

REPORTING THE KILL CHAIN

Types of Security Assessments

- Vulnerability Assessment
- Penetration Test
- Code Review
- Red Teaming
- Attack Simulation
- Audit
- White/Grey/Black-box Assessment
- Risk Assessment
- Threat Assessment
- Threat Modeling
- ...

Easy reports

The screenshot shows the Nessus interface for a scan of host 192.168. The top navigation bar includes 'Scans 88' and 'Policies'. The breadcrumb trail is 'Hosts > 192.168 > Vulnerabilities 52'. A table of vulnerabilities is displayed with columns for Severity, Plugin Name, Plugin Family, and Count. A red box highlights a specific vulnerability: 'Patch X is missing on target Y. Fix because vulnerability Z.' To the right, the 'Host Details' section shows IP, MAC, OS (Linux Kernel 3.10, 3.5, 3.8, 3.9), and scan start/end times. A 'Vulnerabilities' donut chart shows the distribution of severity levels: High (orange), Medium (yellow), and Info (blue).

Severity	Plugin Name	Plugin Family	Count
HIGH	NFS Share User Mountable	RPC	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	2
MEDIUM	SSL Certificate with W...		
MEDIUM	SSL Self-Signed Certi...		
MEDIUM	AFP Server Directory		
MEDIUM	Microsoft Windows SMB Guest Account Local User Access	Windows	1
MEDIUM	MySQL Protocol Remote User Enumeration	Databases	1
MEDIUM	NFS Exported Share Information Disclosure	RPC	1
MEDIUM	NFS Shares World Readable	RPC	1
MEDIUM	SMB Signing Disabled	Misc.	1
INFO	Nessus SYN scanner	Port scanners	16
INFO	RPC Services Enumeration	Service detection	12
INFO	Service Detection	Service detection	9

