EGI/PRACE/EUDAT Joint Security Training

Urpo Kaila
urpo.kaila@csc.fi

ACCESS CONTROLS
SECURITY MONITORING
SECURITY WORKSHOP

SEVENTH FRAMEWORK PROGRAMME

EUDAT

Acknowledgement

- Many thanks to Ralph Niederberger r.niederberger@fz-juelich.de, EUDAT Deputy Security Officer for providing material for this presentation

ACCESS CONTROLS

- Principles of Access Controls
- Network based access controls
- Host based access controls
- Accounts based access controls
- Demo/Exercise

Principles of Access Controls

The most perhaps fundamental security control

- *Access Control domain covers mechanisms by which a system grants or revokes the right to access data or perform an action on an information system.*

- *Access Control systems include:*
  - *File permissions, such as “create,” “read,” “edit,” or “delete” on a file server.*
  - *Program permissions, such as the right to execute a program on an application server*
  - *Database access rights: No Access, Read, Read & Add, Own records only, Edit, Manage*
  - *Data rights, such as the right to retrieve or update information in a database*

EUDAT

Understanding Access Controls

- Types of controls (preventive, detective, corrective)
- Discretionary vs mandatory
- Identification, Authentication, Authorisation, Logging
- Decentralized/distributed access control techniques
- Authorization mechanisms
- Logging and monitoring

Understand access control attacks

- Treats and attack vectors
- Asset evaluation
- Vulnerability management
- Aggregation of multiple credentials

EUDAT

Types of Access Controls

- Administrative
- Technical
- Physical

- Preventive
- Detective
- Corrective
- Recovery

The Bell–LaPadula model

- A classical Access contol model
- The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:
- The Simple Security Property - a subject at a given security level may not read an object at a higher security level (**no read-up**).
- The ★-property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (**no write-down**).
- The Discretionary Security Property - use of an access matrix to specify the discretionary access control.

Source: wikipedia

Access Controls for accounts

- Authentication -> weak/strong/open?
- Account locking
- Monitoring
- Processes
- EULA/Terms of use
- Abuse/CSIRT

Enforcement for privacy protection BDSG (Attachment to §9 part 1)

1. Access control: against unauthorized physical access to IT resources
2. Access control: against unauthorized usage access to IT resources
3. Access control: Defining roles of access (provide adequate priviledges (not root at all)
4. Access control: Secure transmissions and storage of data
5. Log control: Store information, who access the data (time, kind of access; storage, change, deletion)
6. Control of order-data processing: Securing access to data in accordance to terms of contracts (i.e „Outsourcing“)
7. Availability control: Guarantee that data is available and not corrupted
8. Separation control: Ensure data is not mixed if collected for different purposes

BDSG = Bundesdatenschutzgesetz (German Data Protection Law)

By Ralph Niederberger - r.niederberger@fz-juelich.de

EUDAT

Access Controls and Compliance 1 (2)

ISO/IEC 27001:2005

11.1 Business Requirement for Access Control
11.1.1 Access control Policy

11.2 User Access Management
11.2.1 User Registration
11.2.2 Privilege Measurement
11.2.3 User password management
11.2.4 Review of user access rights

11.3 User Responsibilities
11.3.1 Password Use
11.3.2 Unattended user equipment
11.3.3 Clear Desk and Clear Screen Policy

EUDAT

Access Controls and Compliance (2)

11.4 Network Access control
11.4.1 Policy on use of network services
11.4.2 User authentication for external connections
11.4.3 Equipment identification in networks
11.4.4 Remote diagnostic and configuration port protection
11.4.5 Segregation in networks
11.4.6 Network connection control
11.4.7 Network Routing control
11.5 Operating System Access Control
11.5.1 Secure Log-on procedures
11.5.2 User identification and authentication
11.5.3 Password Management system
11.5.4 Use of system utilities
11.5.5 Session Time-out
11.5.6 Limitation of connection time
11.6 Application access control
11.6.1 Information access restriction
11.6.2 Sensitive system isolation
11,7 Mobile Computing and Teleworking
11.7.1 Mobile computing and communication
11.7.2 Teleworking

EUDAT

Network based Access controls

What are they?

