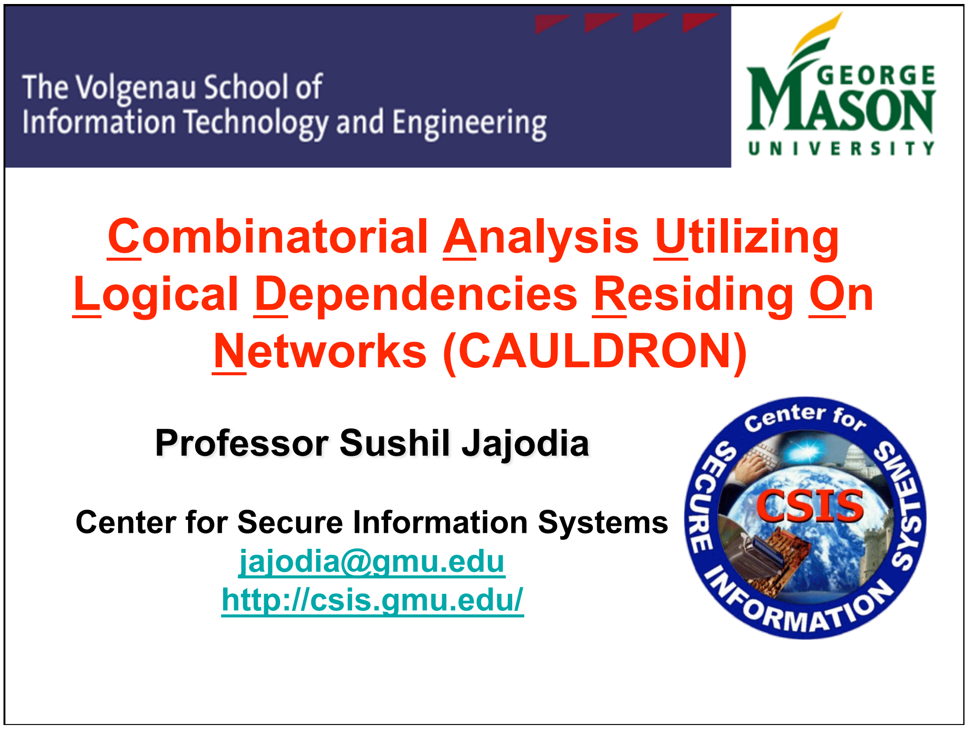


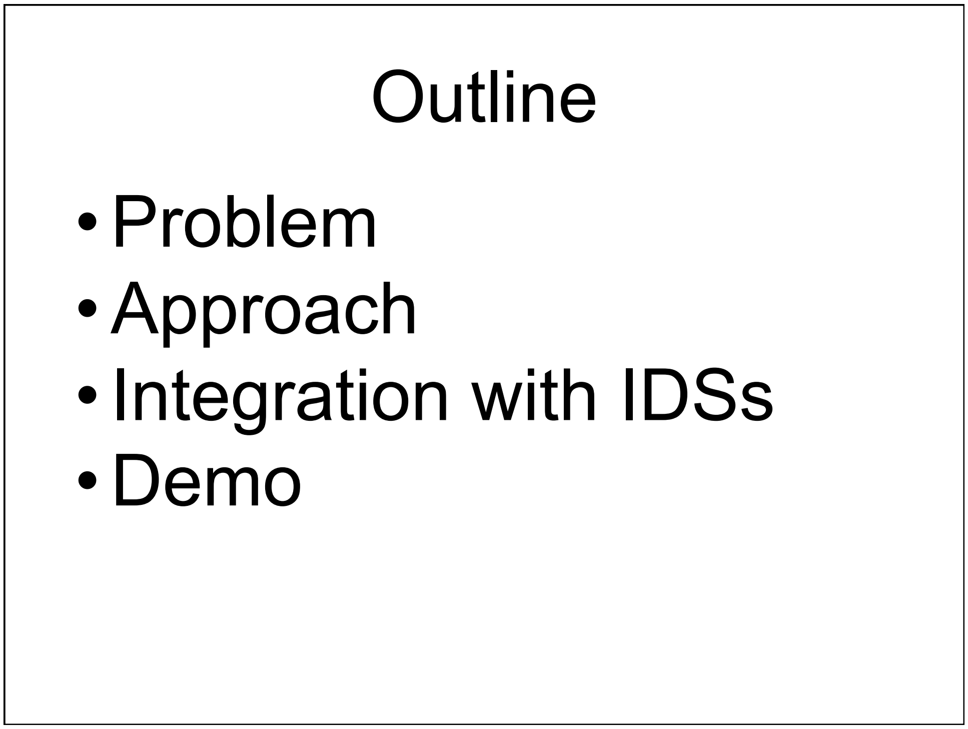
The Volgenau School of Information Technology and Engineering

GEORGE MASON UNIVERSITY

Combinatorial Analysis Utilizing Logical Dependencies Residing On Networks (CAULDRON)

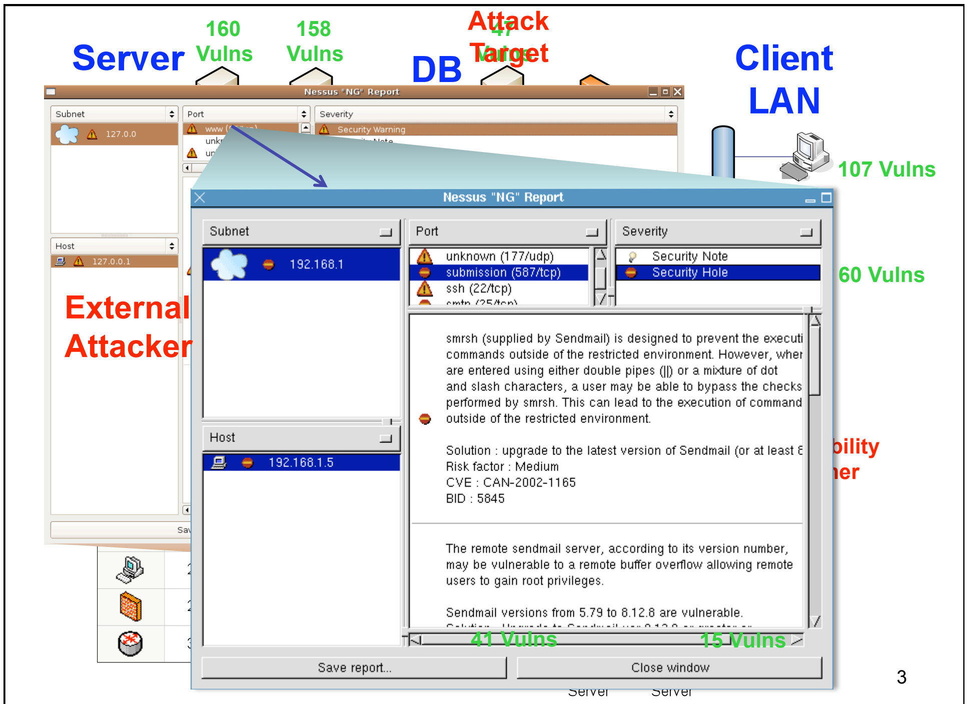
Professor Sushil Jajodia

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



Outline

- Problem
- Approach
- Integration with IDSs
- Demo



- unknown (177/udp)
- submission (587/tcp)
- ssh (22/tcp)
- smtp (25/tcp)

- 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.

