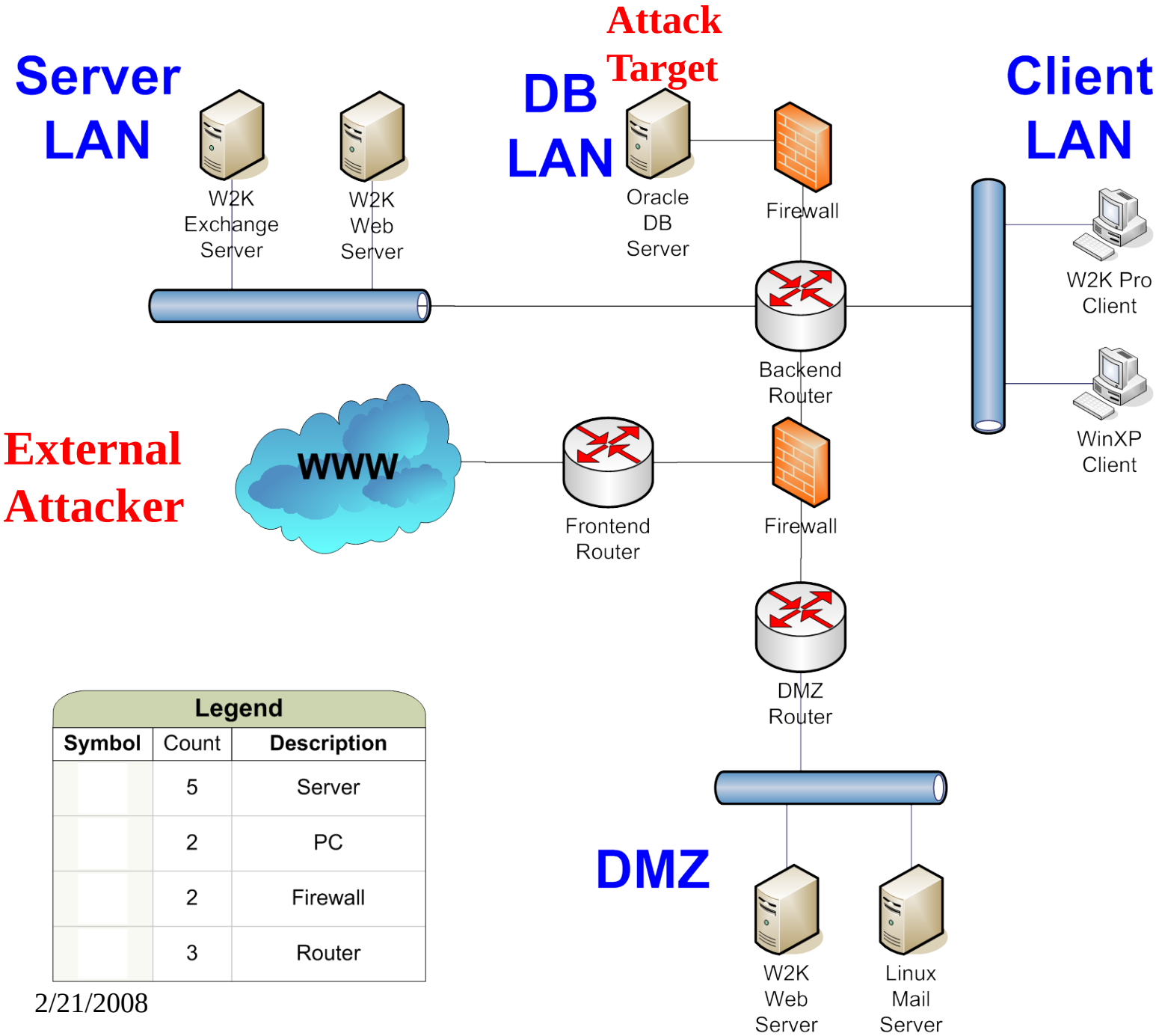

Solution 1
Solution 1
Solution 1
nessus.10671(attack,web)
execute(attack)
nessus.10537(attack,web)
nessus.10357(attack,web)
iis_decode_bug(attack,web)
iis_dir_traversal(attack,web)
msadcs_dll(attack,web)
Solution 2
Solution 2
nessus.10280(web,mail)
execute(web)
nessus.10205(web,mail)
ntalk_detect(web,mail)
telnet(web,mail)
rlogin(web,mail)
wu_ftpd_site_exec(web,mail)
Solution 2
Solution 2
execute(mail)
execute(mail)
wu_ftpd_site_exec(mail,mail)
ntalk_detect(mail,mail)
superuser(mail)


nessus.10671(attack,web)
execute(attack)
nessus.10537(attack,web)
nessus.10357(attack,web)
iis_decode_bug(attack,web)
iis_dir_traversal(attack,web)
msadcs_dll(attack,web)
No impact
No impact
nessus.10168(web,mail)
nessus.10280(web,mail)
execute(web)
nessus.10205(web,mail)
nessus.10452(web,mail)
ntalk_detect(web,mail)
telnet(web,mail)
rlogin(web,mail)
wu_ftpd_site_exec(web,mail)
nessus.10452(mail,mail)
execute(mail)
execute(mail)
nessus.10168(mail,mail)
wu_ftpd_site_exec(mail,mail)
ntalk_detect(mail,mail)
superuser(mail)

