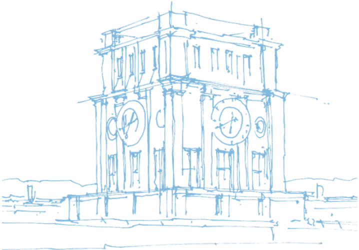
Network Discovery Orchestration

Final talk for the Master's Thesis by

Michael Eder
advised by Jonas Jelten, Simon Bauer

Wednesday 15th May, 2019

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich



Agenda

- Motivation
- Implementation
- Evaluation
  - Testbed evaluation
  - Scanning from internal and external vantage points
  - Deep dive: TLS certificates
  - Comparison with other scanners
  - Multiple nodes on a single host

Motivation

Distributed scanning capabilities

- Asynchronous scanners: vertical scaling by sending as many packets as possible
- Work distribution: approach that has been neglected in the last years, but:
  - Allows to scale linear to number of scanning nodes
  - Allows to have less load on scanner nodes and network components
  - Allows to create views of different vantage points, e.g. DMZ, public WiFi and Internet
  - Scan is resilient against failures, e.g. scanning nodes getting disconnected

Motivation

Runtime requirements and missing functionality of existing scanners

Runtime requirements of existing scanners (e.g. Nmap, ZMap, Masscan)

- Require elevated privileges
- Require specific operating systems (e.g. ZMap doesn’t run on Windows)
- Require runtime libraries (e.g. libpcap, pfring)
- Static binaries for other operating systems / architectures often difficult to build

→ Existing scanners too unflexible for dynamic deployments leveraging existing infrastructure

Implementation

Design decisions

- Prototype implemented in Go
  - Static, native binaries for all platforms. Cross compiling for every platform possible
  - Built-in concurrency via asynchronous, leightweight goroutines
- Running unprivileged in user space
- Server-Client architecture
- Communication: TCP, TLS 1.2 possible (also with mutual authentication)
- Work distribution via pooling
  - Each pool contains all targets
  - Each pool may have arbitrary scanner nodes working on it
  - Allows to create views while still being able to speed the scan up

Implementation

Design decisions

- Pull-based work distribution: Nodes ask for work → Easier to traverse firewalls/NAT and less book keeping at the server
- Rate limiting: Difficult due to lack of low level hardware access → limit number of concurrent goroutines that call the actual scan function
- Scan interruption: Server can pause / stop all nodes at any time
- Dead man's switch: If a node loses server connection, the scan is paused until the connection is reestablished

Implementation

Architecture

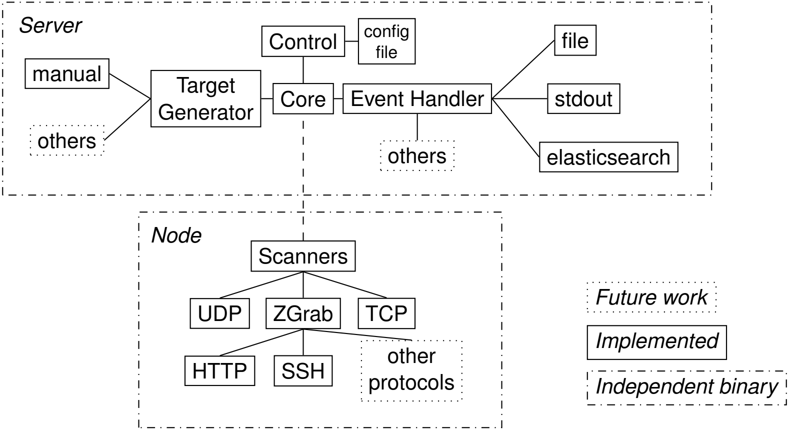


Figure 1: Architecture of the prototype.

Evaluation

Testbed evaluation - quick facts

- Mininet → reproducible, possible to control packet loss etc.
- Two networks connected via a router
- Open ports by several computers exposed to the network
- Scan complete network from both vantage points
- Goals:
  - Verify the scanner actually works
  - Find out how packet loss due to congestion affects the scan

