

Network Vulnerability Scanning

Looking from Afar

Tobias Dussa
WP8-T1

Webinar, June 2021

Public

www.geant.org

Game Plan

- Setting the stage.
- Discussing the interesting questions:
 - What to scan?
 - From where to scan?
 - How hard to scan?
- Putting it all together (and then some).
- Questions/discussion/open mike session.

Intro and Basics: What Is This Guy Talking About?!?

The Objective at Hand

- Identify vulnerable systems
- ... in your network
- ... from afar
- **and** how they are vulnerable.
- Ultimate goal:
Make sure no vulnerable systems will be compromised.

General Approach

- Find systems in your network (that you care about).
- Determine whether they are vulnerable (from wherever you are looking).
- Mitigate discovered vulnerabilities.

None of these steps is trivial!

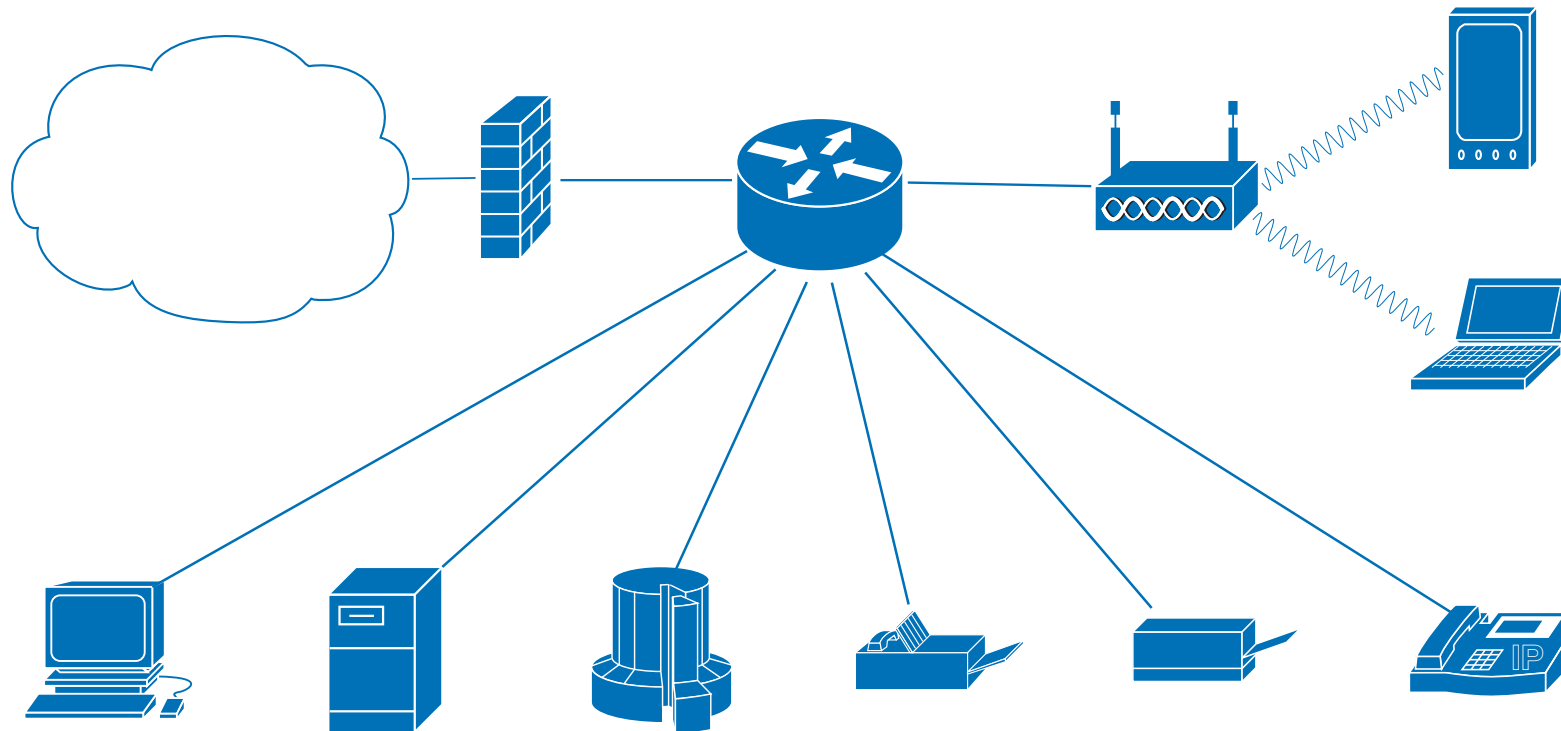
We will ignore mitigation for this talk.