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

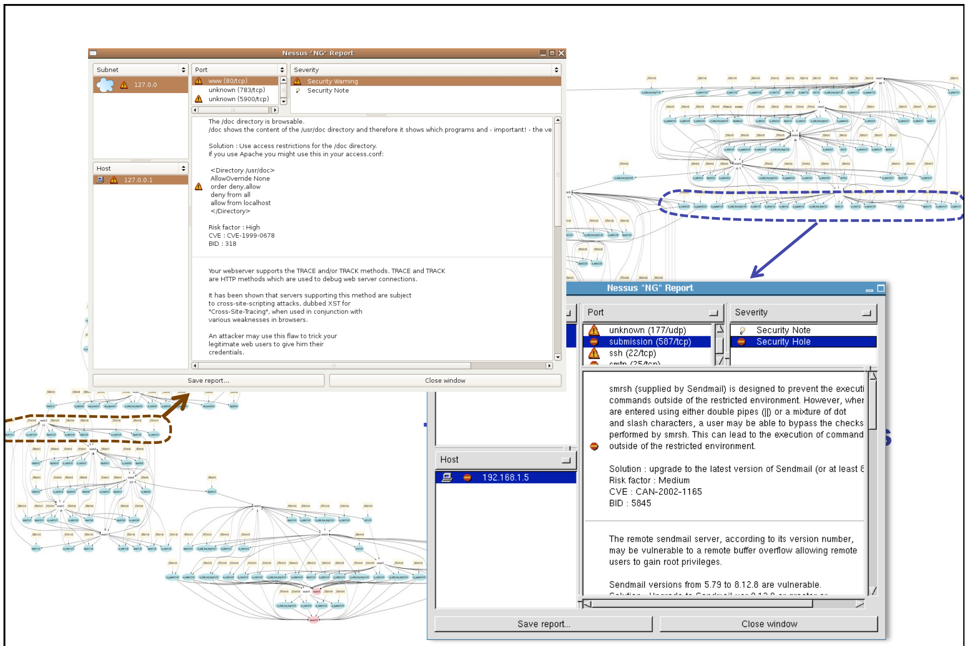
- Generate overwhelming number of alerts
- Many false alerts – normal traffic or failed attacks
- Alerts are isolated
- No indication of how alerts can be combined
- Incomplete alert information
- Where does a security administrator start?
- Is the attacker trying to obtain access to Crown Jewels?
-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

```
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.
```

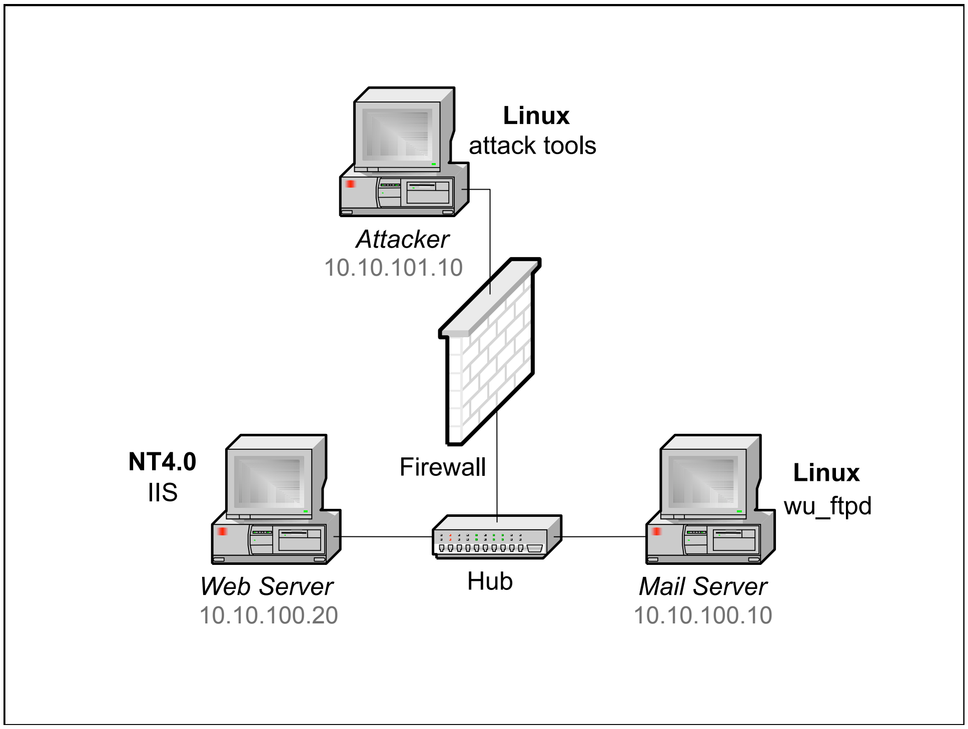
Simply Listing Problems Misses the Big Picture!

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

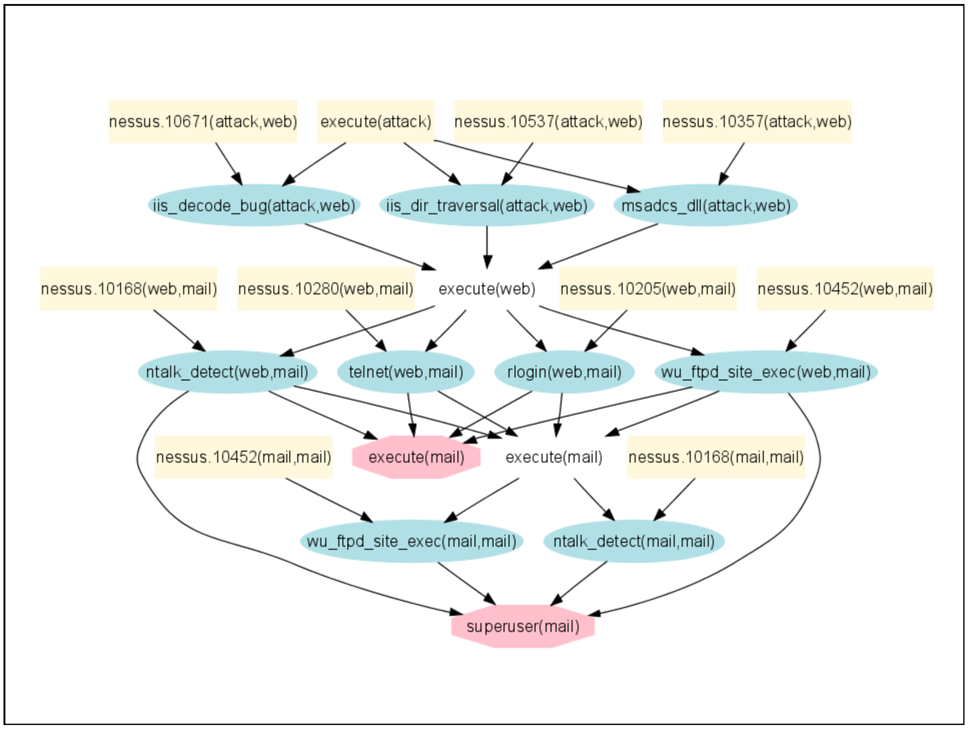
NT4.0
IIS

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)