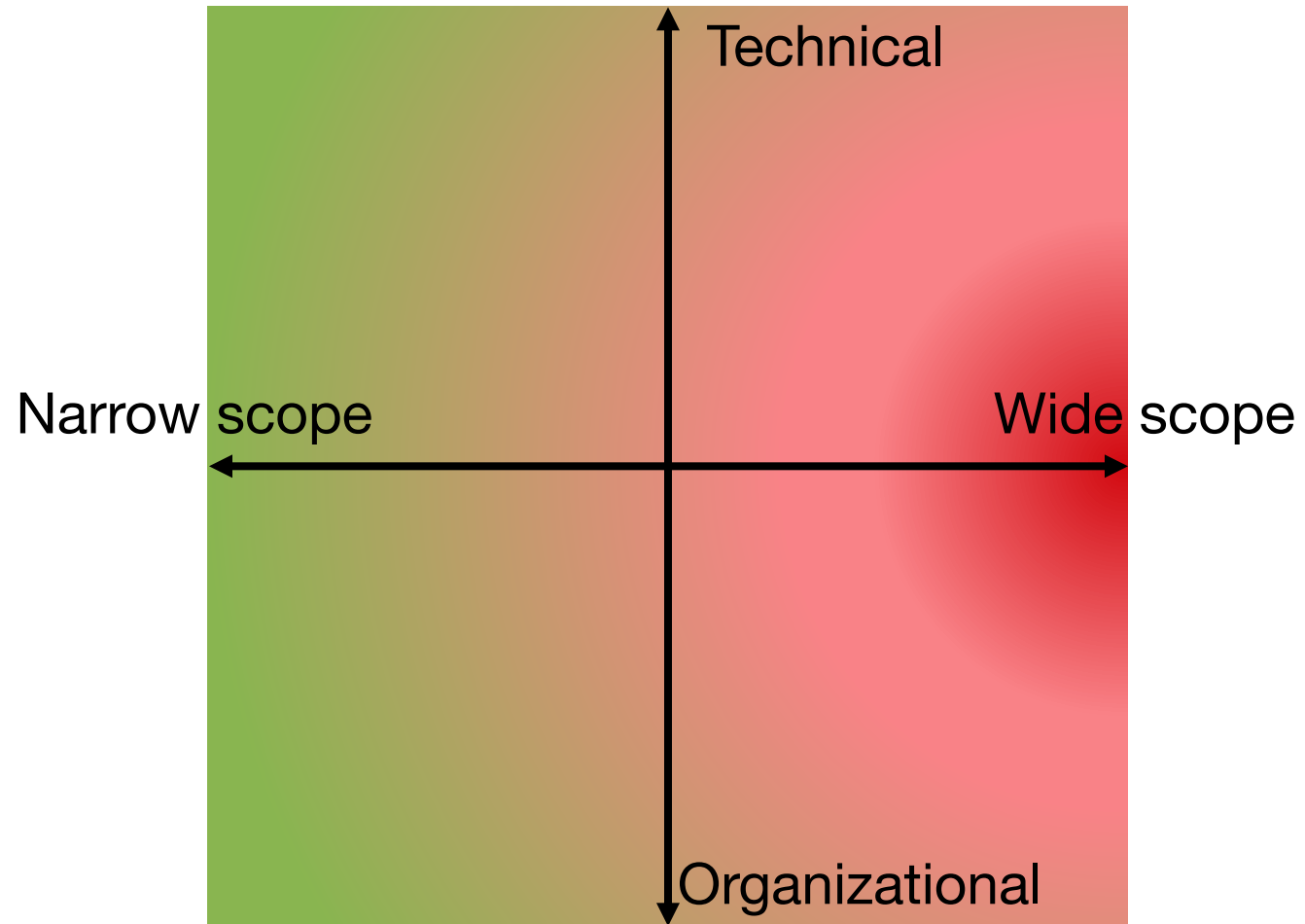
Host Details

- IP: [Redacted]
- MAC: [Redacted]
- OS: Linux Kernel 3.10, Linux Kernel 3.5, Linux Kernel 3.8, Linux Kernel 3.9
