

Security Workshop UVsec

Netzwerküberwachung mit Hilfe von Distributed Intrusion Detection Systems (DIDS)

uwe.grawert@rz.hu-berlin.de

Gliederung

- Erläuterung (Was ist ein IDS)
- Verschiedene Angriffsarten
- Aufbau eines IDS
- Arbeitsweise und Wirkungsgrad
- Voraussetzungen für den Einsatz



Was ist ein IDS

- Erkennt Angriffe auf das eigene Netzwerk
- Erkennt Abweichungen des normalen Netzwerkbetriebes
- Prüft die festgelegte Netzwerkkonfiguration

Was wird erkannt

- Portscans
  - Sammeln von Informationen über das Netzwerk
  - Angriffsziele suchen (offene Ports)
- Attacken auf Server
  - Exploit (Ausnutzen von Software- und Konfigurationsfehlern)
  - Trojaner (unerwünschte Anlaufstelle auf dem eigenen Server)
  - Viren und Würmer
- Anomalien
  - Denial of Service (Blockierung des Dienstes)
  - Scan des Netzwerks nach einem bestimmten Dienst

Prüfung der Netzkonfiguration



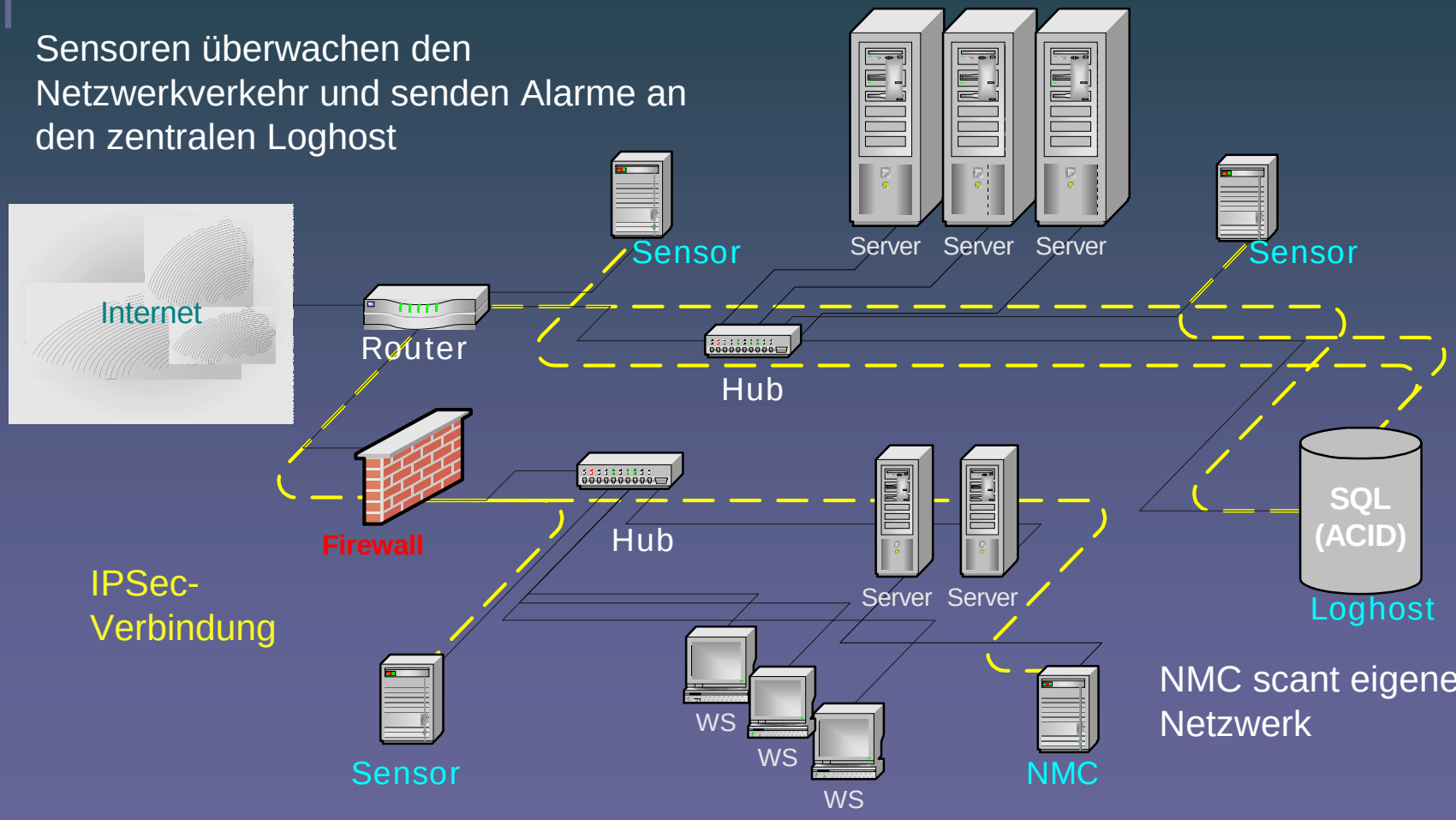
- Welches Betriebssystem läuft
- Welche Version der Software läuft
- Welche IP-Adressen werden benutzt
- Prüfung der Server auf Verwundbarkeit