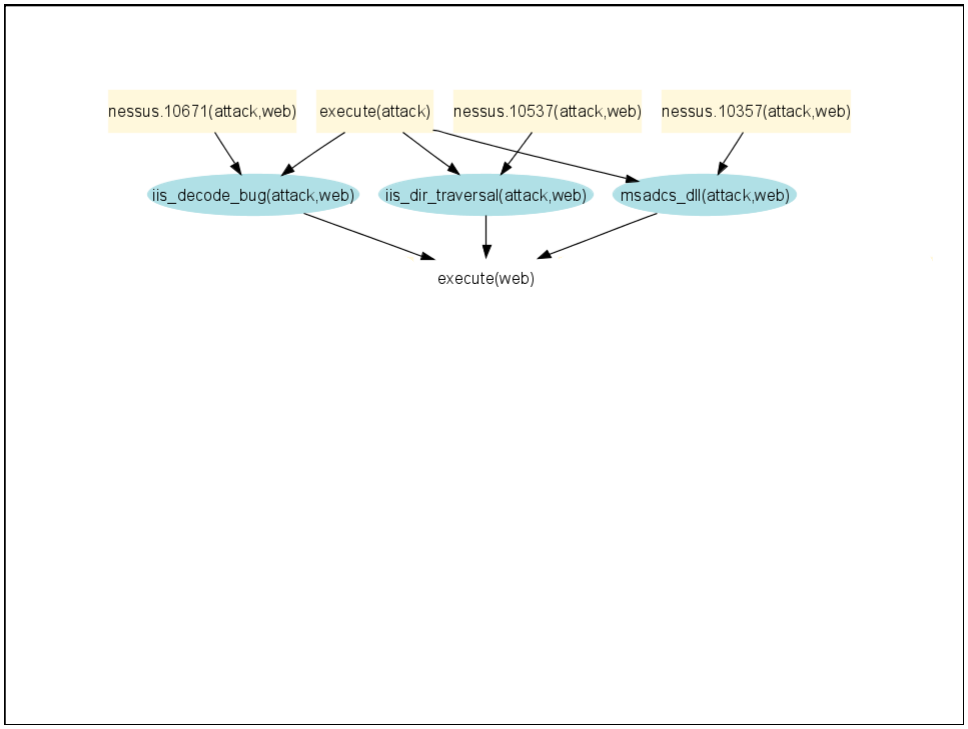
nessus.10168(web,mail)
nessus.10280(web,mail)
execute(web)
nessus.10205(web,mail)
nessus.10452(web,mail)

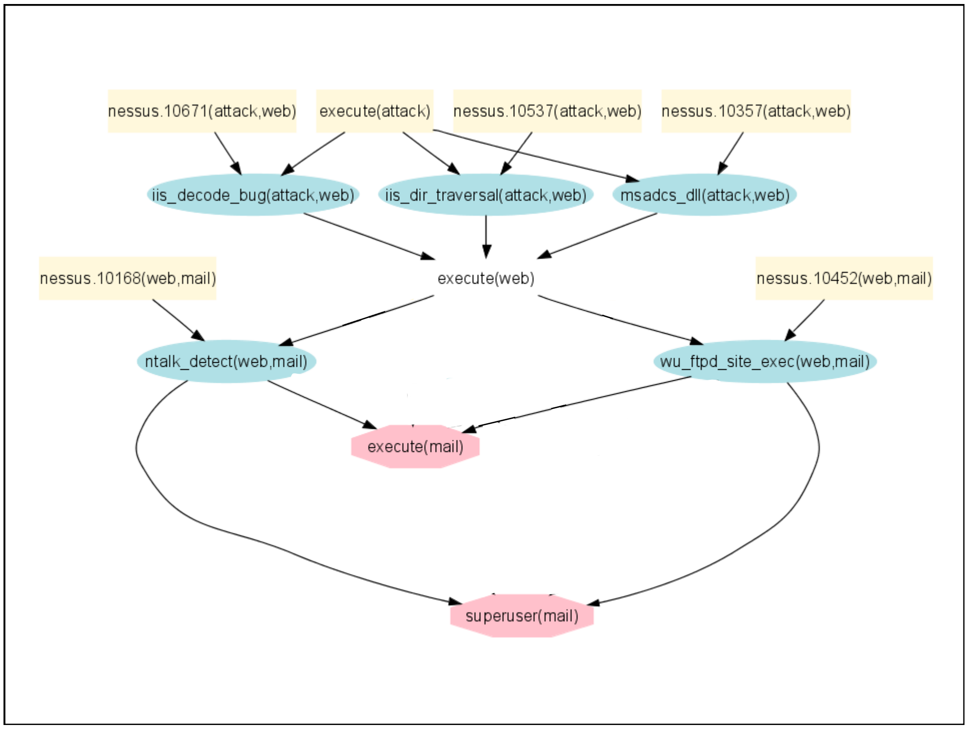
ntalk_detect(web,mail)
telnet(web,mail)
rlogin(web,mail)
wu_ftpd_site_exec(web,mail)

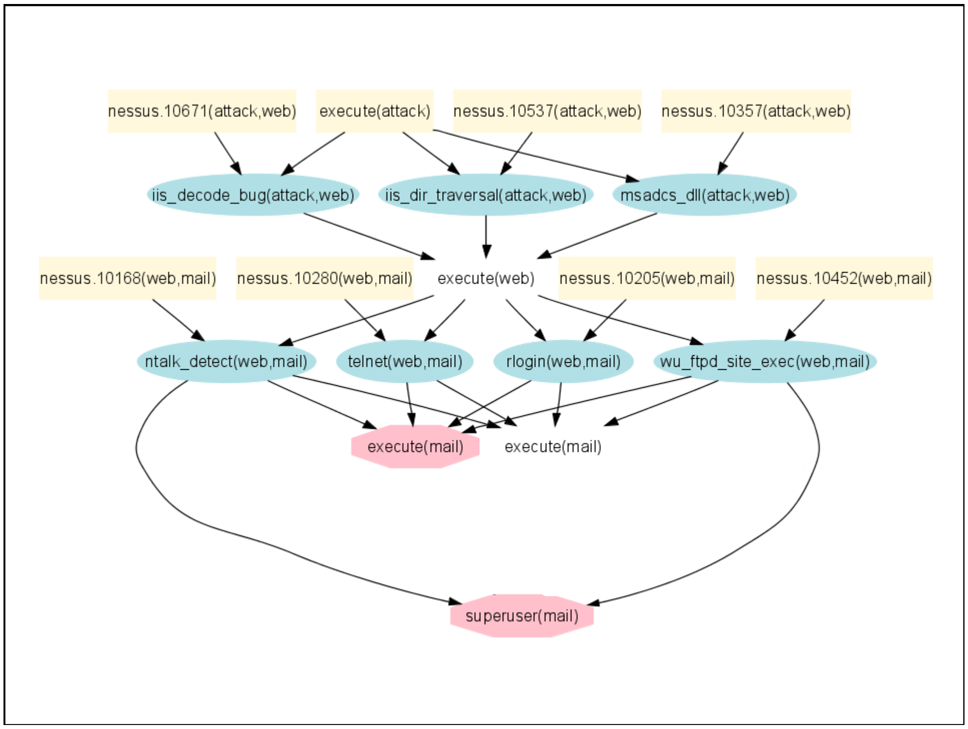
nessus.10452(mail,mail)
execute(mail)
execute(mail)
nessus.10168(mail,mail)