EUDAT

Firewalls

- Control traffic and deny unwanted traffic concerning defined rules at the entrance to your corporate network
- Firewall requirements:
  - Should be fast enough (no time delays)
  - Mostly free communication from inside to outside, but only real needed communication from outside to inside
  - Implement as much security as possible
  - Minimize time and effort for sysadmins
  - Be sure to secure any communication path to your network
- Available solutions:
  - Different solution available. You can choose dependend on time, money, and expertise

By Ralph Niederberger - r.niederberger@fz-juelich.de

Personal Firewalls

- For local security policy control use Personal Firewalls and/or TCP-Wrappers
- Those can be configured to personal needs
- Allows to implement a more secure polica than for the one defined for your corporation
- Additionally implements protection against internal threats.
- Logging on host level possible

- Examples:
  - Kaspersky Virus scanner
  - Avira AntiVir
  - TCP-Wrapper
  - Windows 7-Firewall
  - Iptables for LINUX

By Ralph Niederberger - r.niederberger@fz-juelich.de

Iptables

Man iptables

Iptables is used to set up, maintain, and inspect the tables of IPv4 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.

Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.

- a statefull firewall

- Ipv6tables, xtables….
- UI´s, such as ufw

Iptables exercise

Login in on your host and perform the following tasks (with sufficient credential):

1. What is your current iptables rules?
2. Install apache (use yum or apt-get, depending on your platform) and start it to run on port 80
3. Check if you can access port 80 from localhost and from a remote host
4. Deny access to port 80 to your remote host
5. Check that access was denied

Iptables exercise 2

6. Allow established traffic
7. Allow ssh only from localhost and remote host; http and ICMP from everywhere, deny rest
8. Limit http to 50 connections*
9. Limit traffic to 50 established connections*

* We do this with iptables only, no need to touch httpd conf yet

Host based access controls?

What are they?

EUDAT

sshd_config

- Man sshd_config
- Best practices:
  - Allow only SSH2
  - Limit root access (source, keys only)
  - Disable/limit host.based authentication
  - Warning banner
  - Disable empty passwords
  - Use tcpwrappers
  - Mitigate brute-force attacks

Other host based access controls

- /etc/hosts.allow
- /etc/hosts.deny
- /etc/passwd, /etc/shadow
- /etc/groups
- Grub.conf
- /etc/login.defs
- Selinux
  - Enforcing/Permissive/Disabled
- Directory rights and ownerships

Exercise/ host based access controls

- On your host:
  - Enable sshd best practices
    - Install failtoban ,allow five failed logins
    - Test, test ,test
  - Examine
    - Your other host based configuration
    - freese (nologin) unneccesay accounts
    - Require 8 char passwords not older than 6 months

SECURITY MONITORING

- Availability monitoring
- Port Scans
- Integrity checks
- Penetration testing

Availability monitoring

- The A in the CIA ‘formula’
- Availability is mostly way security interfaces with the rest of their organisation?
- How many ‘nines’ do we need? (see wikipedia ;)

Availability %	Downtime per year	Downtime per month*	Downtime per week
90% ("one nine")	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
97%	10.96 days	21.6 hours	5.04 hours
98%	7.30 days	14.4 hours	3.36 hours
99% ("two nines")	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% ("three nines")	8.76 hours	43.8 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds

EUDAT

Example of Availability Monitoring/EGI

NGI	Availability Aug-2013	Reliability Aug-2013	Availability Jul-20132	Availability Jun-20132
Albania	NA	NA	NA	NA
Armenia	98,8%	98,8%	79,1%	93,2%
AsiaPacific	98,0%	100,0%	100,0%	99,8%
Austria	100,0%	100,0%	100,0%	100,0%
Belarus	NA	NA	NA	NA
Bosnia Herzegovina	98,5%	98,5%	95,3%	99,4%
Bulgaria	99,7%	99,7%	91,1%	99,6%
CERN	99,9%	99,9%	98,5%	100,0%
Croatia	100,0%	100,0%	100,0%	100,0%
Cyprus	100,0%	100,0%	100,0%	88,3%
Czech Republic	100,0%	100,0%	99,9%	100,0%
Denmark	NA	NA	NA	NA
Estonia	NA	NA	NA	NA
FYR Macedonia	97,1%	97,1%	99,2%	100,0%
Finland	NA	NA	NA	NA