Wozu IDS im HU-Netz

- Ergänzung des Firewall-Konzeptes
- Sammeln von Informationen über das Netzwerk
- Erkennen von Gefahren
- Schnelles Reagieren bei Gefahren

Aufbau eines IDS

Sensoren überwachen den Netzwerkverkehr und senden Alarme an den zentralen Loghost



Komponenten (Open-Source

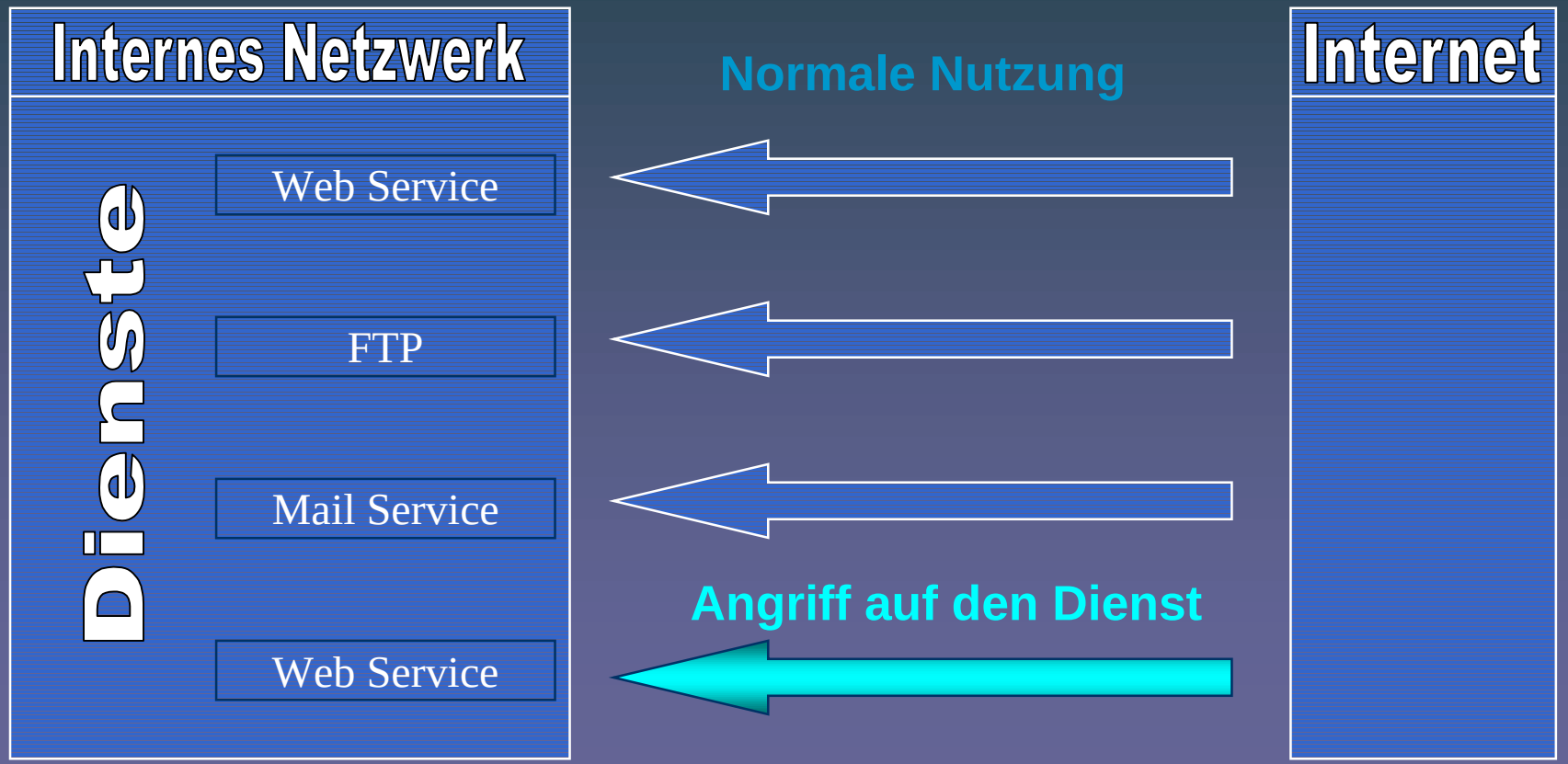


- Sensoren (Snort)
  - Untersuchung des Netzwerkverkehrs
- NMC (Network Management Console)
  - Scan des eigenen Netzwerks mit Nmap
  - Testangriffe auf die eigenen Server mit Nessus
- Loghost (Datenbank)
  - Sammeln und Bereitstellen der Daten mit PostgreSQL und ACID

Genutzte Software

- Snort (IP-Paket Sniffer)
- ACID (Analysis Console for Intrusion Databases)
- PostgreSQL (Datenbank)
- Nmap (intelligenter Netzwerkscanner)
- AIDE (prüft Integrität des Dateisystems)
- Nessus (Angriffstool)
- Nlog (Web-Interface für Nmap)