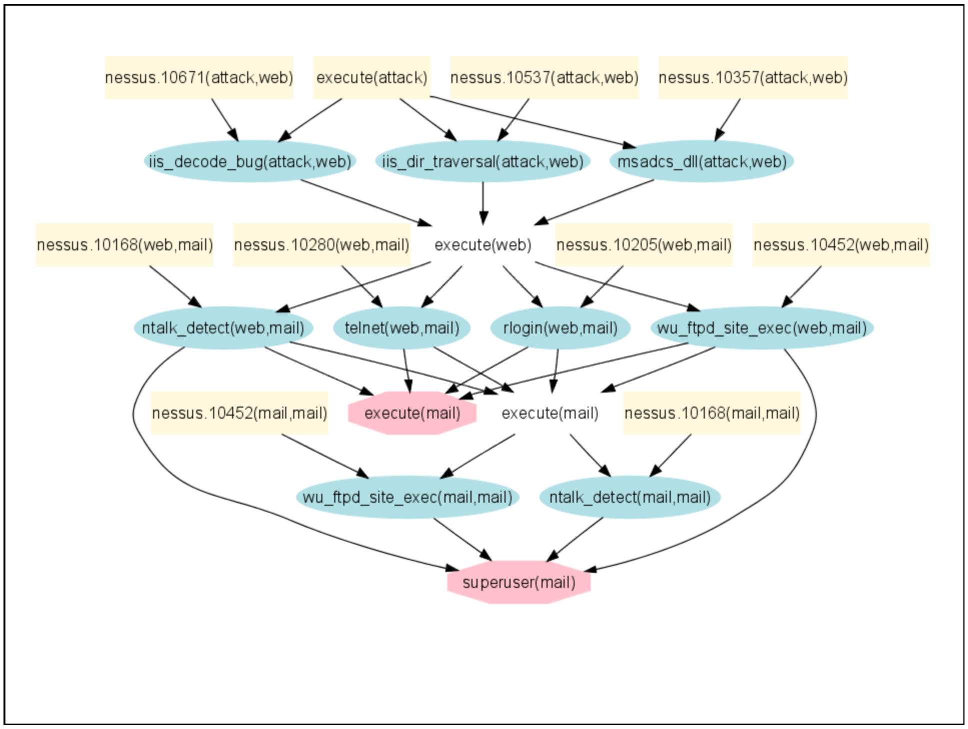
wu_ftpd_site_exec(mail,mail)
ntalk_detect(mail,mail)

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)

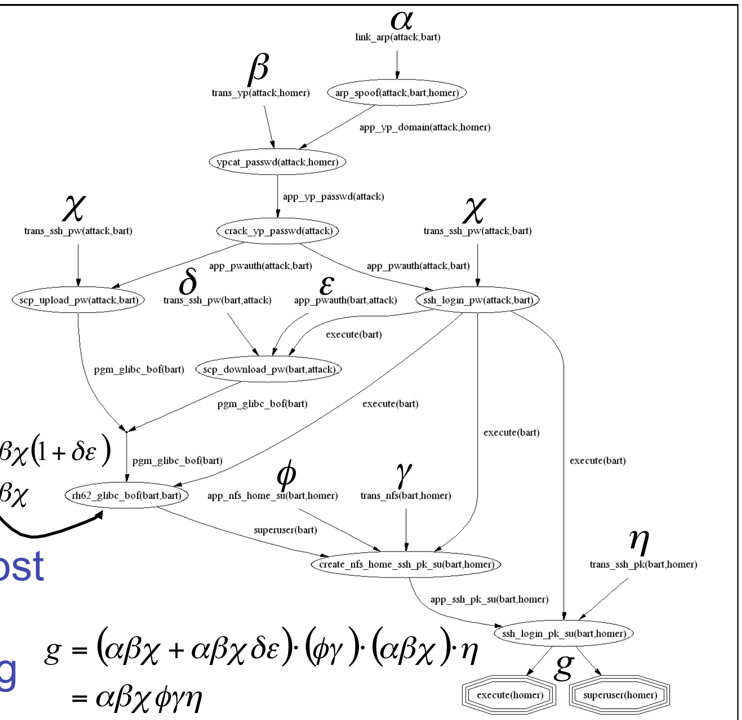

nessus.10671(attack,web)
execute(attack)
nessus.10537(attack,web)
nessus.10357(attack,web)
iis_decode_bug(attack,web)
iis_dir_traversal(attack,web)
msadcs_dll(attack,web)
nessus.10168(web,mail)
execute(web)
nessus.10452(web,mail)
ntalk_detect(web,mail)
wu_ftpd_site_exec(web,mail)
execute(mail)
superuser(mail)


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)

Reference

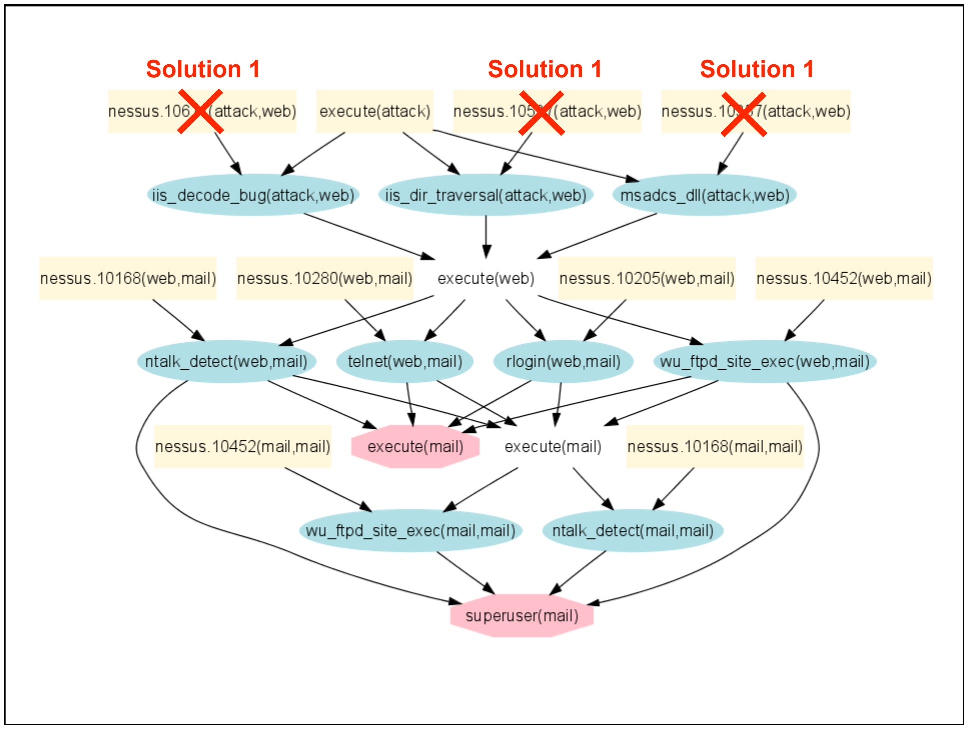
- Sushil Jajodia, Steve Noel, Brian O’Berry, “Topological analysis of network attack vulnerability,” in *Managing Cyber Threats: Issues, Approaches and Challenges*, Vipin Kumar, Jaideep Srivastava, and Aleksandar Lazarevic, eds., Springer, 2005, pages 248-266.