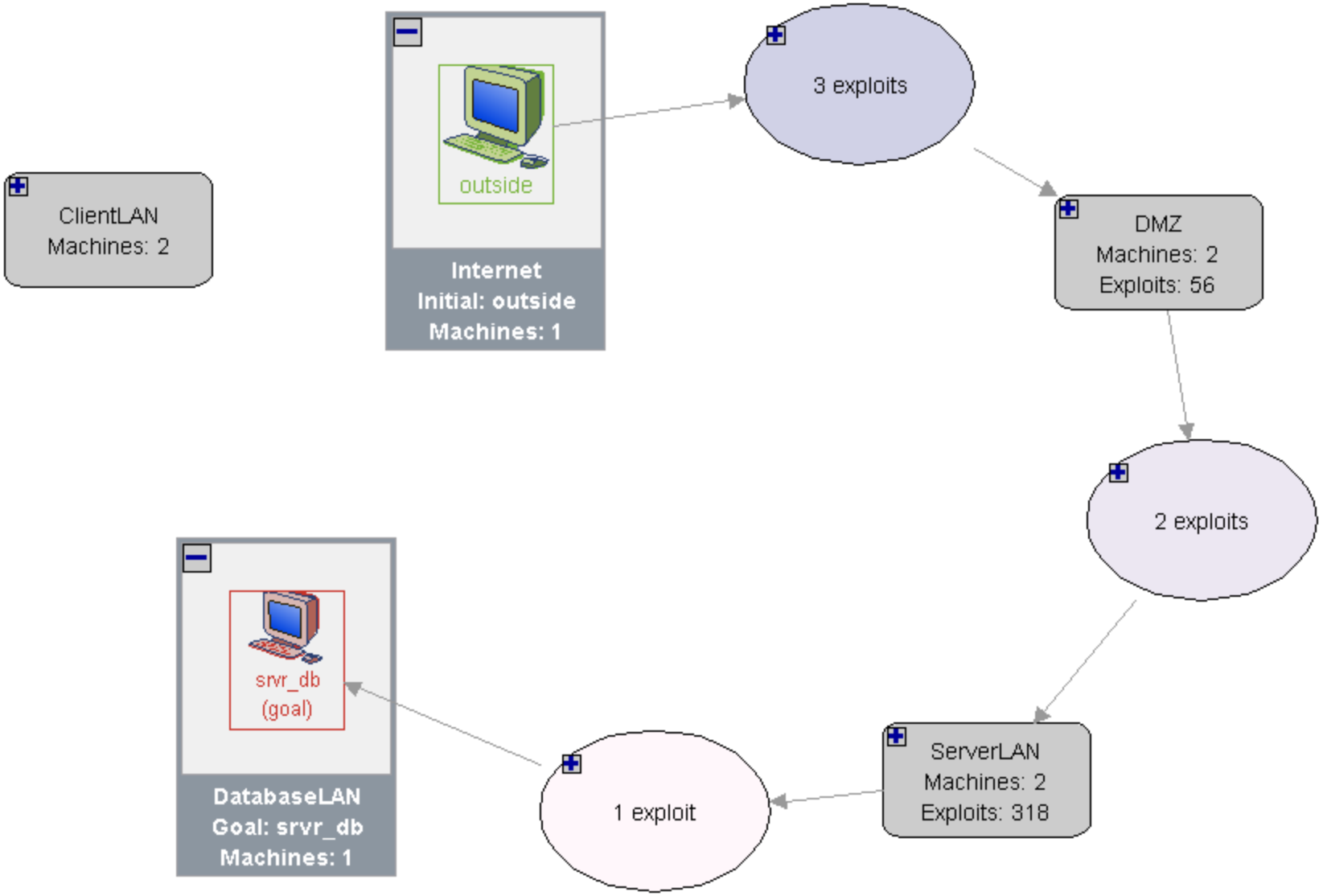
Attack Graph Visualization Problem

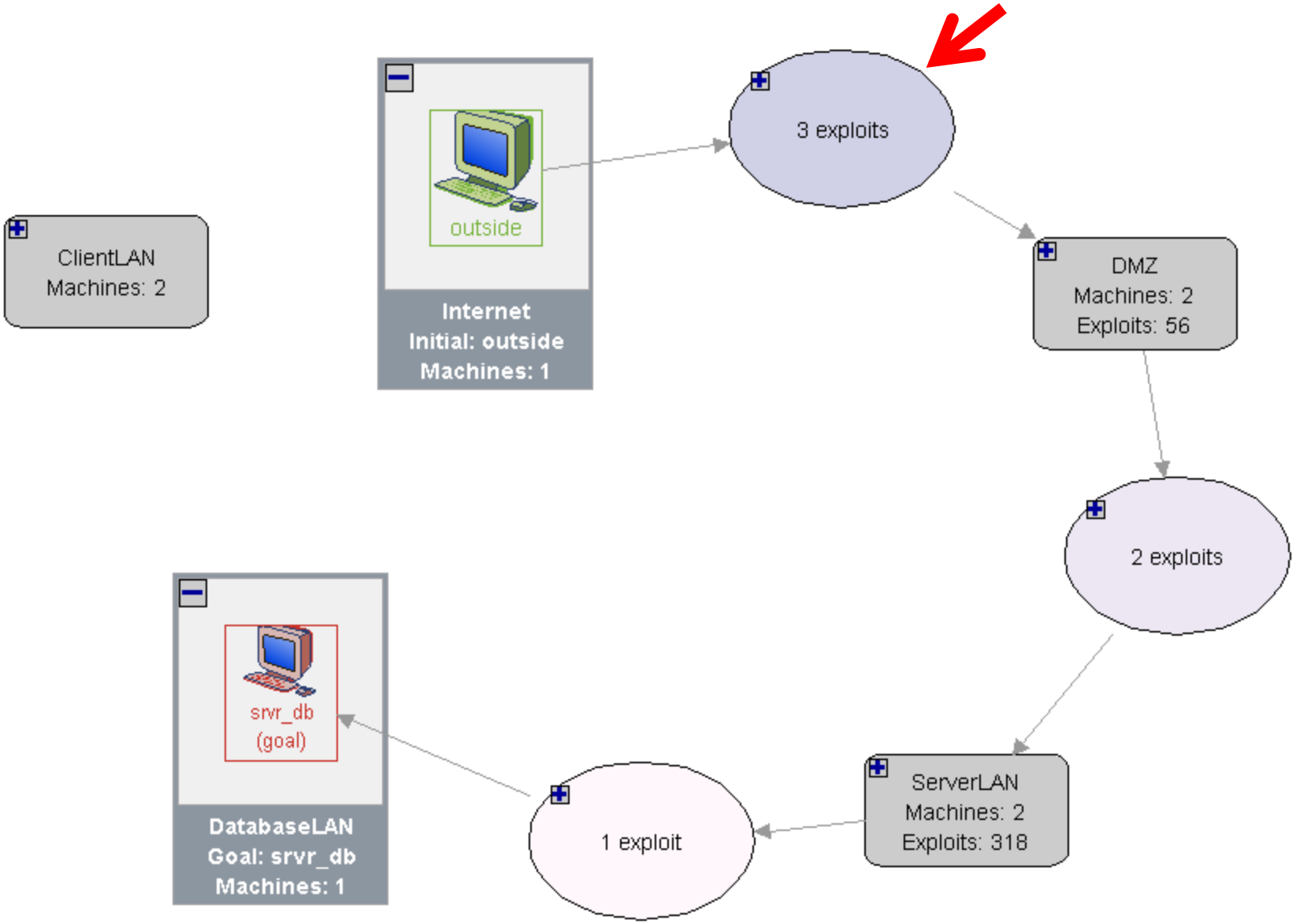


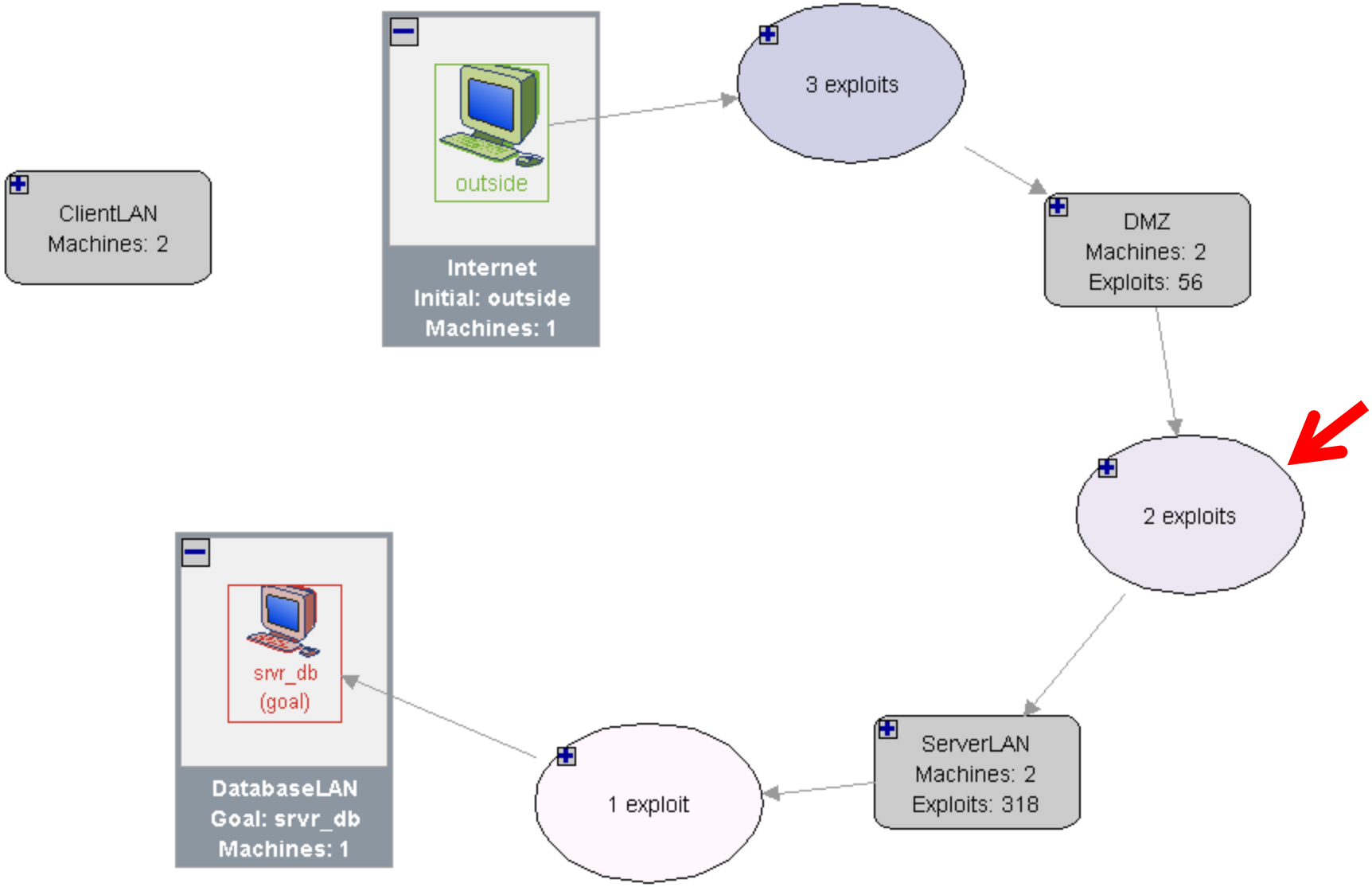
Even small networks can yield complex attack graphs!