Angriff auf einen Server



Erkennen des Angriffs

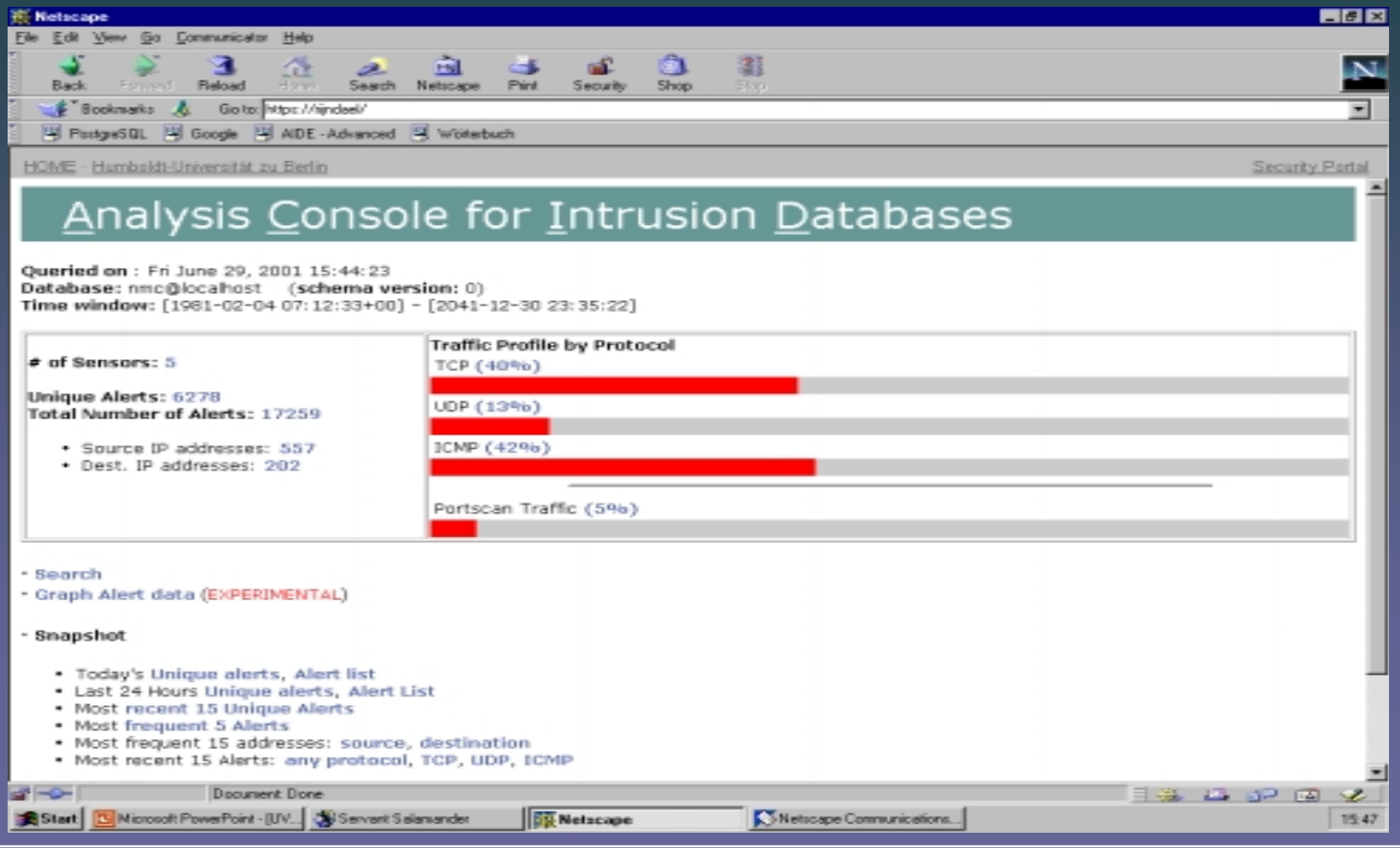


IP Header:
Source Address
Destination Address
Flags
Daten:
Angriffsmuster

Regelwerk von Snort:
Alert tcp any -> tcp 21 (content:“Angriffsmuster“;)
Alert tcp any -> tcp 23 (content:“Angriffsmuster“;)
Alert tcp any -> tcp 53 (content:“Angriffsmuster“;)
Alert tcp any -> tcp 80 (content:“Angriffsmuster“;)
Alert tcp any -> tcp 447(content:“Angriffsmuster“);
...
...
...
...
...