Necessary Decisions Along the Way

- What systems do you care about?
- Where do you want to be looking from?
- How hard do you want to look?

Again, all of the above decisions are tricky!

The Overall Picture



Decisions, Decisions

What to Scan

- Obvious approach:
Go to the ITIL configuration management database and get a list of all devices.
- If this works for you, great!

However:

- CMDB might be outdated.
- Only managed devices listed.
- Potentially not all devices reachable (dynamic addresses).

What to Scan - Cont'd

- Alternative approach:
Scan your network ranges (nmap, zmap).
- Might work well. If it does, great again!

This is potentially not trivial either:

- IPv6 comes with **huge** address spaces, so full scans are prohibitive.
- IPv6 comes with privacy extensions → unlikely that all devices have stable IP addresses.
- MAC randomization → not even stable MAC addresses.

What to Scan - Cont'd Cont'd

- Yet another idea:

Pulling in other data sources:

- From the inside: Network equipment caches/state tables,
 - from the outside: services like `shodan.io`,
 - or “specialized” lists for particular scans (for example, SSL certificate lists for scans targeting SSL vulnerabilities).
- Likely to produce very accurate device lists.

Obviously, this requires extra effort though.

What to Scan - Some Musings

- Building device lists is, well, reconnaissance.
- Some approaches look an awful lot like black-hat attacks.
- The more devices you scan, the more vulnerable devices you might find.
- Do you care about all devices equally?
- Be sure to talk to device owners beforehand (at least for critical devices).