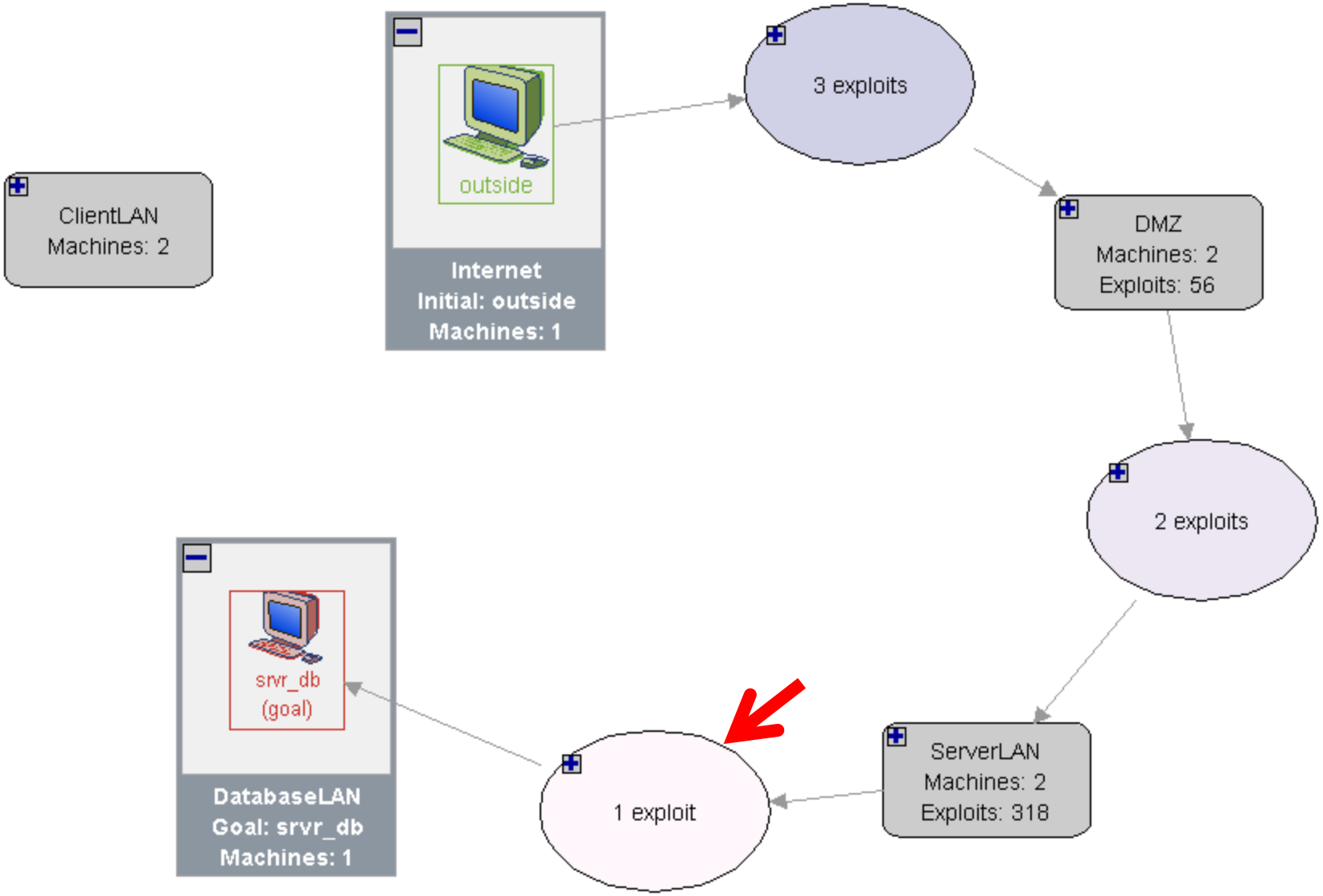


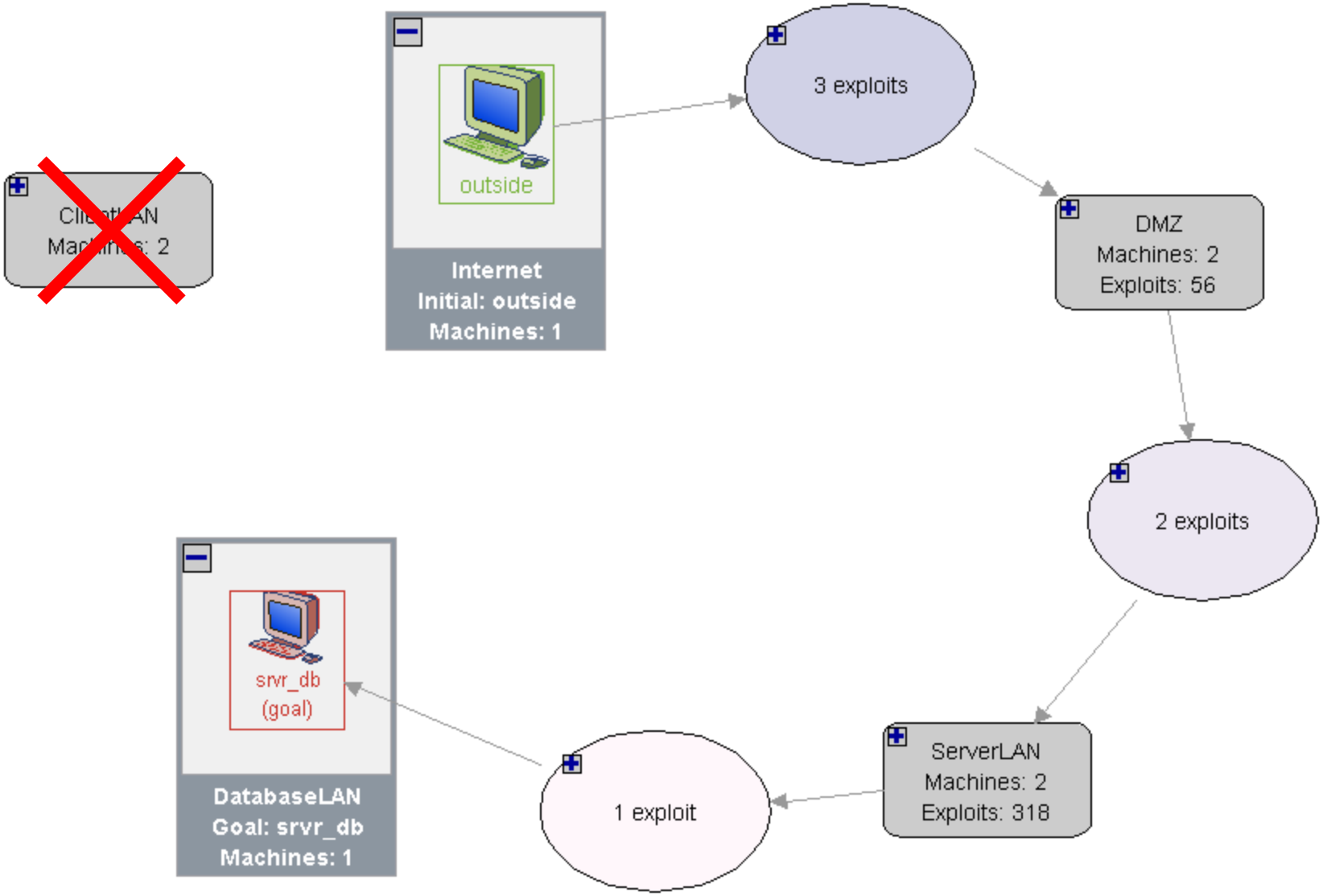
Legend		
Symbol	Count	Description
	5	Server
	2	PC
	2	Firewall
	3	Router


ClientLAN
Machines: 2
outside
Internet
Initial: outside
Machines: 1
3 exploits
DMZ
Machines: 2
Exploits: 56
2 exploits
ServerLAN
Machines: 2
Exploits: 318
1 exploit
srvr_db
(goal)
DatabaseLAN
Goal: srvr_db
Machines: 1


ClientLAN
Machines: 2
outside
Internet
Initial: outside
Machines: 1
3 exploits
DMZ
Machines: 2
Exploits: 56
2 exploits
ServerLAN
Machines: 2
Exploits: 318
1 exploit
srvr_db
(goal)
DatabaseLAN
Goal: srvr_db
Machines: 1


ClientLAN
Machines: 2
outside
Internet
Initial: outside
Machines: 1
3 exploits
DMZ
Machines: 2
Exploits: 56
2 exploits
ServerLAN
Machines: 2
Exploits: 318
1 exploit
srvr_db
(goal)
DatabaseLAN
Goal: srvr_db
Machines: 1