Evaluation

Testbed evaluation - setup

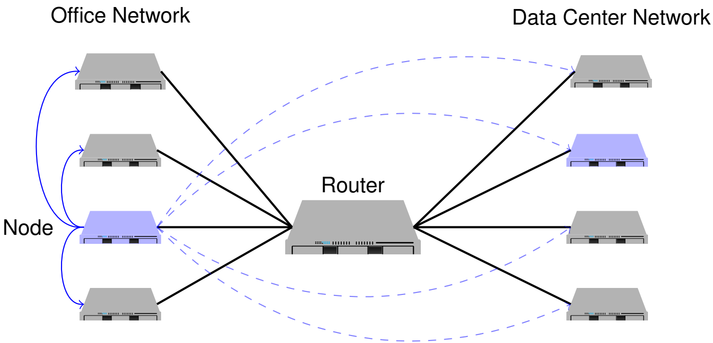


Figure 2: Simplified schema of the testbed

Evaluation

Testbed evaluation - Results

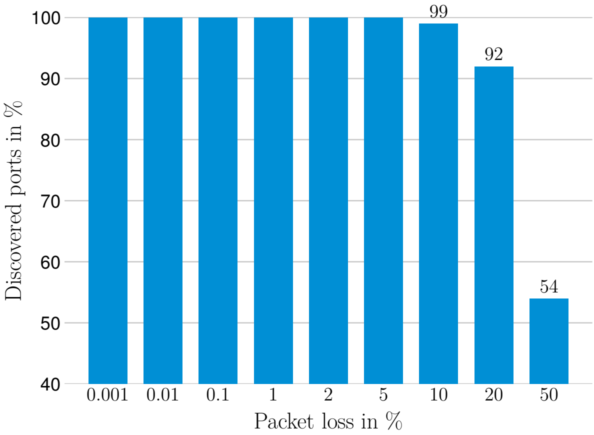


Figure 3: Discovered ports when scanning from office to data center network with various packet loss configurations.

Evaluation

Scan from external and internal vantage point - Idea

- Scan RBG network (minus highly dynamic ranges like eduroam) from inside and Internet using Nmap “Top 50” ports
- Which services are available and exposed to the internal network/Internet

Evaluation

Scan from external and internal vantage point - Results

		M1		M2		M3	
Port	Service	int	ext	int	ext	int	ext
22	SSH	1846	523	1821	531	1825	524
25	SMTP	105	5	103	4	100	4
53	DNS	29	8	30	8	30	8
80	HTTP	640	509	651	514	645	515
443	HTTPS	502	394	506	400	506	401
445	SMB	101	0	237	1	232	0
465	SMTP	26	25	25	24	25	24
587	SMTP	23	23	23	22	22	22
993	IMAP	21	17	22	18	22	18
995	POP3	13	9	14	10	14	10
3389	RDP	146	53	156	51	148	49

Table 1: Excerpt: Ports discovered by scanning from internal and external (the Internet) vantage points.

Evaluation

Scan from external and internal vantage point - Results

		M1		M2		M3	
Port	Service	int	ext	int	ext	int	ext
22	**SSH**	**1846**	**523**	**1821**	**531**	**1825**	**524**
25	SMTP	105	5	103	4	100	4
53	DNS	29	8	30	8	30	8
80	HTTP	640	509	651	514	645	515
443	HTTPS	502	394	506	400	506	401
445	SMB	101	0	237	1	232	0
465	SMTP	26	25	25	24	25	24
587	SMTP	23	23	23	22	22	22
993	IMAP	21	17	22	18	22	18
995	POP3	13	9	14	10	14	10
3389	**RDP**	**146**	**53**	**156**	**51**	**148**	**49**

Table 2: Excerpt: Ports discovered by scanning from internal and external (the Internet) vantage points.

Evaluation

Scan from external and internal vantage point - Results

		M1		M2		M3	
Port	Service	int	ext	int	ext	int	ext
22	SSH	1846	523	1821	531	1825	524
25	**SMTP**	**105**	**5**	**103**	**4**	**100**	**4**
53	**DNS**	**29**	**8**	**30**	**8**	**30**	**8**
80	HTTP	640	509	651	514	645	515
443	HTTPS	502	394	506	400	506	401
445	**SMB**	**101**	**0**	**237**	**1**	**232**	**0**
465	SMTP	26	25	25	24	25	24
587	SMTP	23	23	23	22	22	22
993	IMAP	21	17	22	18	22	18
995	POP3	13	9	14	10	14	10
3389	RDP	146	53	156	51	148	49

Table 3: Excerpt: Ports discovered by scanning from internal and external (the Internet) vantage points.