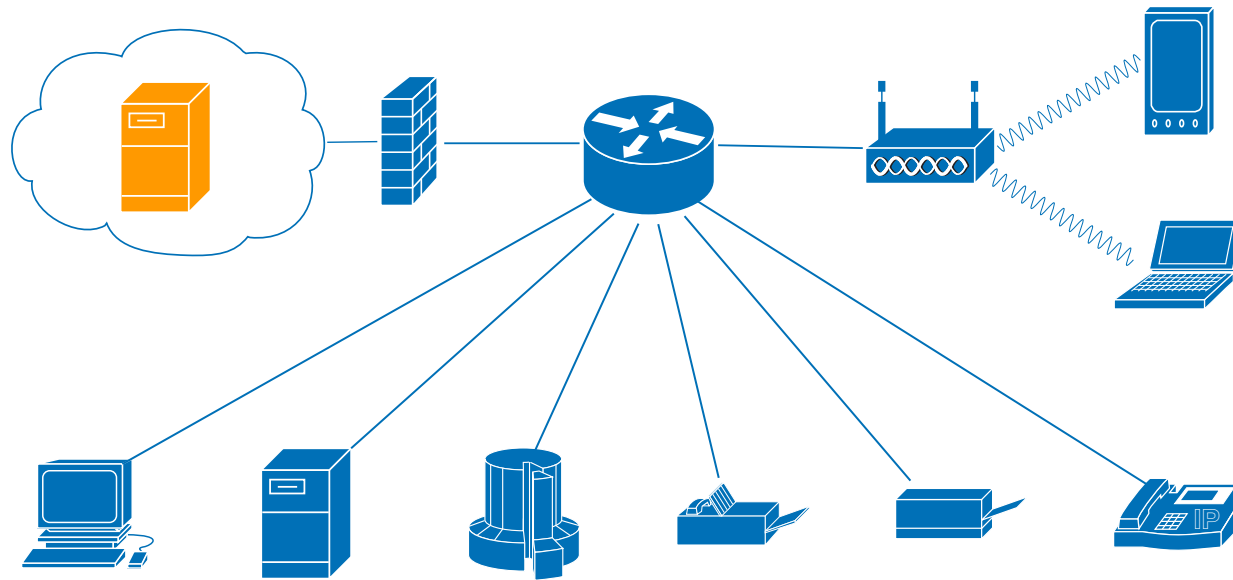
What to Scan - Wrap-Up

- More complete scans are desirable,
- **but** create a higher workload.
- Devices that you cannot act upon are at least debatable scan targets.
- Starting with the most valuable systems seems to be a sensible approach.

From Where to Scan

- This is a crucial decision!
- Essentially, three options:
 - From the outside (in other words, from outside the firewall),
 - from the inside (in other words, from inside the firewall), or
 - on the devices themselves.

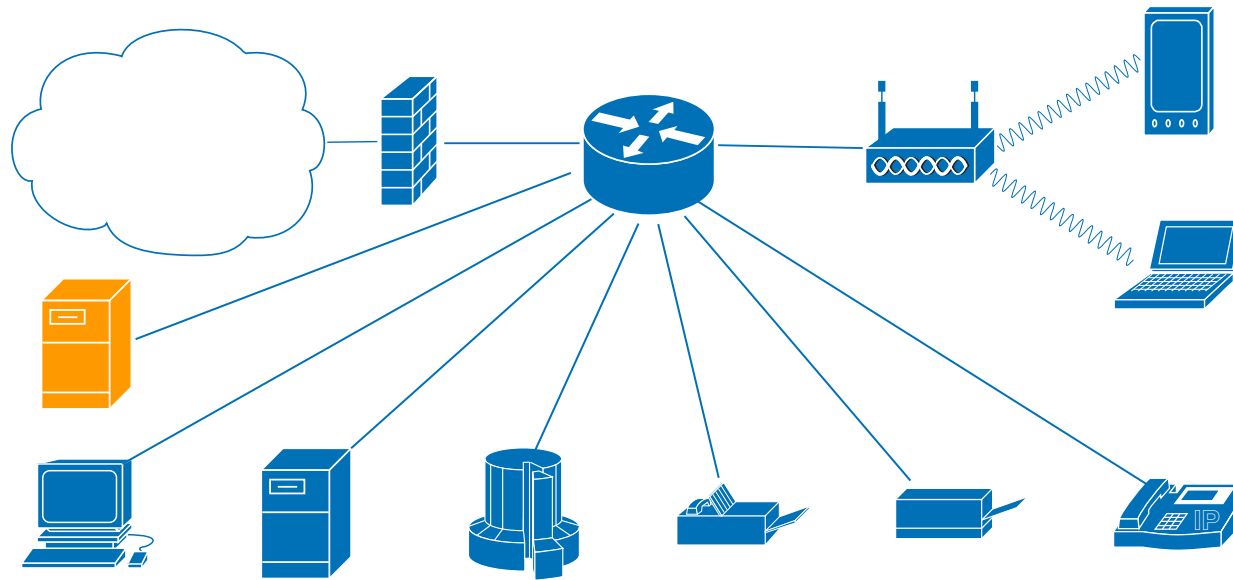
Scanning from the Outside - Overview



Scanning from the Outside - Considerations

- All network-based protections are in place and effective.
→ **Not** an complete picture of all vulnerabilities.
- Carries a significant amount of detection uncertainty.
- **However**, this is what an attacker sees.