SITE	NGI	LINE CHART	GANTT CHART	AVAILABILITY	RELIABILITY
CSC	NGI_FI			99.56	99.56
FI_AA	NGI_FI			96.69	96.69
				.00	100.00
FI_Helsinki	NGI_FI			100.00	100.00
FI_JYU	NGI_FI			100.00	100.00
FI_LUT	NGI_FI			97.22	97.22
FI_Oulu	NGI_FI			100.00	100.00
FI_TUT	NGI_FI			100.00	100.00
FI_UEF	NGI_FI			99.86	99.86
FI_UTU	NGI_FI			100.00	100.00

EUDAT

Port Scans

- A good tool to identify risky services
- Should be run regularly
- Use netcat, nessus, …
- It is important to manage the results of the scans
  - Policy!
  - Who is In charge of changes

Intrusion Detection Systems

- Analyses traffic on suspicious patterns, which indicate possible attacks (e.g. port scans)
- Located somewhere in your network, so that communication streams can be read. Not able to stop traffic, only reactive behaviour (see IPS below)
- Requirements on Intrusion Detection Systems (IDS):
  - Fast, so that any traffic can be scanned
  - Always up-to-date virus database needed
  - Easy to configure (only small time efforts, well organized management
  - Prozedural analysis possible
  - Interaction with firewall appriciated
- Available solutions:
  - Different solution available. You can choose dependend on time, money, and expertise

By Ralph Niederberger - r.niederberger@fz-juelich.de

Intrusion Prevention Systeme

- Similar to Intrusion Detection System
- Analyses traffic on suspicious patterns, which indicate possible attacks (e.g. port scans)
- Located within communication stream, forwards data only after scanning it, i.e. proactive behaviour
- Requirements on Intrusion Prevention Systems (IDS):
  - Fast, so that any traffic can be scanned
  - Always up-to-date virus database needed
  - Easy to configure (only small time efforts, well organized management
  - Procedural analysis needed; should work without admin interaction
  - Interaction with firewall appriciated (in principle it is a FW already)
- Available solutions:
  - Different solution available. You can choose dependend on time, money, and expertise

By Ralph Niederberger - r.niederberger@fz-juelich.de

Security Monitoring and Compliance

ISO/IEC 27001:2005
6.1.8 Independent review of information security
7.1 Responsibility for Assets
8.1.1 Roles and Responsibilities
8.2.1 Management Responsibility
8.2.2 Information security awareness, education and training
8.2.3 Disciplinary process
8.3 Termination or change of employment
8.3.1 Termination responsibility
8.3.2 Return of assets
8.3.3 Removal of access rights
9.1.1 Physical security Perimeter
11.2.4 Review of user access rights
… and many more!