- Start: Today at 7:19 PM
- End: Today at 7:23 PM
- Elapsed: 4 minutes
- Download

Vulnerabilities

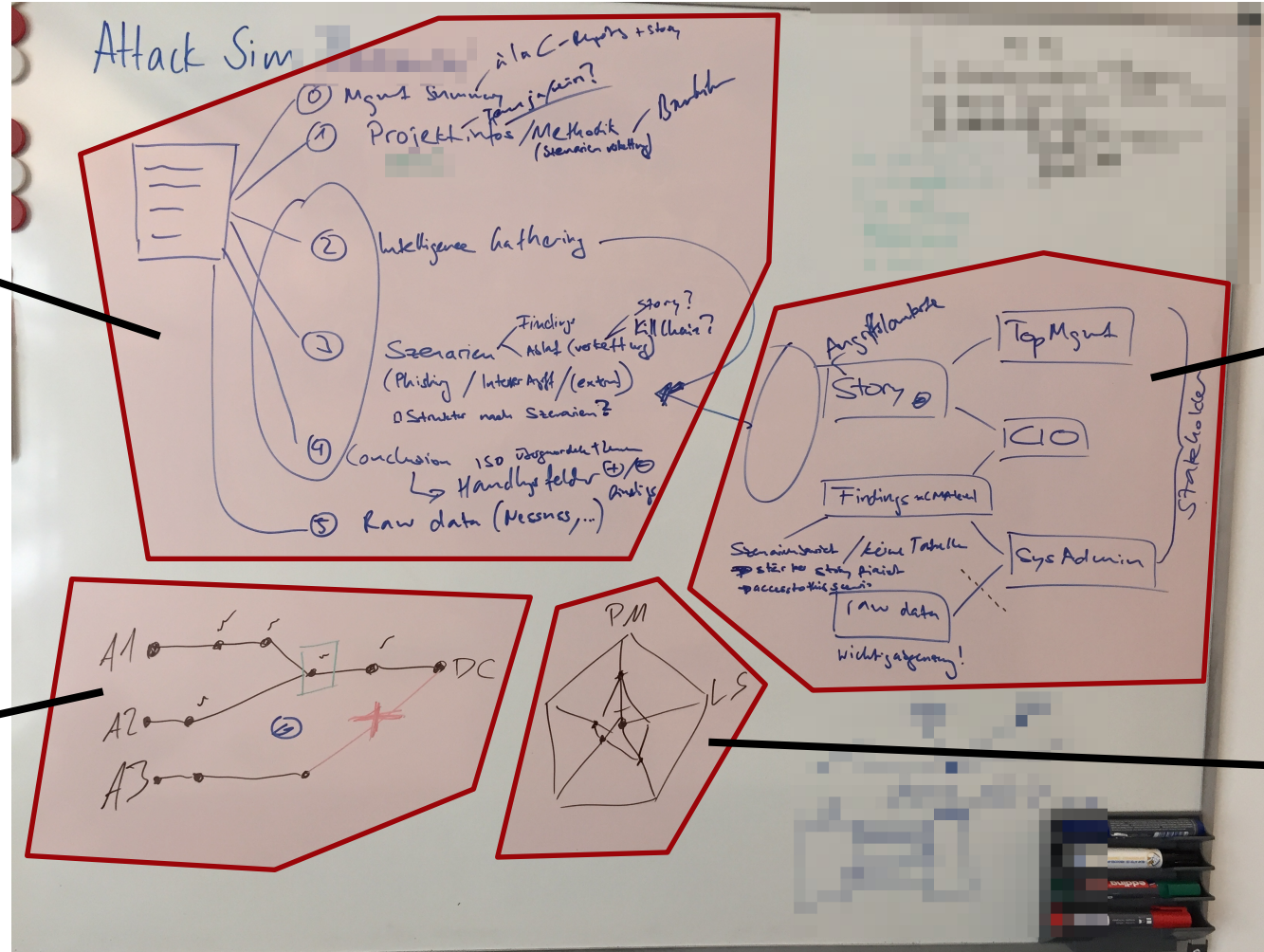
- High (Orange)
- Medium (Yellow)
- Info (Blue)