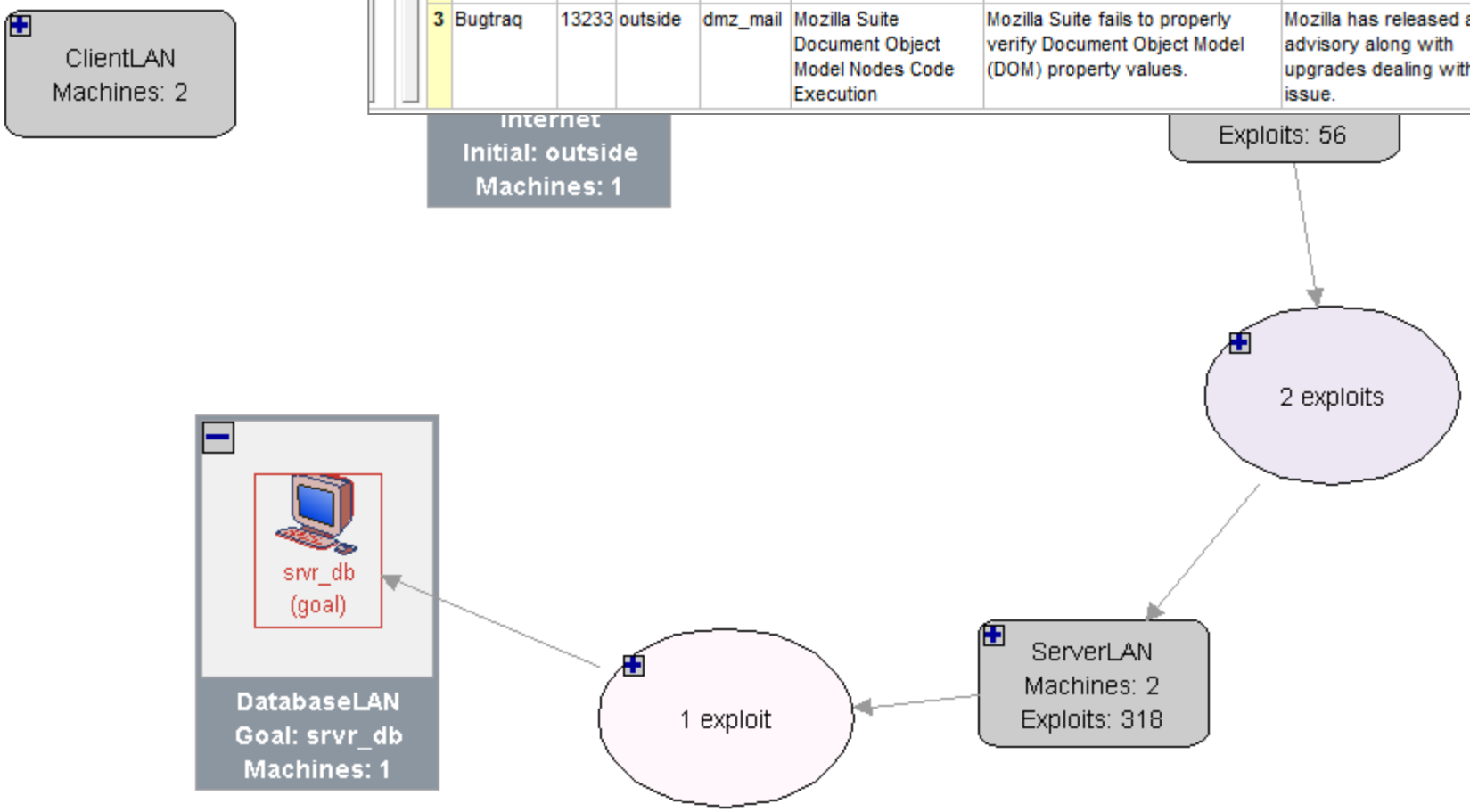

ClientLAN
Machines: 2
outside
Internet
Initial: outside
Machines: 1
3 exploits
DMZ
Machines: 2
Exploits: 56
2 exploits
ServerLAN
Machines: 2
Exploits: 318
1 exploit
srvr_db
(goal)
DatabaseLAN
Goal: srvr_db
Machines: 1

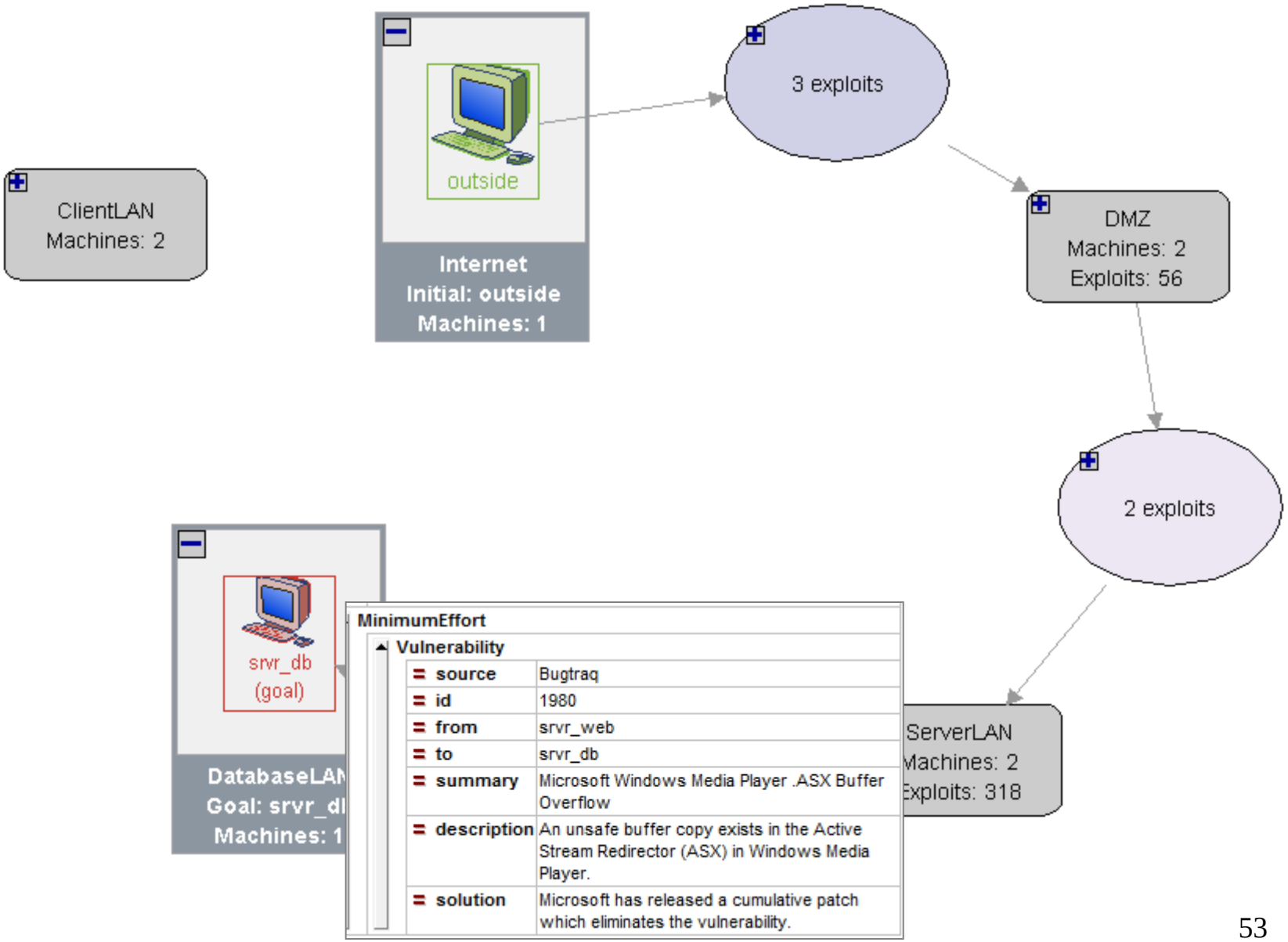

ClientLAN
Machines: 2
outside
Internet
Initial: outside
Machines: 1
3 exploits
DMZ
Machines: 2
Exploits: 56
2 exploits
ServerLAN
Machines: 2
Exploits: 318
1 exploit
srvr_db
(goal)
DatabaseLAN
Goal: srvr_db
Machines: 1