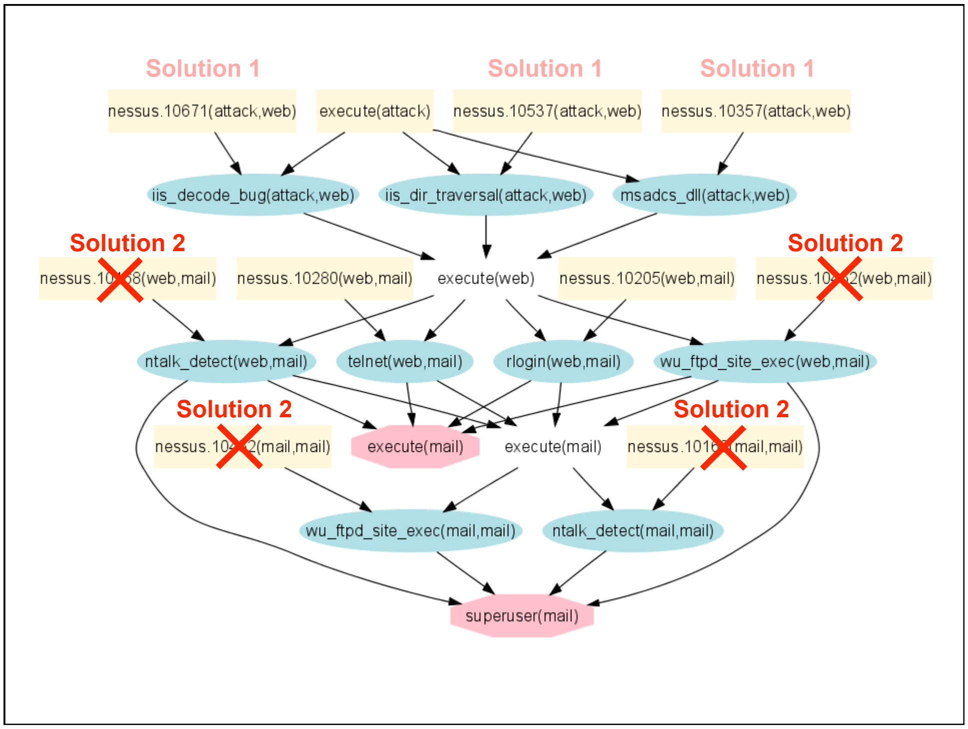


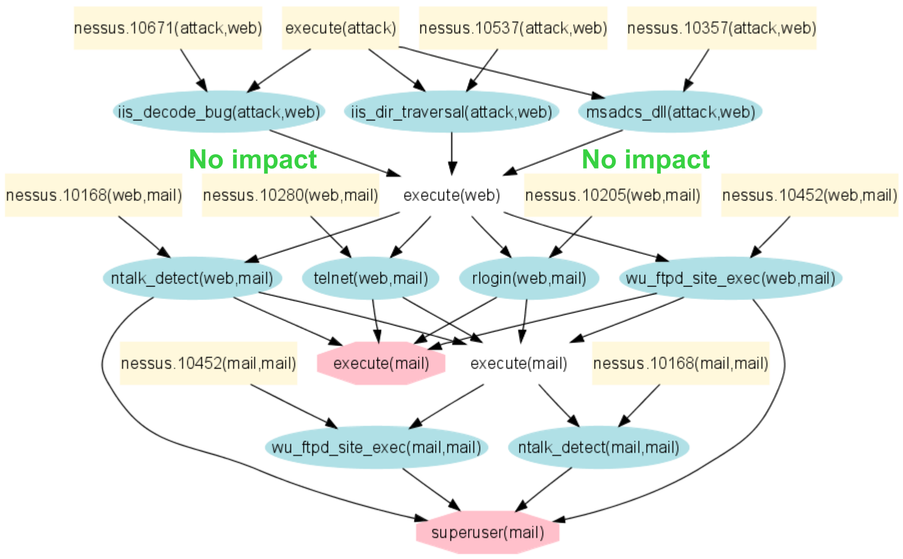
$$\alpha\beta\chi + \alpha\beta\chi\,\delta\varepsilon = \alpha\beta\chi(1 + \delta\varepsilon)$$
$$= \alpha\beta\chi$$

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)

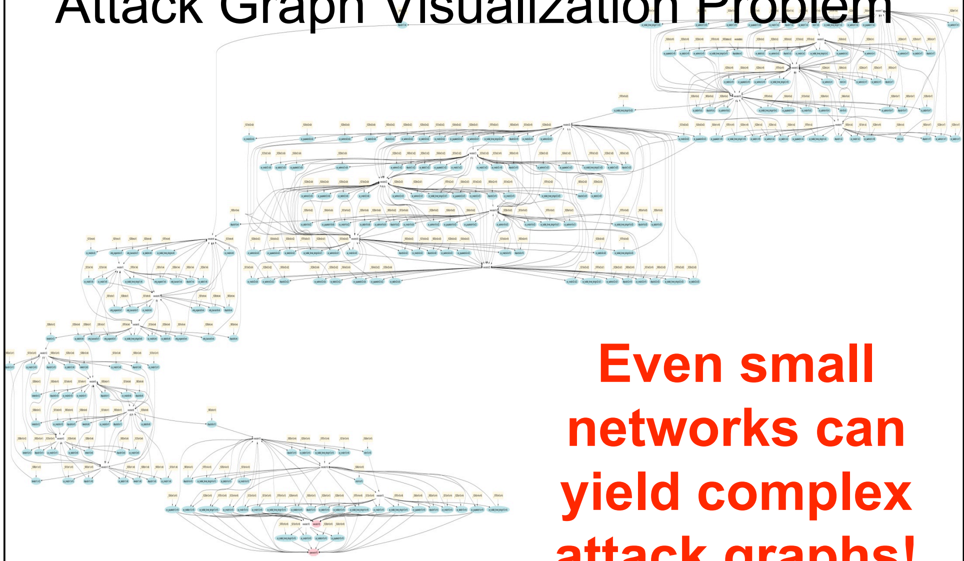

Solution 1
Solution 1
Solution 1
nessus.10671(attack,web)
execute(attack)
nessus.10537(attack,web)
nessus.10357(attack,web)
iis_decode_bug(attack,web)
iis_dir_traversal(attack,web)
msadcs_dll(attack,web)
Solution 2
Solution 2
nessus.10 8(web,mail)
nessus.10280(web,mail)
execute(web)
nessus.10205(web,mail)
nessus.10 2(web,mail)
ntalk_detect(web,mail)
telnet(web,mail)
rlogin(web,mail)
wu_ftpd_site_exec(web,mail)
Solution 2
Solution 2
nessus.10 2(mail,mail)
execute(mail)
execute(mail)
nessus.101 mail,mail)
wu_ftpd_site_exec(mail,mail)
ntalk_detect(mail,mail)
superuser(mail)