EUDAT

Security Audits and Security Exercises

EUDAT

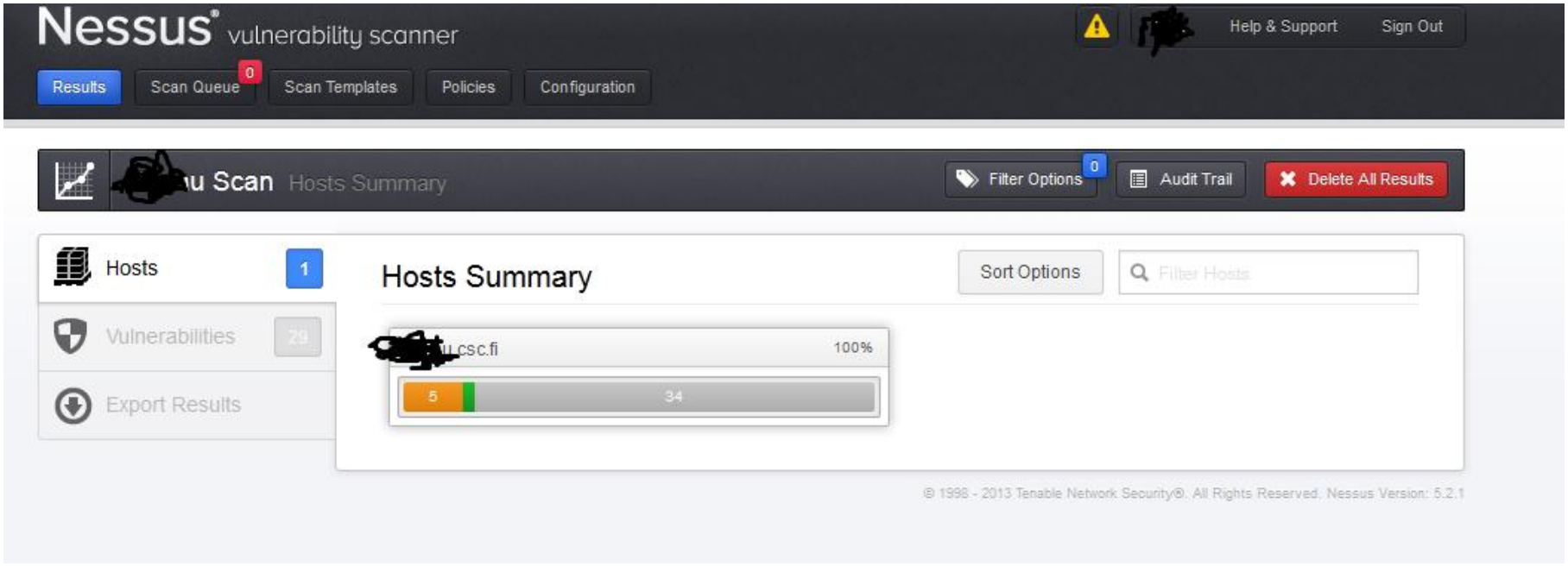
Internet Security Scanner (ISS) /Nessus

Objective: **To be faster than a hacker**

- Checks all/important hosts/server within your infrastructure on security vulnerability
- Automatic Up-Date of pattern database
- Automatic generation of vulnerability reports
- Analysis of hosts on admin request or automatically if a service on the host is accessible from outside
- Vulnerability report will be send to admin of system

By Ralph Niederberger - r.niederberger@fz-juelich.de

EUDAT


Nessus vulnerability scanner
Help & Support
Sign Out
Results
Scan Queue
0
Scan Templates
Policies
Configuration
Scan Hosts Summary
Filter Options
0
Audit Trail
Delete All Results
Hosts
1
Vulnerabilities
29
Export Results
Hosts Summary
Sort Options
Filter Hosts
csc.fi
100%
5
34
© 1998 - 2013 Tenable Network Security®. All Rights Reserved. Nessus Version: 5.2.1

Integrity checks

- File Integrity checks
  - Tripwire
  - AIDE
  - Check www-securityfocus.com -> Tools – Auditing - > File Integrity
- Accounts
  - Compare with well known good state
- Services, mounts,
  - ps, strace, lsof, netstat, w,…
  - Compare with well known good state
- Packet integrity
  - Use you packet management tool (rpm, apt)
  - rpm -v
- If we have time: Download Nessus Vulnerability Scanner Home edition, free for personal use – and check your host!

- Use your commons sense in all exercises!

EUDAT

Other useful sources of information

- **Utmp -** *current* status of the system, system boot time (used by *uptime*), recording user logins at which terminals, logouts, system events etc.
- **wtmp** acts as a historical utmp
- **btmp** records failed login attempts

- SYSLOG!
  - Facility/severity
  - Access log
  - Error.log

Exercises/ Security Monitoring

- Do a port scan your host
  - nc -z myhost 1-1023
  - # nmap -v -sS 192.168.0.0/24
  - # nmap -v -sT 192.168.0.0/24
- Install and test tripwire, create a baseline
- Check network status
  - net, ifconfig
- Check mounted filesystems and open files
  - Mount, lsof, ps
- Check user accounts
  - Id, finger, history, utmp, wtmp, last

Policies and Best Information Security Practices for Scientific Infrastructures and Sites/ EUDAT

- EUDAT Security Policy
- EUDAT Security Organisation
- EUDAT CSIRT and IH
- EUDAT ToU and SLA
- EUDAT Service Security Assessment

Incident Handling and Coordination

- EUDAT – current status