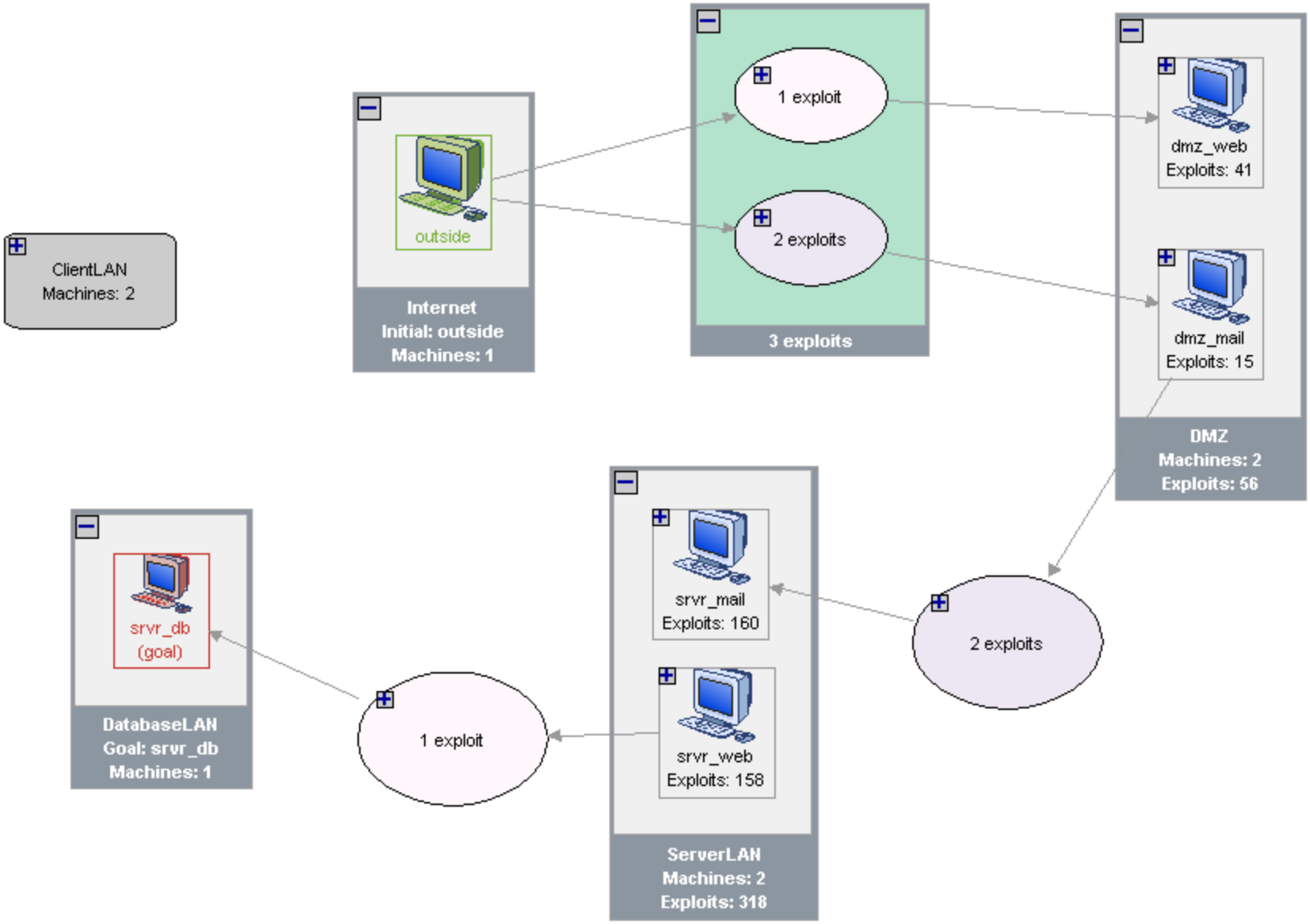
FirstLayer

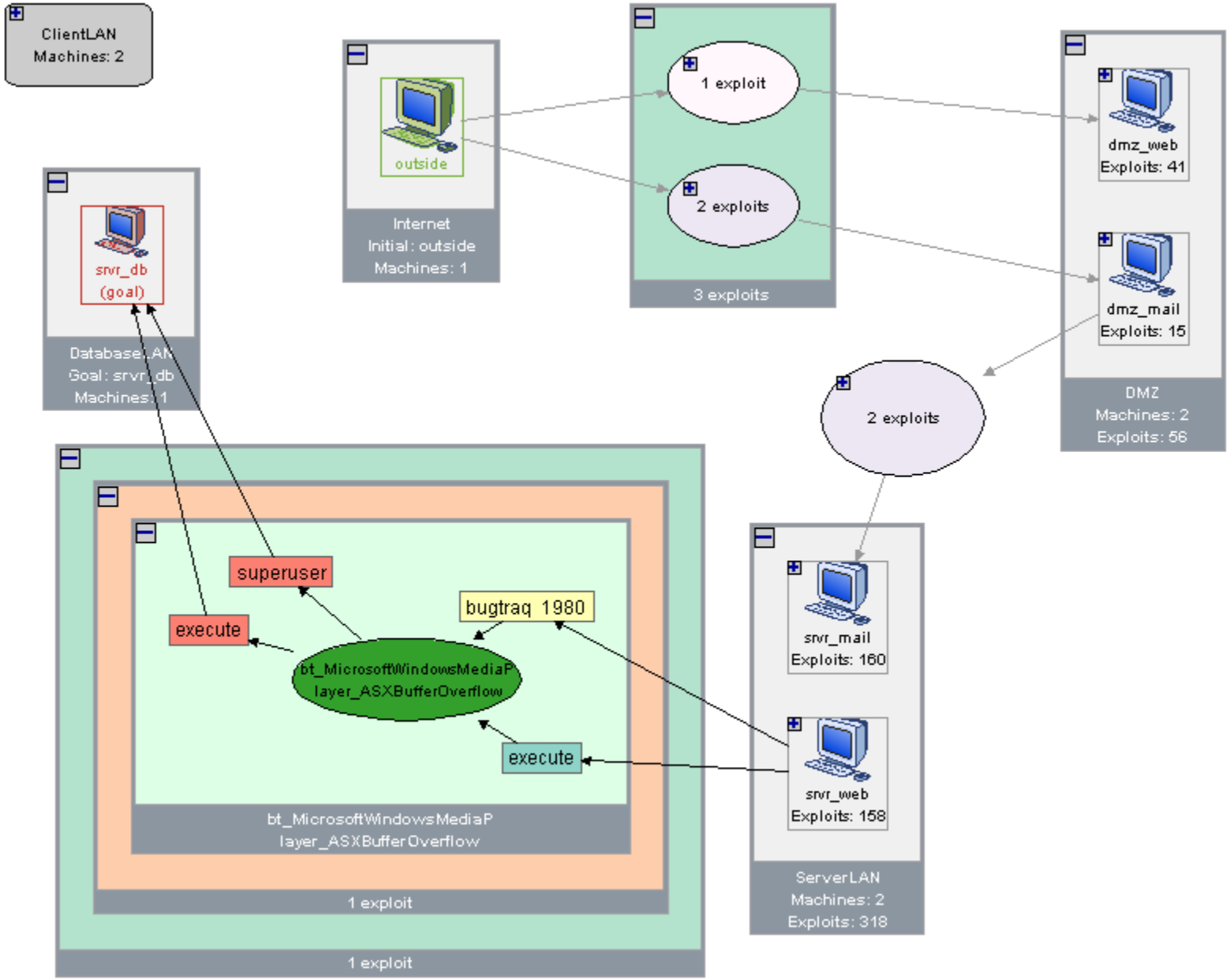
Vulnerability (3)

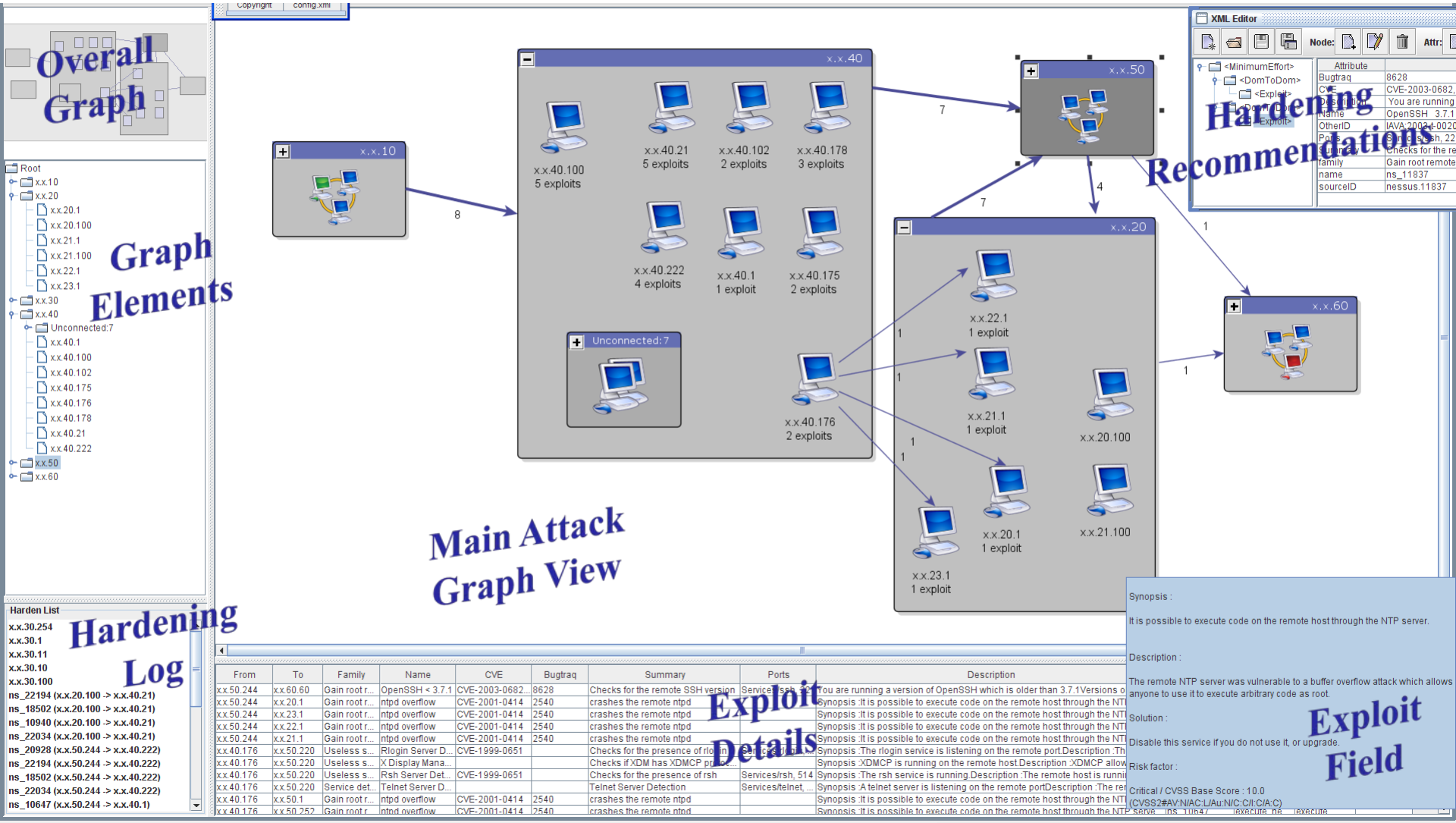
	source	id	from	to	summary	description	solution
1	Bugtraq	1980	outside	dmz_web	Microsoft Windows Media Player .ASX Buffer Overflow	An unsafe buffer copy exists in the Active Stream Redirector (ASX) in Windows Media Player.	Microsoft has released a cumulative patch which eliminates the vulnerability.
2	Bugtraq	13232	outside	dmz_mail	Mozilla Suite XPInstall JavaScript Object Instance Validation	Mozilla Suite fails to verify input passed to installation objects.	Mozilla has released an advisory along with upgrades dealing with this issue.
3	Bugtraq	13233	outside	dmz_mail	Mozilla Suite Document Object Model Nodes Code Execution	Mozilla Suite fails to properly verify Document Object Model (DOM) property values.	Mozilla has released an advisory along with upgrades dealing with this issue.