Reference

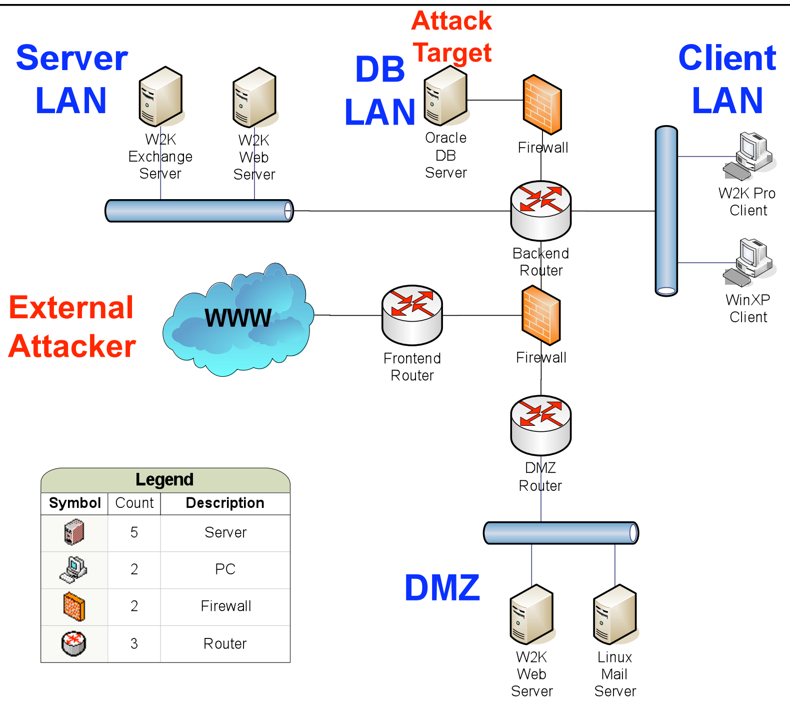
- Lingyu Wang, Steven Noel, Sushil Jajodia, "Minimum-cost network hardening using attack graphs," Computer Communications, 2006.

Attack Graph Visualization Problem



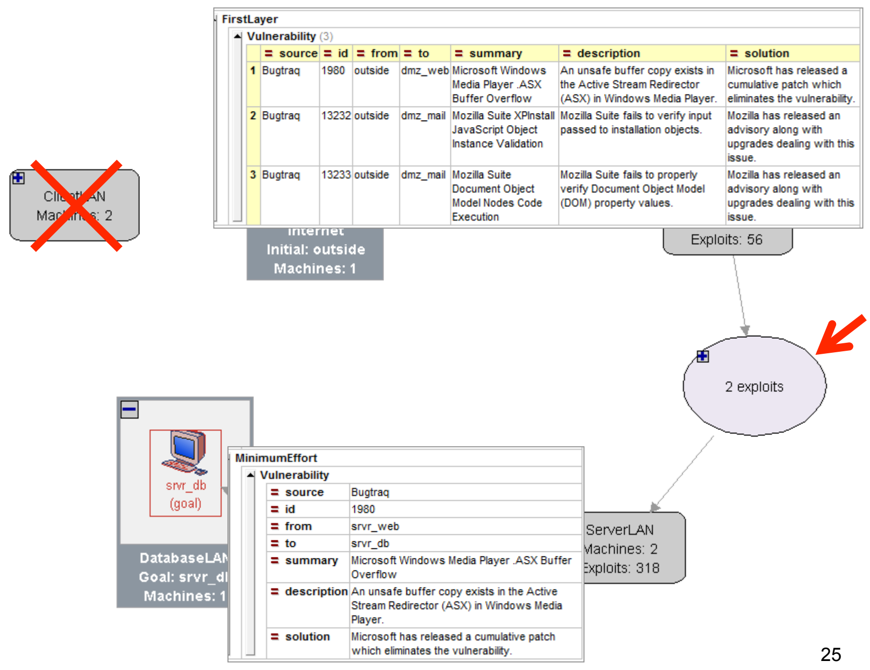
Even small networks can yield complex attack graphs!

23



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

24



FirstLayer

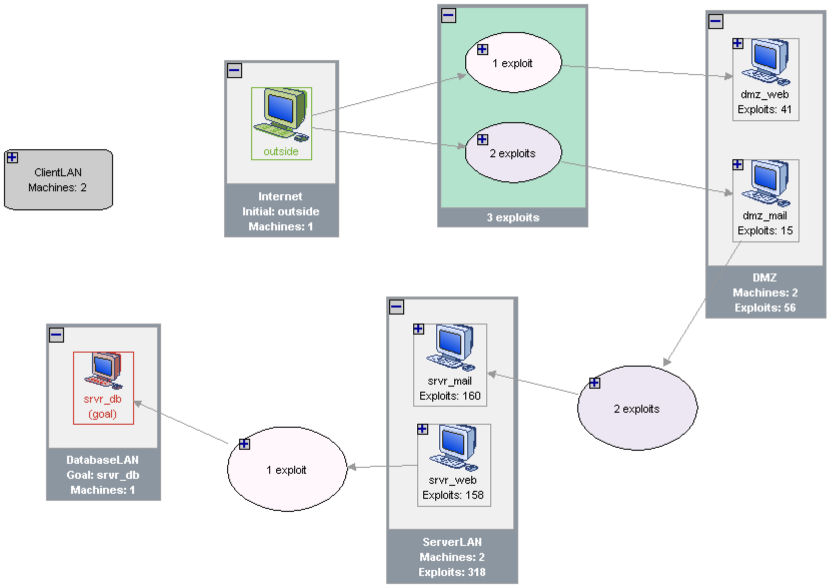
Vulnerability (3)

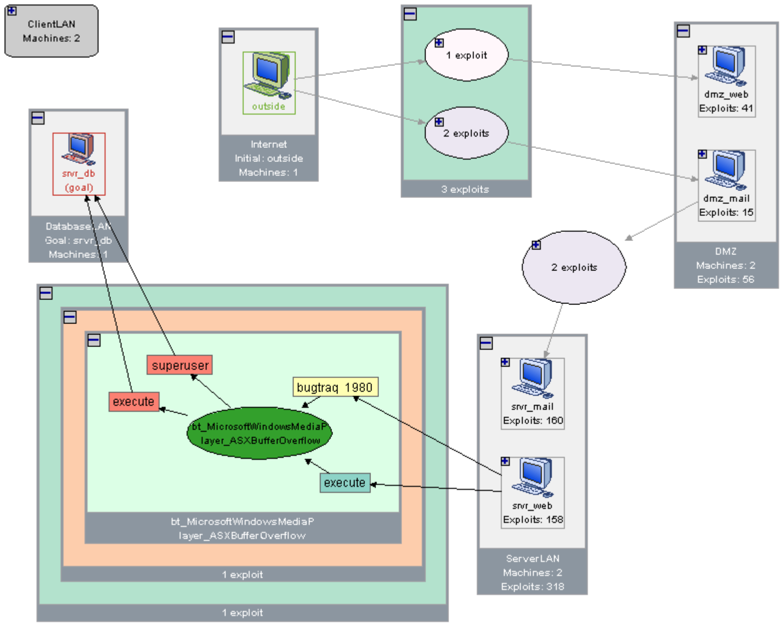
	= source	= id	= from	= to	= summary	= description	= solution
1	Bugtraq	1980	outside	dmz_web	Microsoft Windows Media Player .ASX Buffer Overflow	An unsafe buffer copy exists in the Active Stream Redirector (ASX) in Windows Media Player.	Microsoft has released a cumulative patch which eliminates the vulnerability.
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.