UVsec

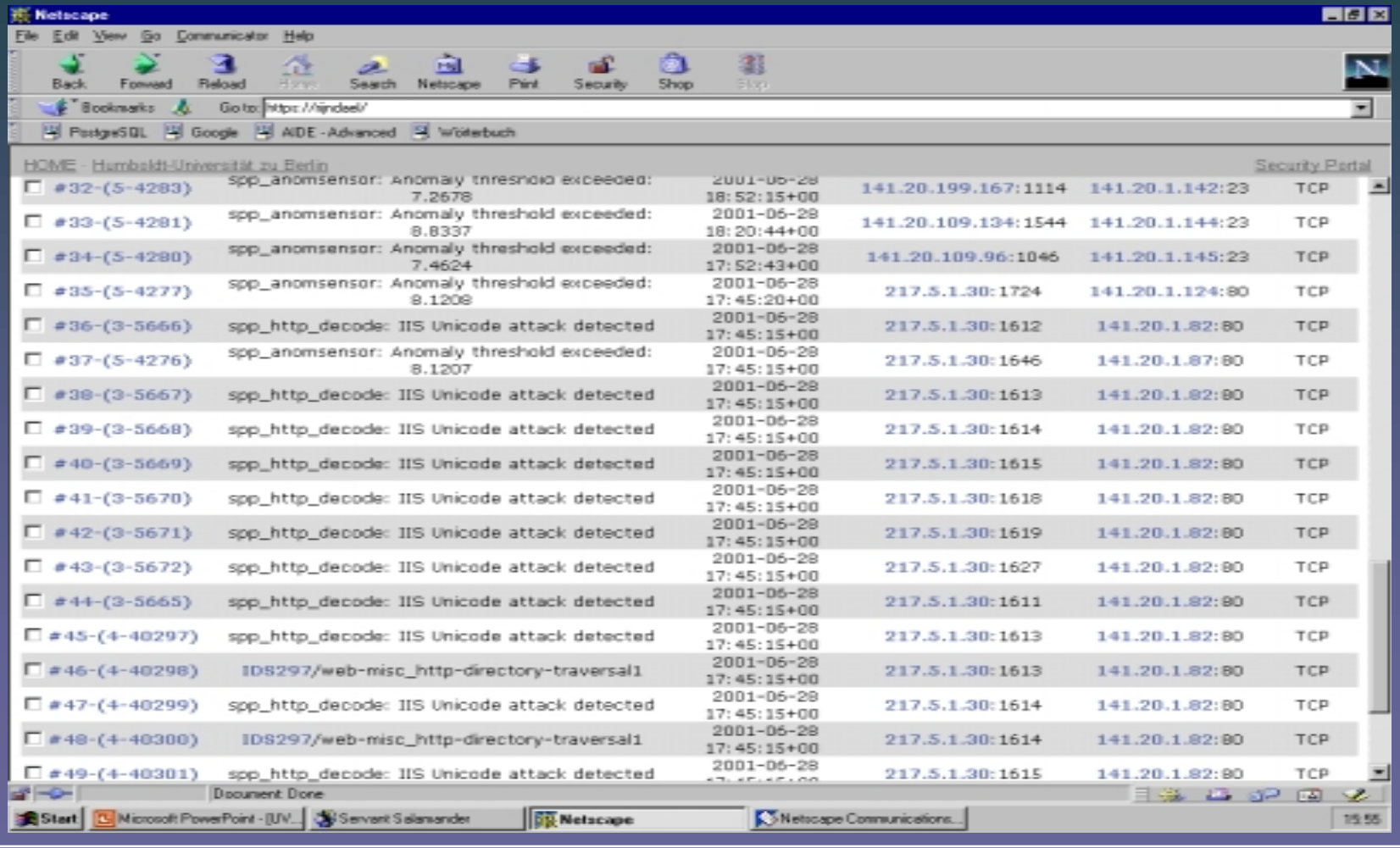
Web-Interface (ACID)



UVsec



Web-Interface (ACID)



Technische Voraussetzungen



- Daten müssen unverschlüsselt passieren
- Datenpakete müssen für den Sensor erreichbar sein
- Anpassung an die Netzwerkdienste
- Regelwerk muss aktualisiert werden

Rechtliche Voraussetzungen

- Mitbestimmung des Personalrates

  (Personalvertretungsgesetz §85 Abs. 2 Ziffer 8-9)

- Gewährleistung des Datenschutzes durch Vier-Augen-Prinzip

  (gemeinsame Entscheidung über Zugang und Auswertung)

- Ergänzung: Datenschutzaudit

  (Prüfung der technischen und organisatorischen Maßnahmen)

Danke Schön

Fragen ?