Forensics 1: Auditing and Intrusion Detection

Kresten Jacobsen

Intro to System Security

Goals

Prevention

Detection

Recovery

C-I-A

Confidentiality

Integrity

Availability

Threats

Snooping

Modification

Spoofing

Repudiation of Origin

Denial of Receipt

Delay

Security Policies

Requirements

- Common understanding (implicit / explicit)
- Trust (in people and computers)
- Assumption (that policies are enforced)

Policy types

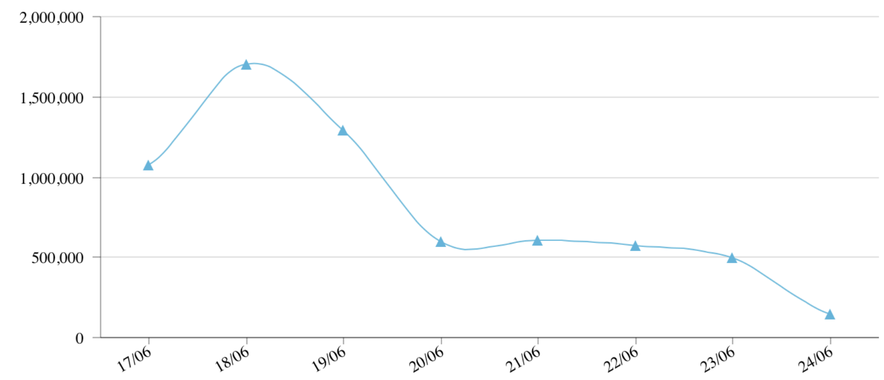
- Confidentiality
- Integrity Policy
- Availability Policy

Auditing

- Logging
  - Recording of events
  - Problem: What do we log?
- Auditing
  - Analysis of records
  - Problem: What do we look for?
  - Notification

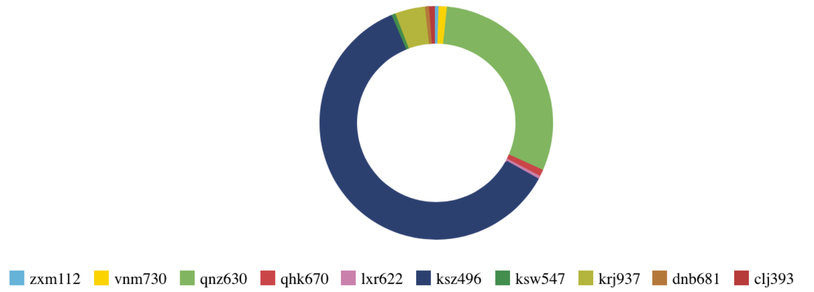
Example Dashboard

UNICPH: Active Directory: Logon failures



Jun 24 08:44 AM - Jun 24 08:45 AM

UNICPH: Active Directory - Logon failures - Top accounts

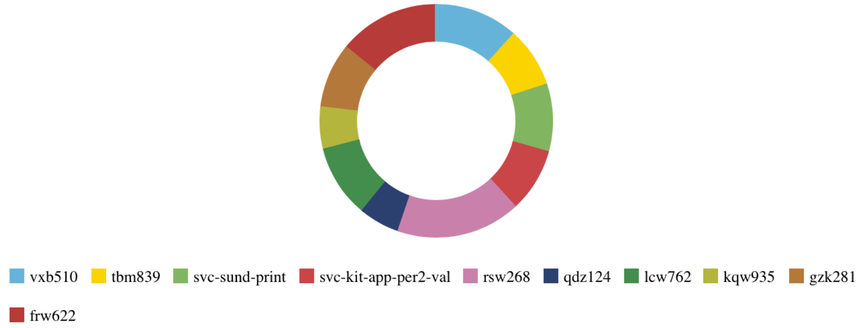


Jun 24 08:44 AM - Jun 24 08:45 AM

UNICPH: Active Directory - Latest users added to groups

event_datetime	dest_user_name	object_name
Jun 24 08:37:22 AM	KU-Post-Student	CN=gnm931,OU=Active,OU=KU Users,DC=unicph,D
Jun 24 08:36:49 AM	KU-Post-Student	CN=cnq140,OU=Active,OU=KU Users,DC=unicph,D
Jun 24 08:36:49 AM	KU-Post-Student	CN=xsr906,OU=Active,OU=KU Users,DC=unicph,DC
Jun 24 08:36:48 AM	KU-Post-Student	CN=kxj450,OU=Active,OU=KU Users,DC=unicph,DC
Jun 24 08:36:47 AM	KU-Post-Student	CN=chq482,OU=Active,OU=KU Users,DC=unicph,D
Jun 24 08:36:09 AM	KU-Post-Student	CN=pkb171,OU=Active,OU=KU Users,DC=unicph,D
Jun 24 08:36:09 AM	KU-Post-Student	CN=rhq214,OU=Active,OU=KU Users,DC=unicph,DC
Jun 24 08:36:08 AM	KU-Post-Student	CN=blh555,OU=Active,OU=KU Users,DC=unicph,DC
Jun 24 08:36:08 AM	KU-Post-Student	CN=rxs292,OU=Active,OU=KU Users,DC=unicph,DC
Jun 24 08:29:30 AM	KU-Enrolled-Student	CN=ndv657,OU=Active,OU=KU Users,DC=unicph,D