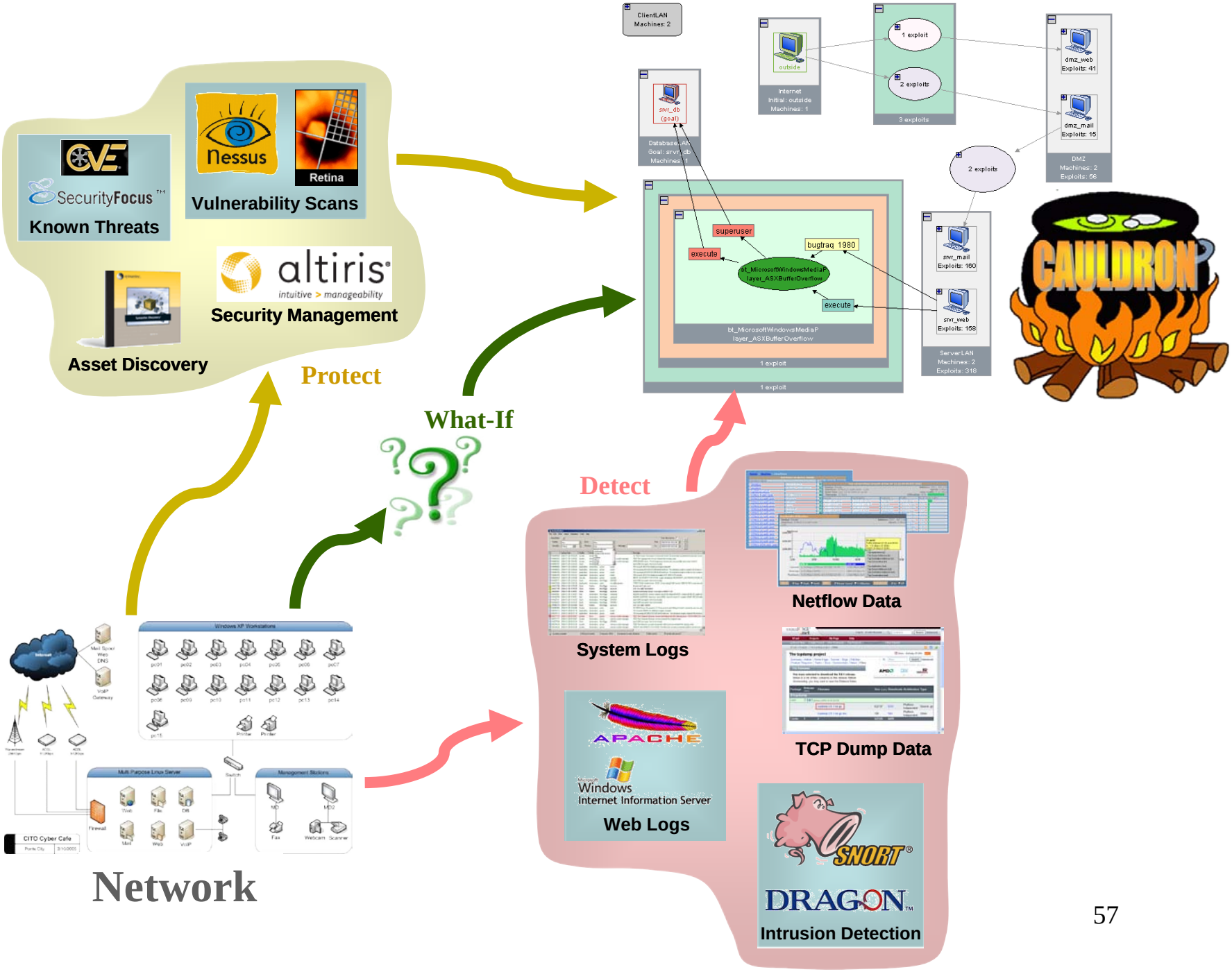



ClientLAN
Machines: 2
outside
Internet
Initial: outside
Machines: 1
3 exploits
DMZ
Machines: 2
Exploits: 56
2 exploits
srvr_db
(goal)
DatabaseLAN
Goal: srvr_db
Machines: 1
ServerLAN
Machines: 2
Exploits: 318
MinimumEffort
Vulnerability
source Bugtraq
id 1980
from srvr_web
to srvr_db
summary Microsoft Windows Media Player .ASX Buffer Overflow
description An unsafe buffer copy exists in the Active Stream Redirector (ASX) in Windows Media Player.
solution Microsoft has released a cumulative patch which eliminates the vulnerability.


ClientLAN
Machines: 2
outside
Internet
Initial: outside
Machines: 1
1 exploit
2 exploits
3 exploits
dmz_web
Exploits: 41
dmz_mail
Exploits: 15
DMZ
Machines: 2
Exploits: 56
srvr_db
(goal)
DatabaseLAN
Goal: srvr_db
Machines: 1
1 exploit
srvr_mail
Exploits: 160
srvr_web
Exploits: 158
ServerLAN
Machines: 2
Exploits: 318
2 exploits


ClientLAN
Machines: 2
outside
Internet
Initial: outside
Machines: 1
1 exploit
2 exploits
3 exploits
dmz_web
Exploits: 41
dmz_mail
Exploits: 15
DMZ
Machines: 2
Exploits: 56
srvr_db
(goal)
Database_AN
Goal: srvr_db
Machines: 1
2 exploits
superuser
bugtraq_1980
execute
bt_MicrosoftWindowsMediaP
layer_ASXBufferOverflow
execute
bt_MicrosoftWindowsMediaP
layer_ASXBufferOverflow
1 exploit
1 exploit
srvr_mail
Exploits: 160
srvr_web
Exploits: 158
ServerLAN
Machines: 2
Exploits: 318

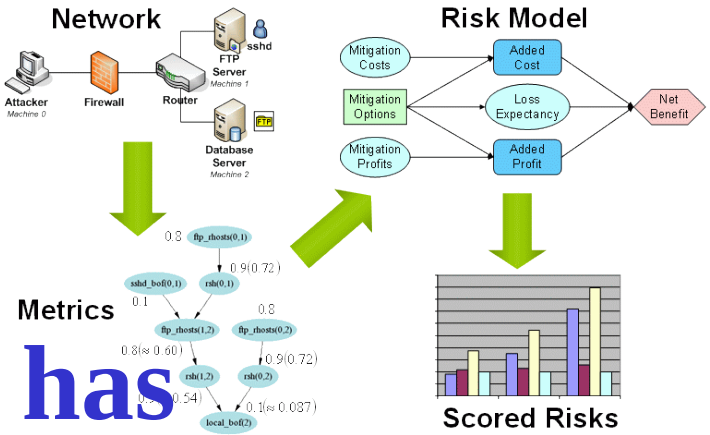

Overall Graph
Graph Elements
Main Attack Graph View
Hardening Log
Exploit Details
Exploit Field
Hardening Recommendations
x.x.10
x.x.40
x.x.50
x.x.20
x.x.60
Unconnected:7
x.x.40.100 5 exploits
x.x.40.21 5 exploits
x.x.40.102 2 exploits
x.x.40.178 3 exploits
x.x.40.222 4 exploits
x.x.40.1 1 exploit
x.x.40.175 2 exploits
x.x.40.176 2 exploits
x.x.22.1 1 exploit
x.x.21.1 1 exploit
x.x.20.100
x.x.20.1 1 exploit
x.x.21.100
x.x.23.1 1 exploit
XML Editor
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)