Complexity of Reporting



What makes a good report

Structure

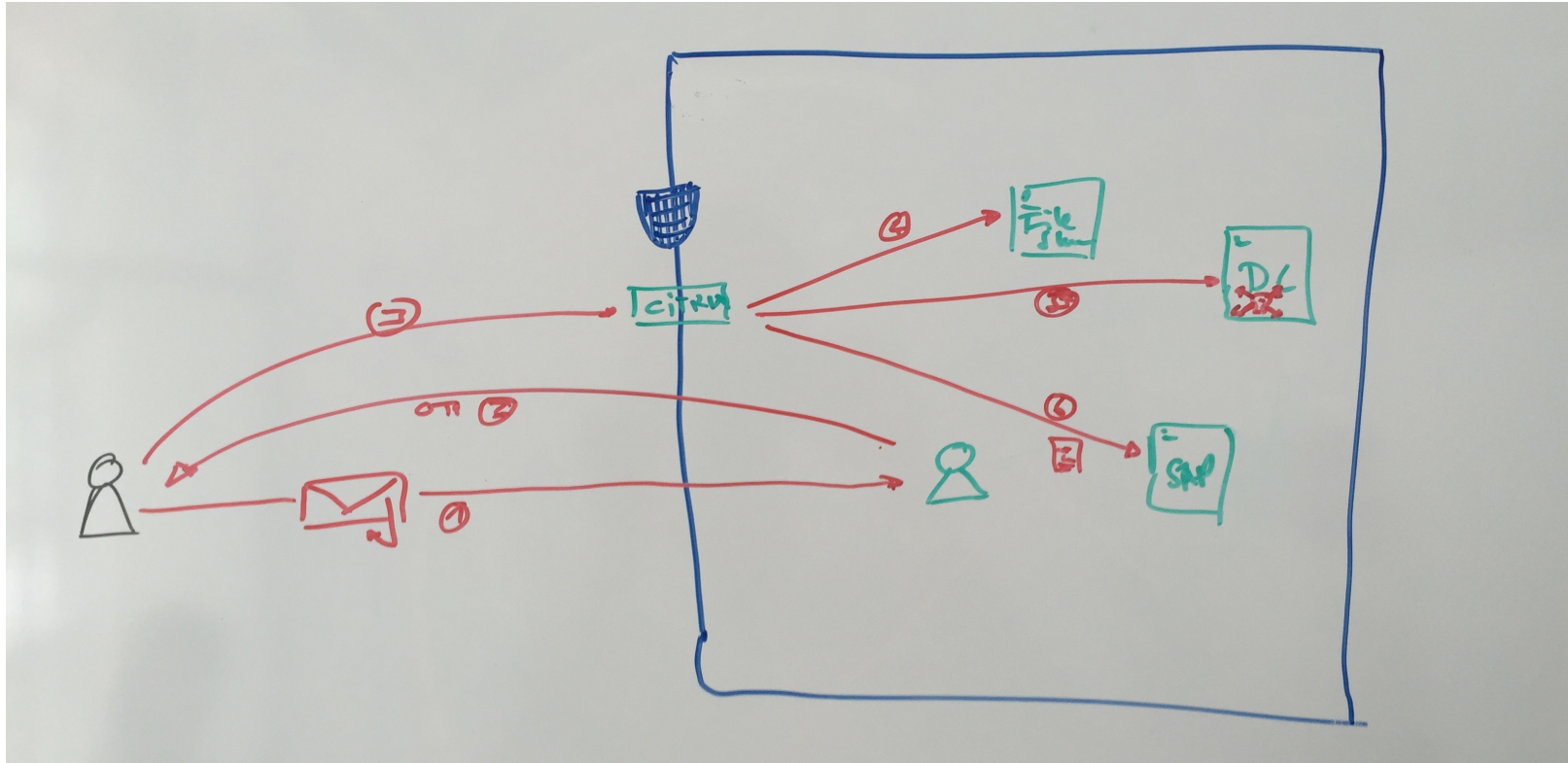


Shareholders

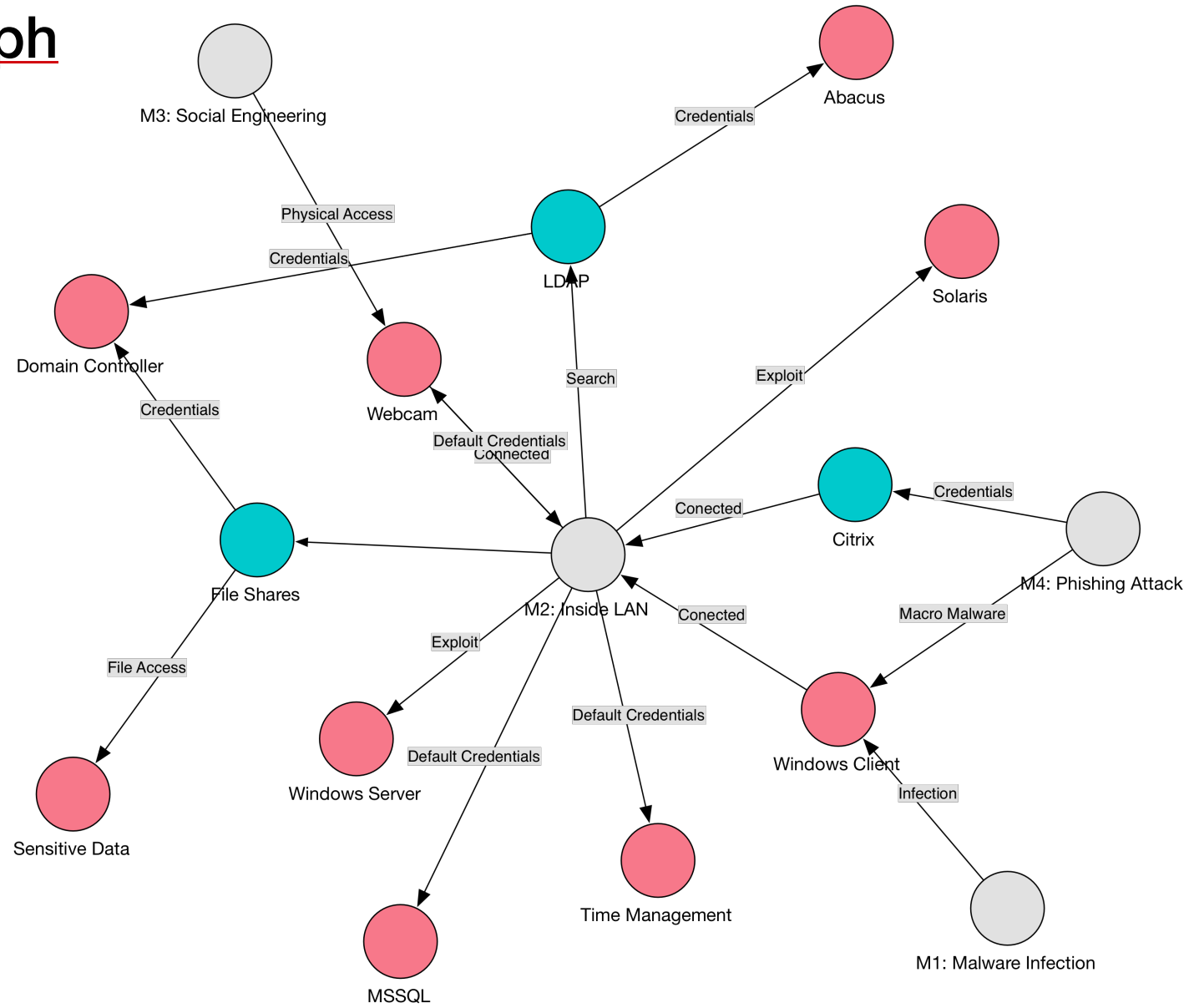
Visualization

Metrics

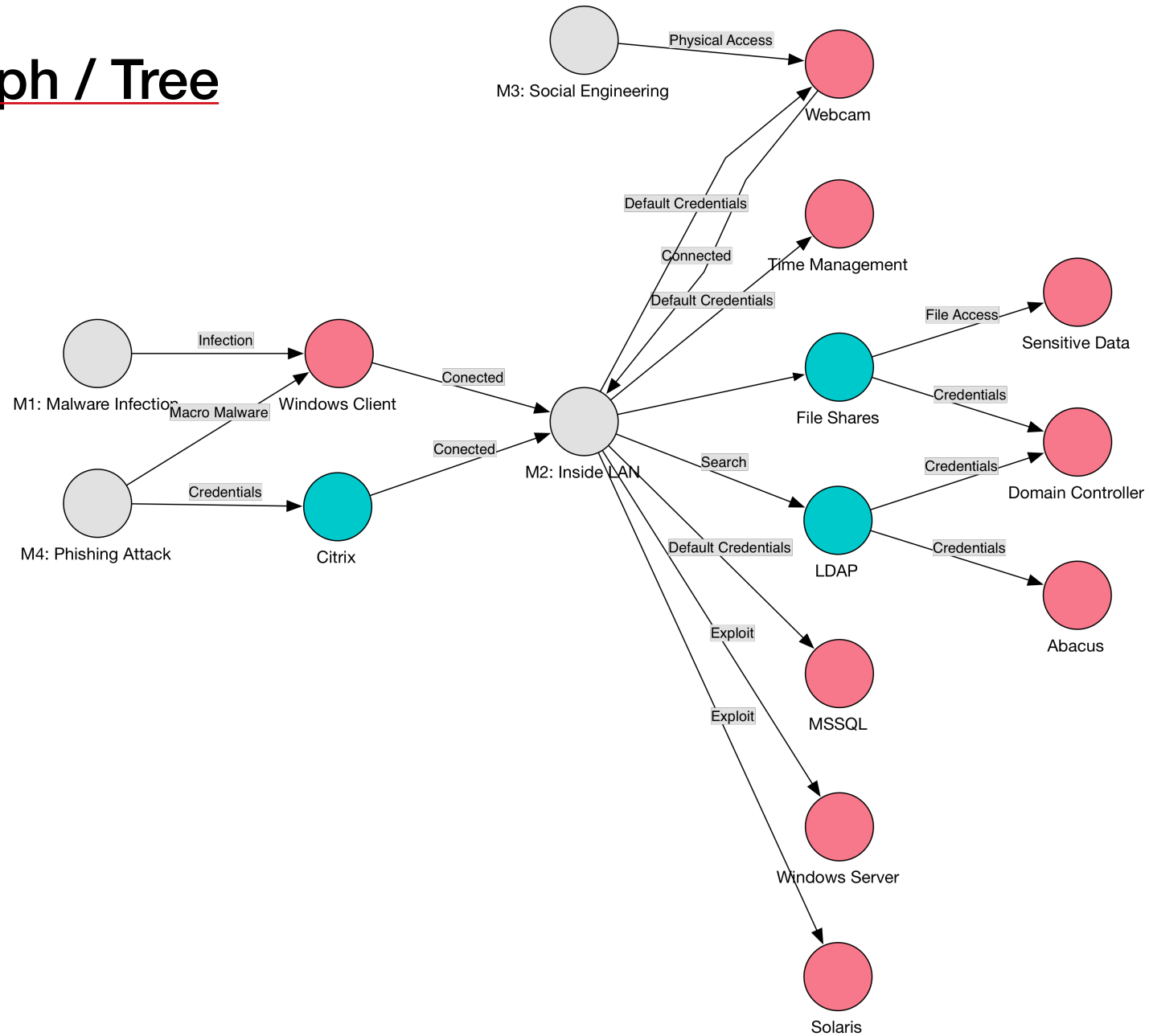
Scope vs. Scenario