MinimumEffort

Vulnerability

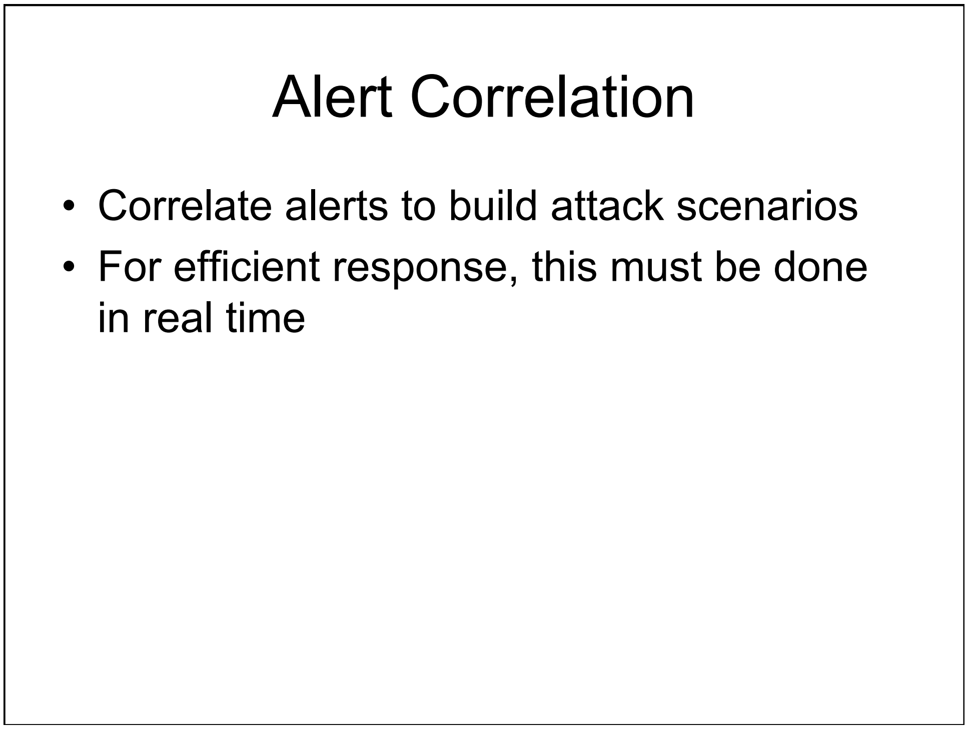
= source	Bugtraq
= id	1980
= from	srvr_web
= to	srvr_db
= summary	Microsoft Windows Media Player .ASX Buffer Overflow
= description	An unsafe buffer copy exists in the Active Stream Redirector (ASX) in Windows Media Player.
= solution	Microsoft has released a cumulative patch which eliminates the vulnerability.





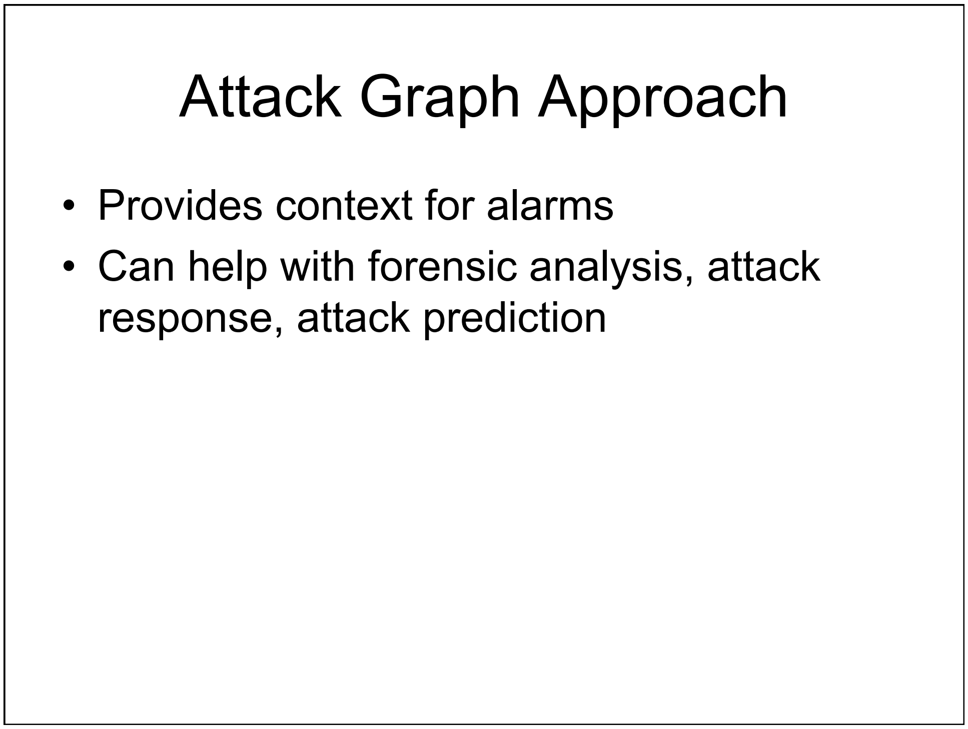
Limitations of IDSs

- 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



Alert Correlation

- Correlate alerts to build attack scenarios
- For efficient response, this must be done in real time