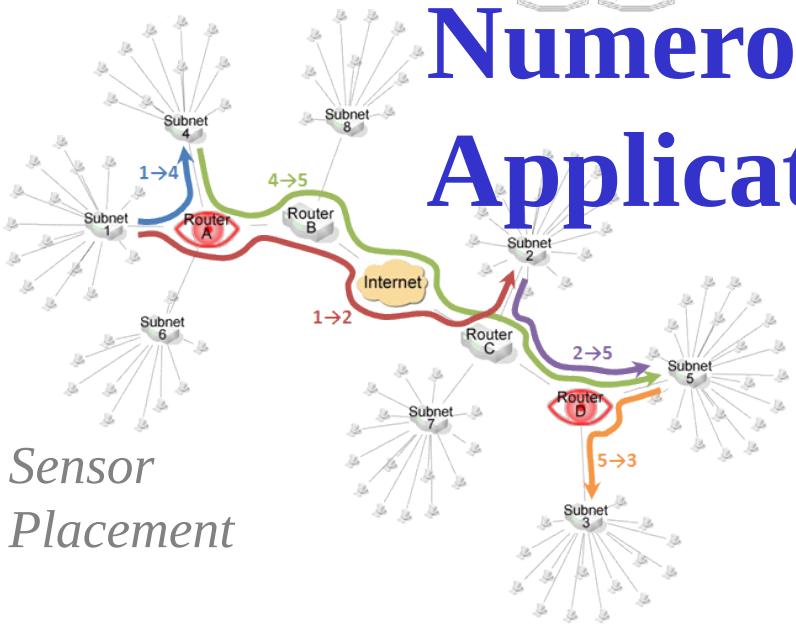

Known Threats
Vulnerability Scans
Security Management
Asset Discovery
Protect
What-If
Detect
Network
System Logs
Netflow Data
TCP Dump Data
Web Logs
Intrusion Detection
CAULDRON

CAULDRON has Numerous Applications

Network Hardening

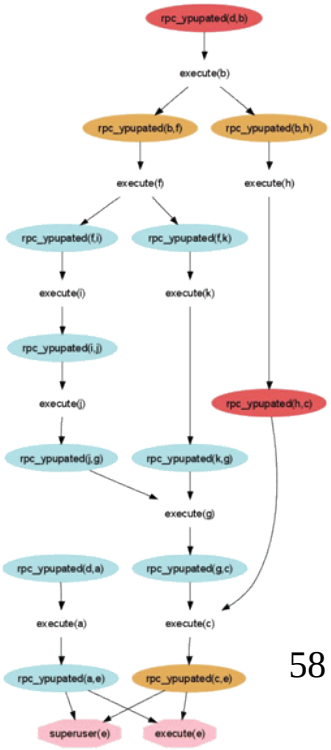
Security Metrics



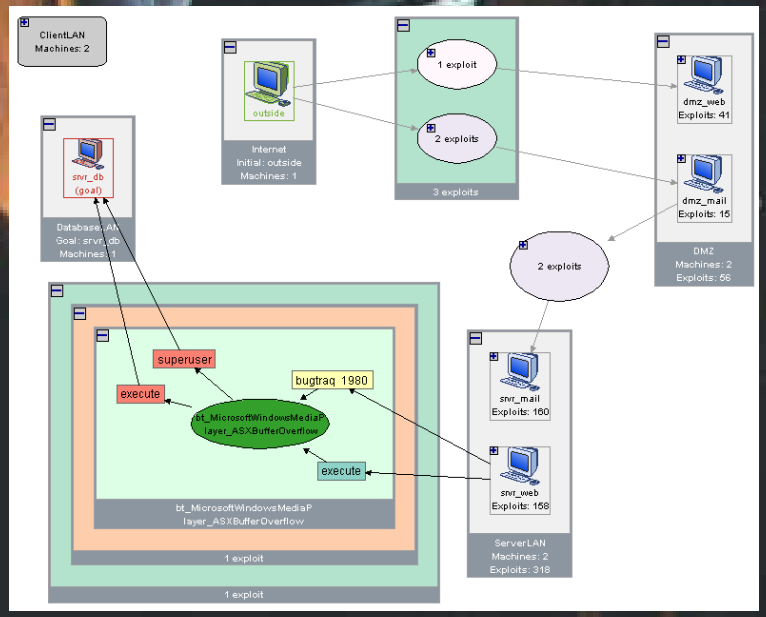


Sensor Placement

Alarm Correlation And Attack Response



FAA CSIRC Deployment, Leesburg, VA

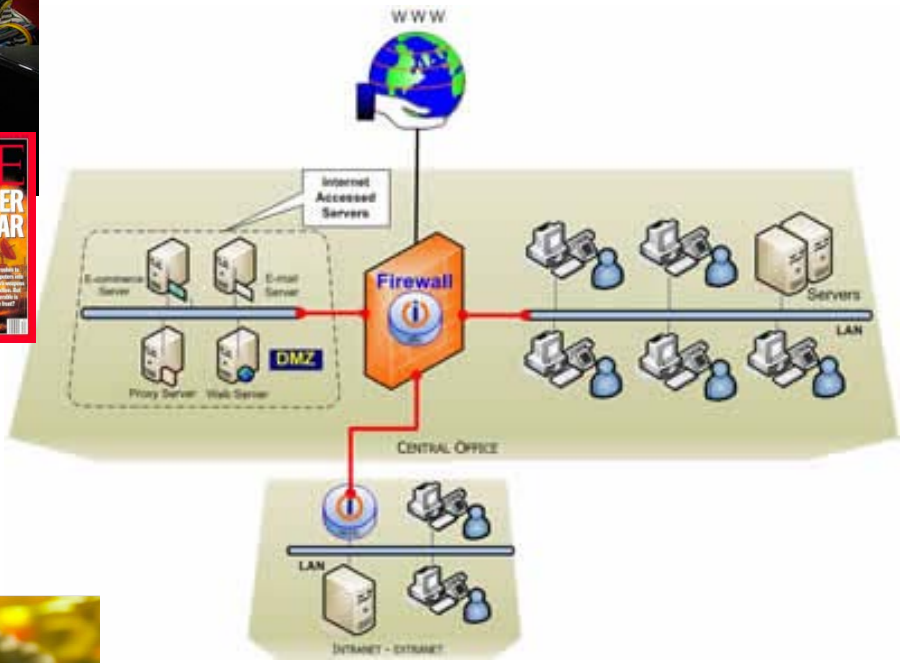


FAA

Final Remarks

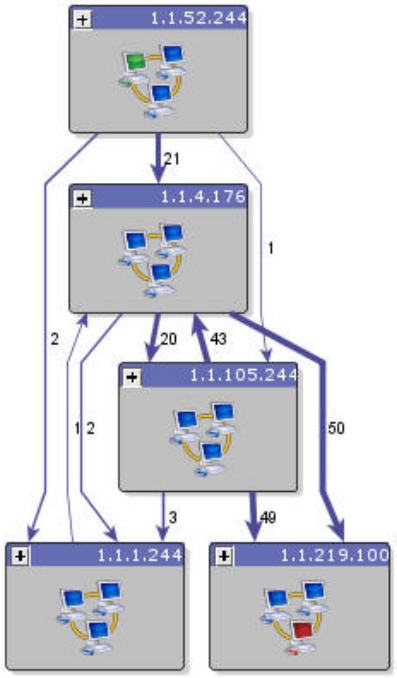
- Not a silver bullet
- Can help with
  - Attack prevention
  - Forensic analysis
  - Multi-step attack correlation
  - Attack prediction
  - Attack response