Evaluation

Scan from external and internal vantage point - Results

		M1		M2		M3	
Port	Service	int	ext	int	ext	int	ext
22	SSH	1846	523	1821	531	1825	524
25	SMTP	105	5	103	4	100	4
53	DNS	29	8	30	8	30	8
80	**HTTP**	**640**	**509**	**651**	**514**	**645**	**515**
443	**HTTPS**	**502**	**394**	**506**	**400**	**506**	**401**
445	SMB	101	0	237	1	232	0
465	**SMTP**	**26**	**25**	**25**	**24**	**25**	**24**
587	**SMTP**	**23**	**23**	**23**	**22**	**22**	**22**
993	**IMAP**	**21**	**17**	**22**	**18**	**22**	**18**
995	**POP3**	**13**	**9**	**14**	**10**	**14**	**10**
3389	RDP	146	53	156	51	148	49

Table 4: Excerpt: Ports discovered by scanning from internal and external (the Internet) vantage points.

Evaluation

Closer look: TLS certificates

- Who issues them? → Ideally only DFN/TUM/LRZ?
- When did expired ones expire? → Identify possibly old/forgotten systems

Evaluation

TLS certificates external and internal - Issuers

	M1		M2		M3	
	int	ext	int	ext	int	ext
DFN / TUM / LRZ	279	236	274	236	280	242
Let’s Encrypt	65	68	70	71	71	73
Unusual CAs	117	64	120	65	122	62
Total	461	368	464	372	473	377

Table 5: Certificates issued grouped by CAs.

Evaluation

TLS certificates external and internal - Expiry

	M1		M2		M3	
	int	ext	int	ext	int	ext
2006	1	0	1	0	1	0
2007	2	1	2	1	2	1
2008	0	0	0	0	0	0
2009	2	2	2	2	2	2
2010	1	1	1	1	1	1
2011	1	1	1	1	1	1
2012	2	1	1	0	2	1
2013	2	1	2	1	2	1
2014	3	2	3	2	3	2
2015	1	1	1	1	1	1
2016	19	4	18	4	18	3
2017	13	6	12	7	13	7
2018	14	11	12	10	12	10
2019	3	3	6	6	4	4
Total	64	34	62	36	62	34

Table 6: Expired certificates found. For each year, the number of certificates expired in this year is shown. For 2019, a certificate is marked as expired if the expiry date was before the scan date.

Evaluation

Comparison with other scanners - Idea

- Perform the scan against RBG network from Internet using different scanners
  - Nmap
  - ZMap
  - Masscan
  - Prototype
- Again, Nmap’s “Top 50”
- Compare results (discovered ports) and scan times

Evaluation

Comparison with other scanners - Result

- Similar results between all scanners
- Timings differ:

Scanner	M1	M2	M3
Nmap	1166m16.330s	1140m21.640s	1201m32.521s
ZMap	7m22.056s	7m22.171s	7m24.316s
Masscan	0m47.282s	0m46.328s	0m46.280s
Prototype	96m54.420s	97m01.517s	96m58.155s

Table 7: Scan durations.

Scanner	M1	M2	M3
Nmap	1.578	1.61	1.521
ZMap	247.03	248.05	245.77
Masscan	2315.89	2372.65	2363.44
Prototype	18.73	18.83	18.73

Table 8: Discovered ports per minute.

Evaluation

Multiple nodes on same host - Idea

- User space process on Linux can have max. 1024 file descriptors
- This is the only thing limiting a scan node from going faster
- Idea: Run multiple scan node processes on a single scanning system → each process can leverage up to 1024 file descriptors

Evaluation

Multiple nodes on same host - Results

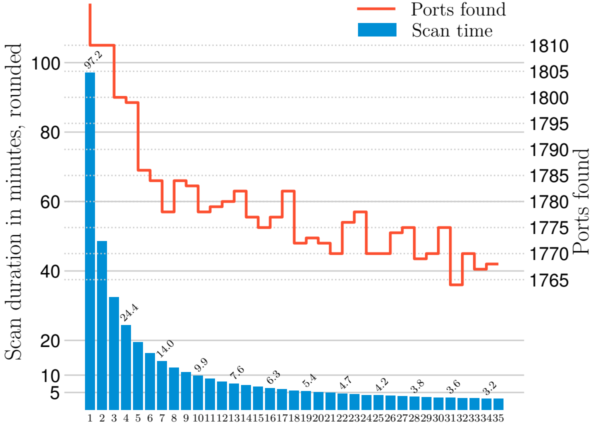


Figure 4: Scan duration in relation to the number of nodes running in parallel on a single scan system.

Last slide

Questions?

Any questions?