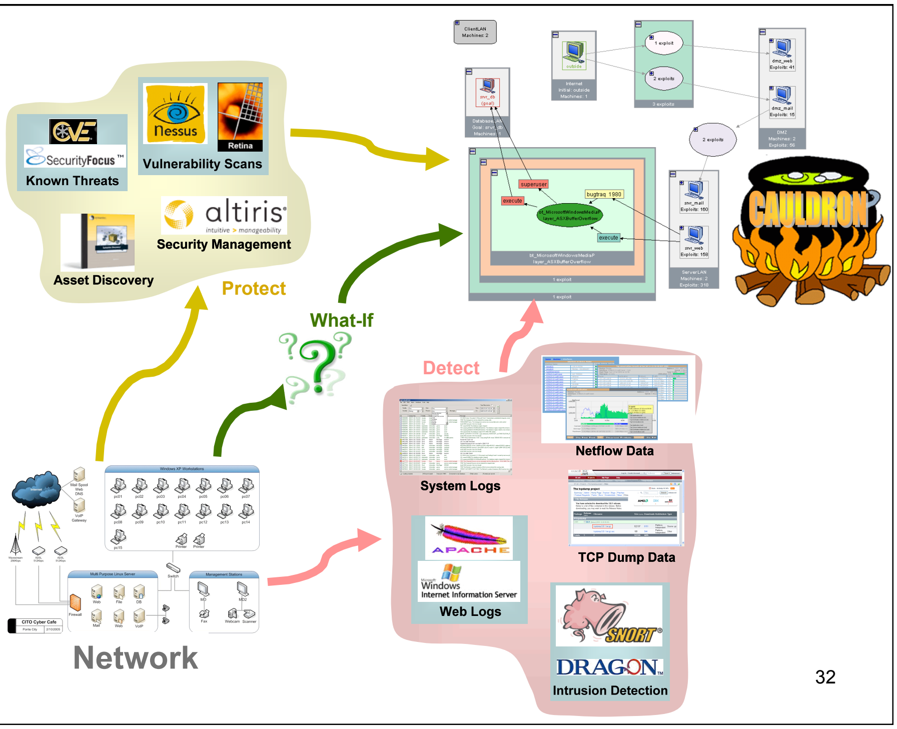


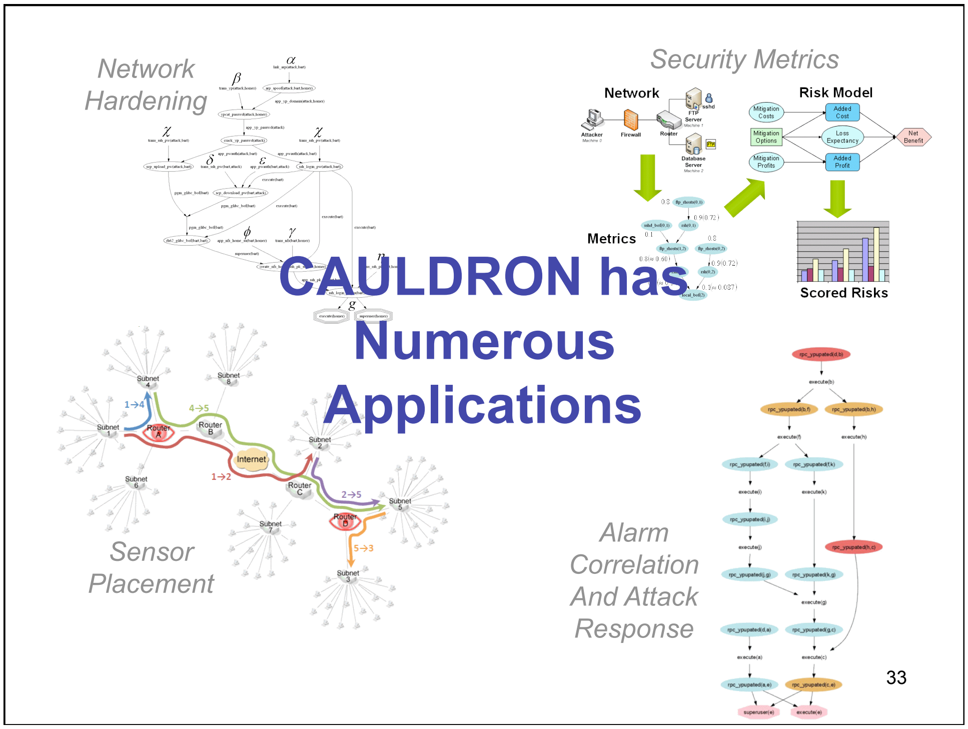
Attack Graph Approach

- Provides context for alarms
- Can help with forensic analysis, attack response, attack prediction

Hypothesizing and Predicting Alerts

- Correlation based on the prepare-for relationship is vulnerable to alerts missed by IDSs - Reassembling a broken attack scenario is expensive and error-prone
- By reasoning about the *inconsistency* between the knowledge (encoded in attack graph) and the facts (represented by received alerts), missing alerts can be hypothesized
- By extending the facts in a way that is consistent with the knowledge, possible consequences of current attacks can be predicted





CAULDRON has Numerous Applications

Network Hardening

Security Metrics

Sensor Placement

Alarm Correlation And Attack Response

33

CAULDRON Has Wide Customer Base

NSA

DHS

FAA

AFOSR

AFRL

NRO

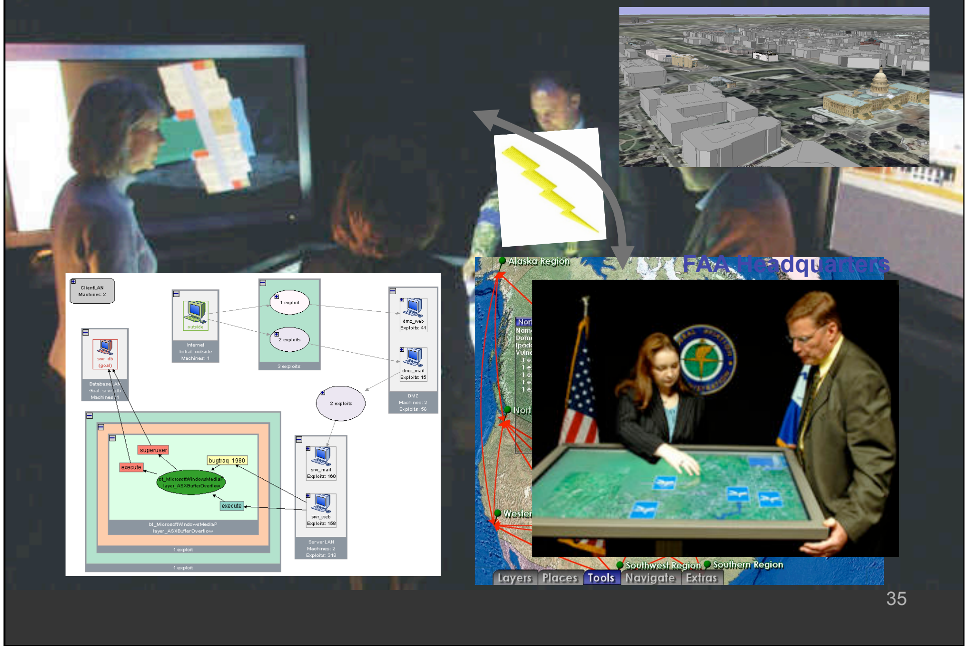
DISA

NIST

JIOC

34

FAA CSIRC Deployment, Leesburg, VA



Summary of CAULDRON

- Automated analysis of all possible attack paths through a network
  - Resulting attack “roadmap” provides context for optimal defenses
  - Transforms volumes of isolated facts into manageable, actionable results
- Integrates with existing tools for capturing network configuration
- Your network is provably secure, with minimum effort
- **Best tool for making informed decisions about network security**

Further Information:

Sushil Jajodia

jajodia@gmu.edu

(703) 993-1653

http://csis.gmu.edu/