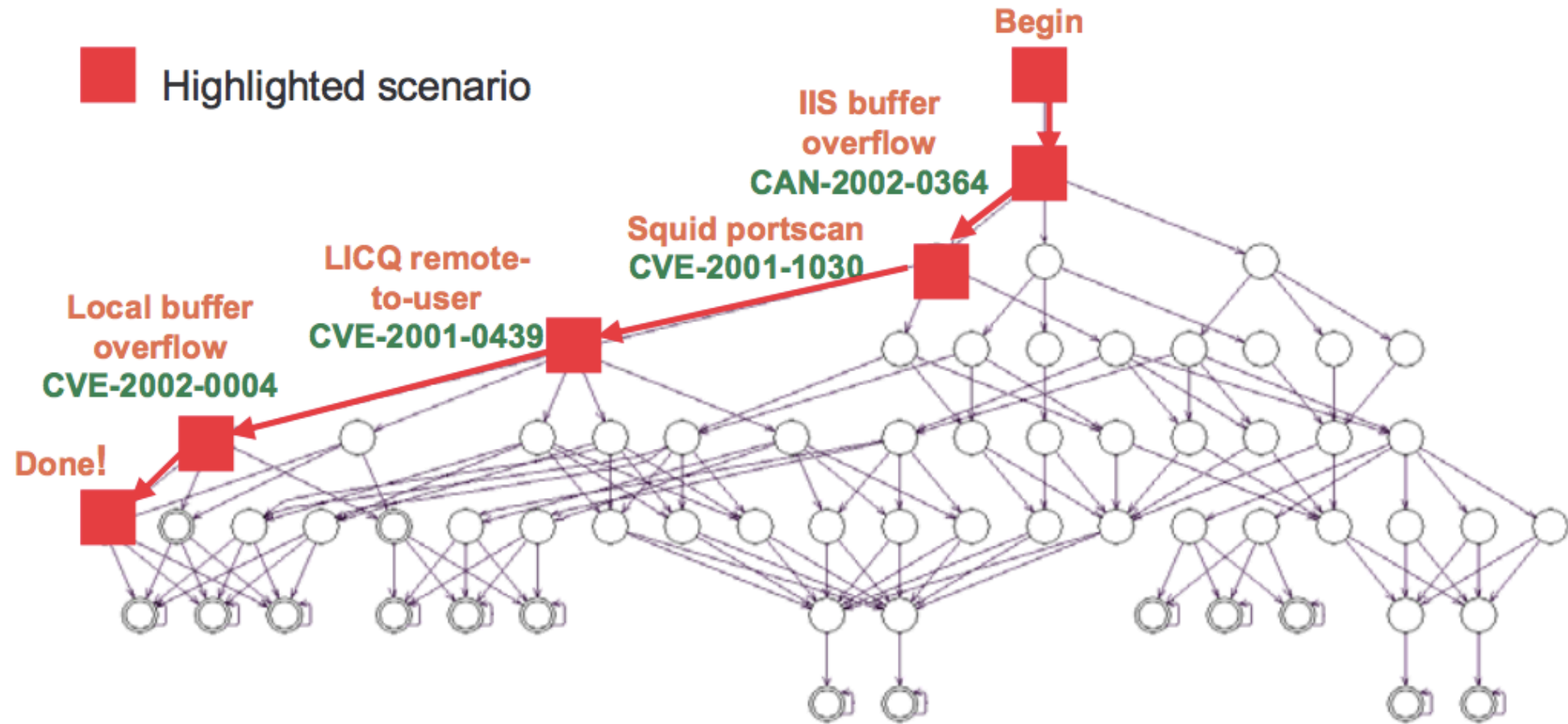
Attack Graph



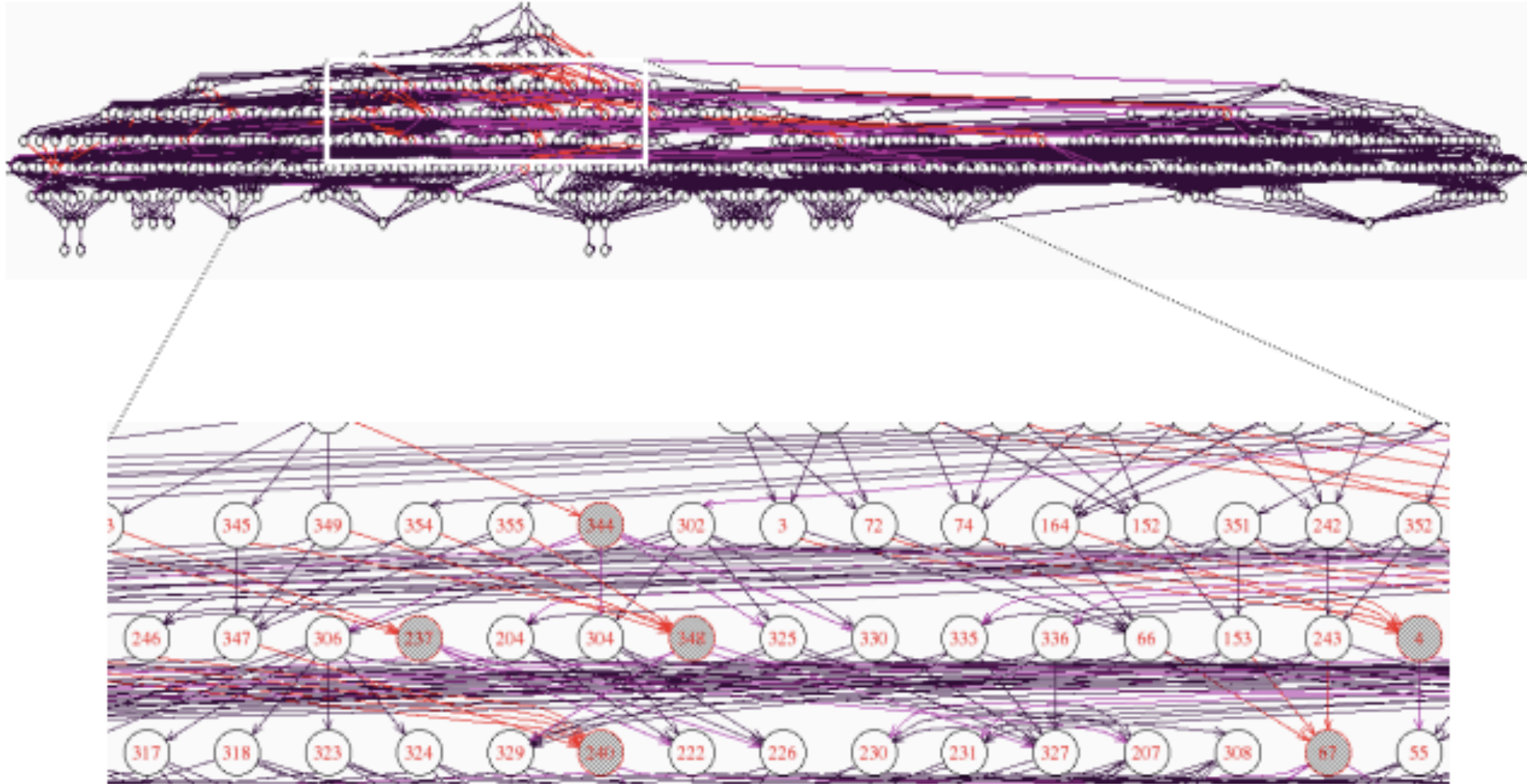
Attack Graph / Tree



Reality



Reality



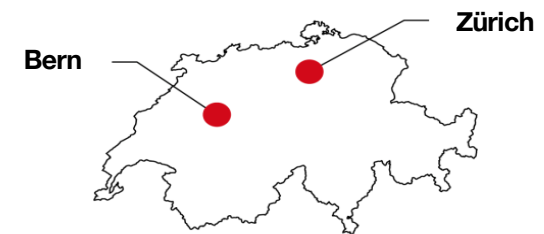
<https://www.cs.cmu.edu/~scenariograph/wing07.pdf>

Some Conclusions

- Vulnerability/Finding based reporting is easy
- We know what the customers want
- Reporting complex attack scenarios is hard
- The amount of data we gather during an assessment is huge
- Increasing complexity of our assessments allows less automation in the reporting phase
- Visualization helps but is also hard
- DIN A4 might not be the best to handle modern reports

Thanks for your attention

REDGUARD
SECURING YOUR ASSETS



Redguard AG Eigerstrasse 60 CH-3007 Bern
T +41 (0)31 511 37 50 www.redguard.ch