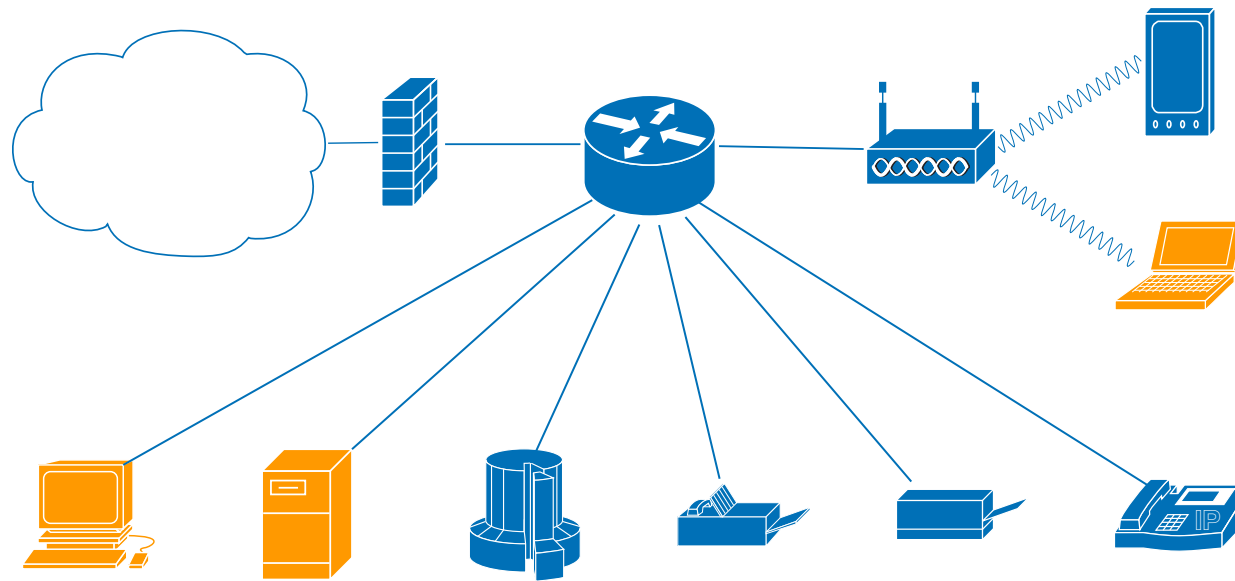
Scanning from the Inside - Overview



Scanning from the Inside - Considerations

- Scanned devices are “naked”, as no network mitigations and protections are in place.
→ Yields a more complete picture of what vulnerabilities actually exist.
- But may raise alarms that are not actually of concern.
- Also carries some detection uncertainty.

Scanning on the Devices - Overview



Scanning on the Devices - Considerations

- Best possible vantage point to detect **all** vulnerabilities.
- Detection uncertainty is small, but not zero.
- **But** requires cooperative devices!
- Locally-installed agent software might introduce new vulnerabilities.
- (Of course, all this touches local vulnerability scanning as discussed by Stefan Kelm.)

From Where to Scan - Additional Musings

- Vulnerability scans may look like actual attacks → good planning, coordination and communication is required.
- Scanning locally on the devices with agents might give you additional benefits for free (for instance, a device inventory).

From Where to Scan - Wrap-Up

- Generally speaking, scanning from “closer” to the target is preferable because of more accurate and more complete results.
- On the other hand, network security measures and mitigations need to be taken into consideration (and tested!) for good situational awareness.

How Hard to Scan

- Delicate balance:

Pushing a system harder can improve detection accuracy,

but pushing a system harder can tip it over and make the system owner mad at you.

- Be sure to consider the consequences if your scan actually (accidentally, of course) trips a system.

Wrap-Up

Final Remarks

- We have discussed
 - what to scan,
 - from where to scan, and
 - how hard to scan.
- Some (mostly) free software packages for vulnerability scanning:
 - Nessus (<https://nessus.org>) or OpenVAS/GSM (<https://openvas.org>) for (not only) network scanning,
 - Pakiti (<https://github.com/CESNET/pakiti-server>) for agent-based scanning.



Thank you

Any questions?

www.geant.org



© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).