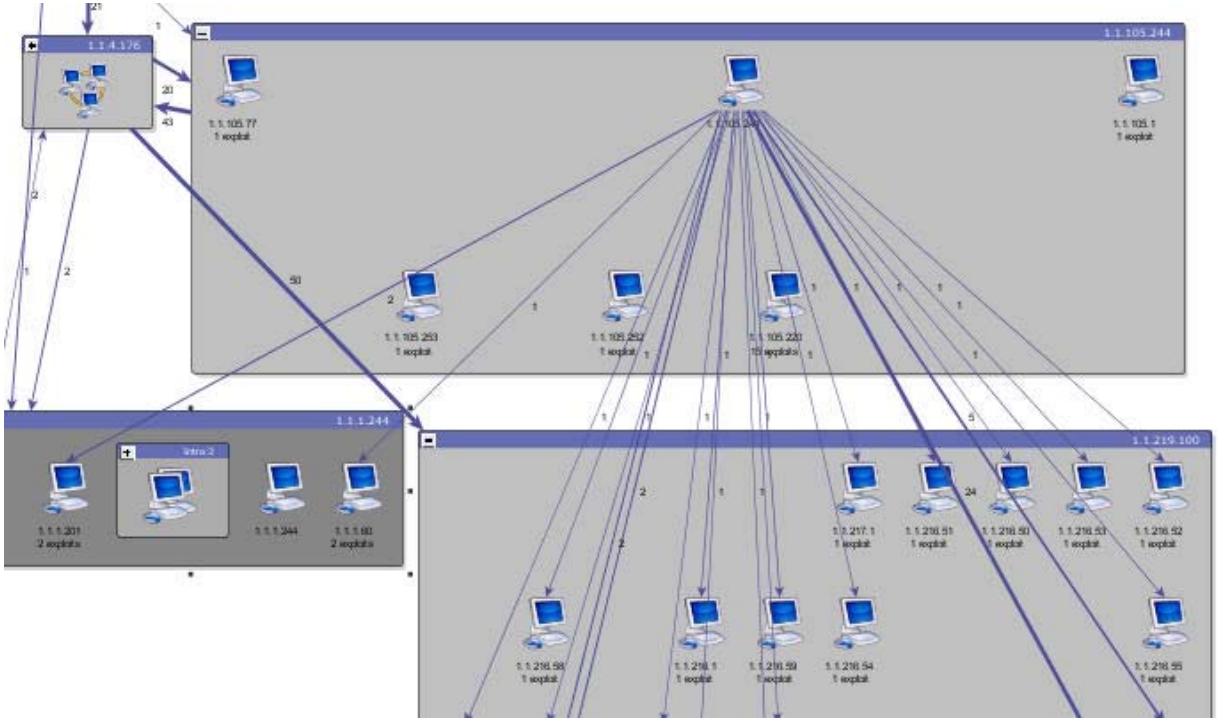
Threats vs. Vulnerabilities



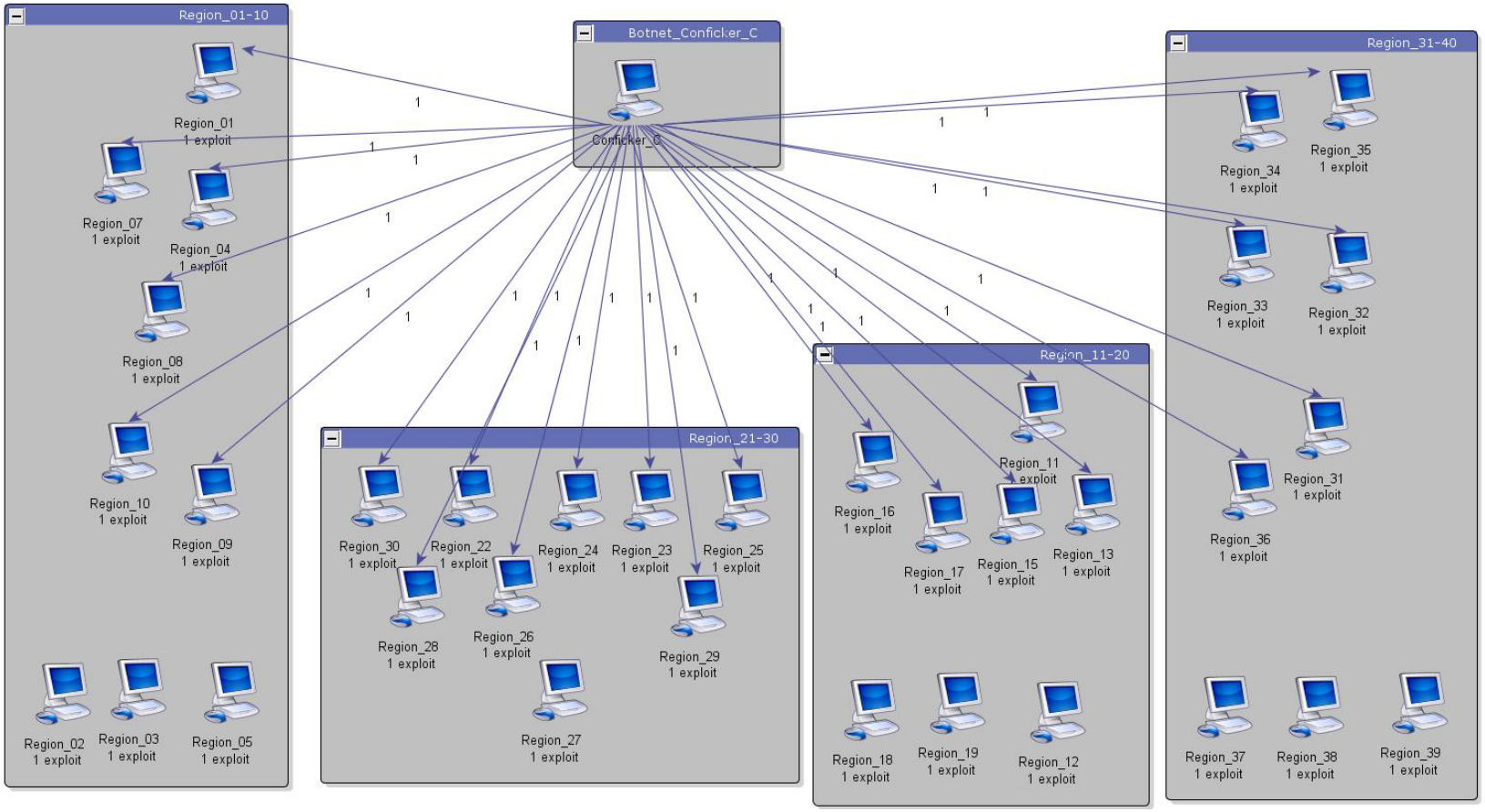
Challenge isn’t getting easier

Understand What's Inside the Environment



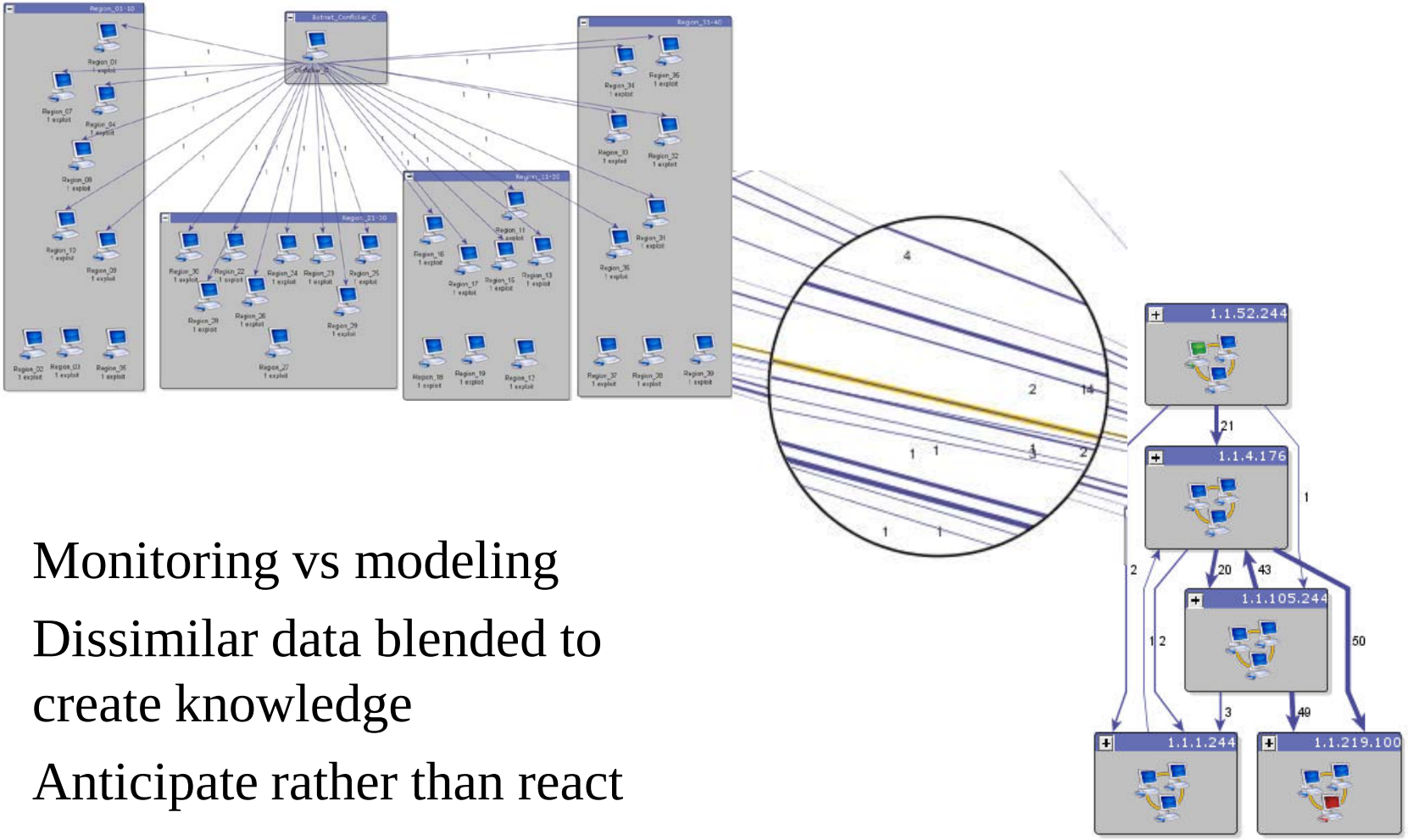


And the Outside World



Malcode, botnets and other systems that may not communicate directly with your assets can still have an impact on your operations.

And Plan Where to Focus Your Efforts



- Monitoring vs modeling
- Dissimilar data blended to create knowledge
- Anticipate rather than react

Further Information:

Sushil Jajodia

jajodia@gmu.edu

(703) 993-1653

http://csis.gmu.edu/jajodia