User Account Locked out - top 10 accounts



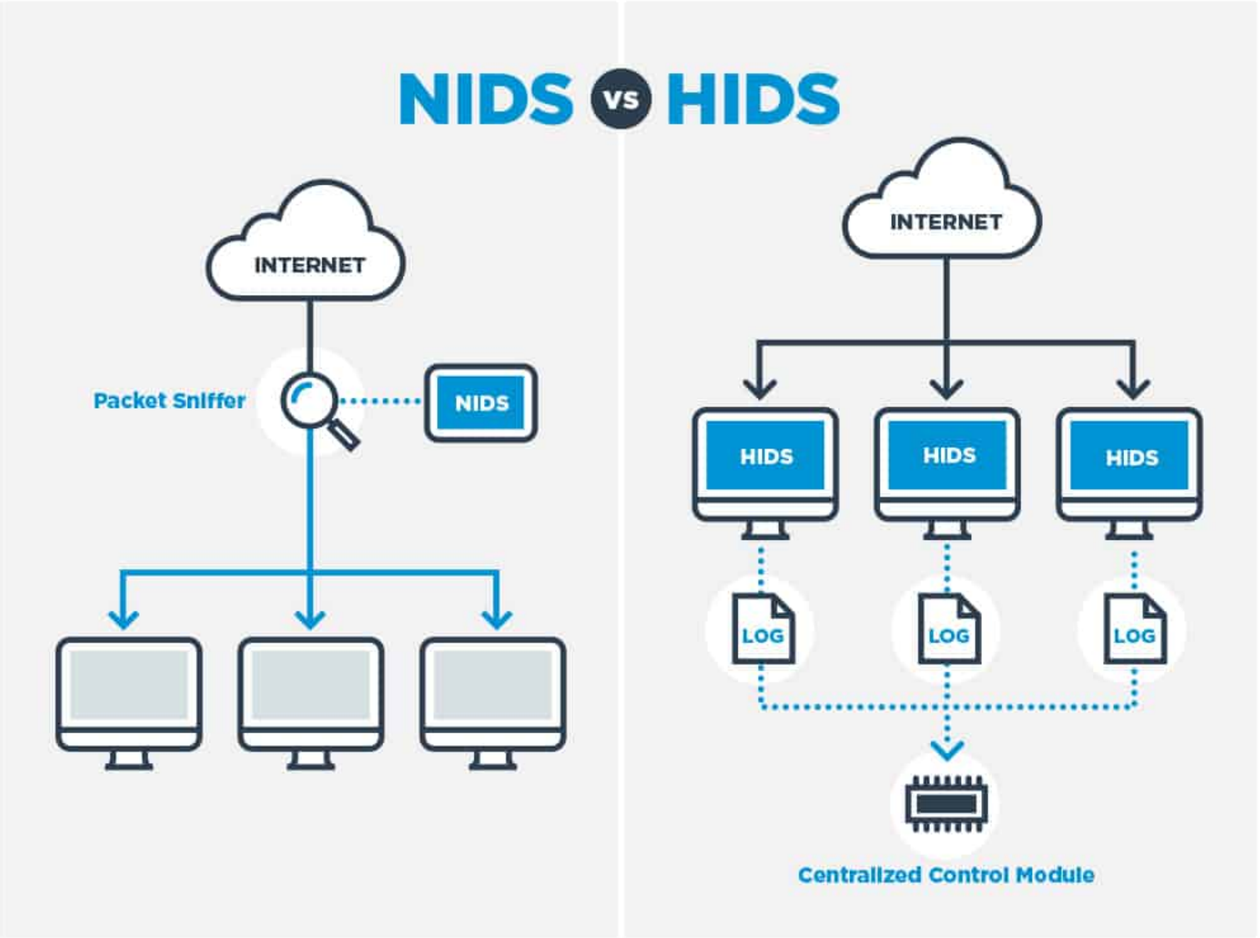
Jun 24 08:44 AM - Jun 24 08:45 AM

Intrusion Detection

- Methods
  - Signature-based detect *known attacks*
  - Anomaly-based detect *unknown attacks*
- Tools
  - Network intrusion detection systems (NIDS)
  - Host intrusion detection systems (HIDS)

Intrusion detection systems

- Network intrusion detection systems (NIDS)
  - Monitoring network traffic
- Host intrusion detection systems (HIDS)
  - Monitoring host traffic and filesystems / operations




Forensics 1: Auditing and Intrusion Detection
Auditing
Logging
Recording of events
Problem: What do I log?
Auditing
Analysis of records
Problem: What do I look for?
File system forensics
Volatile (disks break)
Tools to recover deleted files
Intrusion detection
Get an overview
Collect from multiple sources
Routers
Firewalls
Servers
Access control systems
Centralize!
Look at top-10 and bottom-10