Improving higher education network security by automating scan result evaluation with Dr. Portscan

Daniela Pöhn, Felix von Eye, Wolfgang Hommel, and Stefan Metzger
Overview

• Motivation
• Current Situation
  – DFN-CERT Net Scanner
  – Internal and External Scanner
  – Experience with Port Scans
• Dr. Portscan
  – Requirements
  – Implementation
  – Operating Mode
• Experiences and Future Work
Motivation: Munich Scientific Network

- Approx. 130,000 users
- Approx. 100,000 devices
- More than 500 buildings
- Expansion over Bavaria
- Decentral administration and system responsibility

**BUT:**

LRZ is first contact for external complaints.
Motivation

- Port scans as a proactive security measurement.
- In our scenario we have approx. 1,400 own systems.
- Simple port scans yield more than 10,000 open ports.
- Geographical and temporal distribution of port scanners lead to varying results.

→ No longer manageable manually!

→ Therefore a “Delta Reporting port scanning tool” (Dr. Portscan) is required.
Current Situation: DFN-CERT Net Scanner

Tool: nmap
Location: External
Interval: 28 days
Scan range: xxx.xxx.xxx.0/24
Ports: Approx. 2,500 TCP/UDP
Current Situation: DFN-CERT Net Scanner

- External scan for own net
- Scan interval: 28 days
- Approx. 2,300 TCP and several UDP ports
- Results shown at DFN-CERT portal
Current Situation: Hosting Provider

- **Tool**: nmap
- **Location**: External
- **Interval**: 28 days
- **Scan range**: xxx.xxx.xxx.0/24
- **Ports**: Approx. 2,500 TCP/UDP

---

- **Tool**: nmap
- **Location**: External
- **Interval**: Daily
- **Scan range**: xxx.xxx.xxx.0/23
- **Ports**: Approx. 10,000 TCP

---

DFN-CERT net scanner

Hosting Provider

Higher education network

Vulnerability-Scanner

Network management

CMS

Leibniz Supercomputing Centre
Current Situation: Internal Scanner

**DFN-CERT net scanner**
- Tool: nmap
- Location: Internal (central)
- Interval: Daily/4 hours
- Scan range: xxx.xxx.xxx.0/16
- Ports: all 65,535 TCP/UDP

**Hosting Provider**
- Tool: nmap
- Location: External
- Interval: Daily
- Scan range: xxx.xxx.xxx.0/23
- Ports: Approx. 10,000 TCP

**Network management**
- Tool: Nmap
- Location: External
- Interval: 28 days
- Scan range: xxx.xxx.xxx.0/24
- Ports: Approx. 2,500 TCP/UDP

**Higher education network**
- Tool: samhain
- Location: Internal (local system)
- Interval: 5 minutes
- Scan range: xxx.xxx.xxx.xxx/32
- Ports: 0-1,023 TCP/UDP

12.06.2014
Leibniz Supercomputing Centre
Variations within results
- Comparison scan too long ago
- Different placement of scanner

Reliability of scanner
- Determinism? (e.g., DSL connection)
- Scanner running on virtual server?

Specific services open ports dynamically
  e.g., CORBA-based services for server (only temporarily)

→ Challenge: input with high quality
Dr. Portscan: Requirements

- Support for:
  - Arbitrary amount of port scanner in the net topology
  - Variable time-delayed scans
  - Arbitrary port scanner
  - Overview and Delta-Reports

- Focus on modifications:
  - Modifications since the last scan
  - Modifications regarding point of view (internal / external)

- Modular input and export functionality
Dr. Portscan: Implementation

- Perl-based implementation
- Independent of OS
  - Preconfigured for Linux
- Storage on database with Perl::DBI
  - Perl::DBI supports major database products
  - Preconfigured for SQLite
Newly added features:

- Multi-client capability
  - Adjustable scan areas
  - Individual reporting
- Web-based and script-based control
- Git repository: https://git.lrz.de/?p=DrPortScan.git
- Please test and give us feedback!
Dr. Portscan: Operating Mode

1. Systems to scan
2. Input agents
3. Uniformed data format
4. Delta reporter
5. Output agents
6. Database

- Data sources
  1. Internal nmap
  2. DFN-CERT net scanner
- Firewall
  1. Port scan
- Blocked connection
  1. Port scan
- Portscan
  1. Port scan
- Reports to
  1. Reports to
  2. Writes to
  3. Writes to

12.06.2014
Leibniz Supercomputing Centre
Dr. Portscan: Operating Mode

Data sources:

- External scanner
  - DFN-CERT net scanner
  - nmap
- Internal scanner
  - Samhain
  - nmap
Input agents:

- Transfer results to the central Dr. Portscan instance
- Convert to a uniformed data format
  - IP address
  - Port and protocol
  - Timestamp
Results of the **Delta Reporter**: 

- No change
- New system (IP address seen for the first time)
- System does not run anymore
- Change of DNS name
- Newly opened port
- Port closed
- Port re-opened
Central Database:

- Flexibility through the use of Perl :: DBI
- SQLite preconfigured
- „History“ available in part
- Only one entry per port
- Cleanup
Output agents:

Output is available via

- **Text**
- **Mail**
- **Database access**
- **Scripts** can be triggered (e.g., for detection of open resolvers for open DNS ports)
Multi-client capability

- Adjustable scan areas
- Individual reporting
- Web based control
Experiences

- Started operating ½ year ago
- DMZ and server nets scanned on daily bases
- Positive feedback
  - Detection of new systems
  - Detection of changed ports
- Minimal effort needed for configuration
  - Could be done by clients via web frontend
Future Work

- Integration in SIEM solutions
- IPv6: Automatic detection of systems to be scanned
- More vulnerability scans
Sourcecode available:

https://git.lrz.de/?p=DrPortScan.git

or

git clone git://git.lrz.de/DrPortScan.git

Contact:

Daniela Pöhn          Felix von Eye
poehn@lrz.de          voneye@lrz.de