Greenbone Appliance am IT Center

Erste Erfahrungen mit einem Schwachstellenscanner

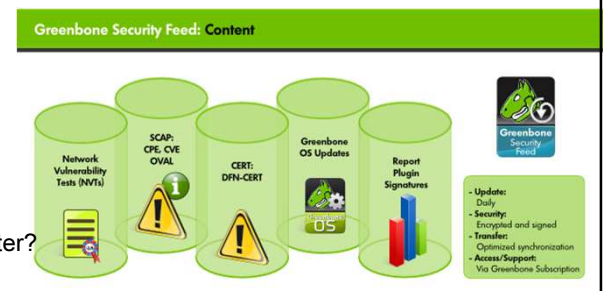
Guido Bunsen

IT Center der RWTH Aachen University

Greenbone Applicance

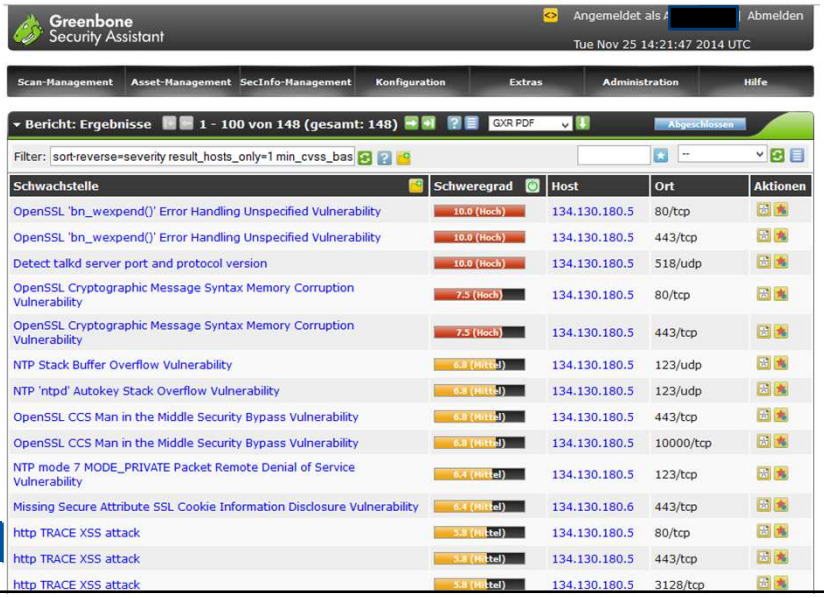
- **Schwachstellenmanagement**
  - → Wo sind Schwachstellen?
  - → Welche Schwachstellen?
  - → Wie kann man sie schließen?

- **Basis ist eine DB mit bekannten Schwachstellen**



- **Wir gewinnen Übersicht**
  - → Wo stehen wir?
  - → Trends?
  - → Wird es besser? Schlechter?

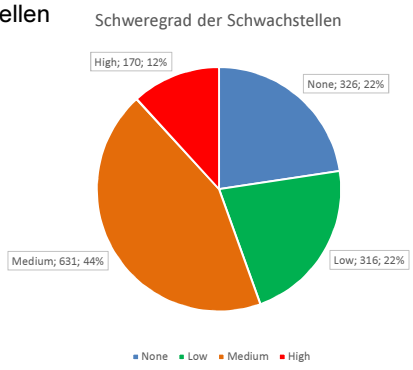
Beispiele (Wohnheim)



Schwachstelle	Schweregrad	Host	Ort	Aktionen
OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability	10.0 (Hoch)	134.130.180.5	80/tcp	
OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability	10.0 (Hoch)	134.130.180.5	443/tcp	
Detect talkd server port and protocol version	10.0 (Hoch)	134.130.180.5	518/udp	
OpenSSL Cryptographic Message Syntax Memory Corruption Vulnerability	7.5 (Hoch)	134.130.180.5	80/tcp	
OpenSSL Cryptographic Message Syntax Memory Corruption Vulnerability	7.5 (Hoch)	134.130.180.5	443/tcp	
NTP Stack Buffer Overflow Vulnerability	6.8 (Mittel)	134.130.180.5	123/udp	
NTP 'ntpd' Autokey Stack Overflow Vulnerability	6.8 (Mittel)	134.130.180.5	123/udp	
OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8 (Mittel)	134.130.180.5	443/tcp	
OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8 (Mittel)	134.130.180.5	10000/tcp	
NTP mode 7 MODE_PRIVATE Packet Remote Denial of Service Vulnerability	6.4 (Mittel)	134.130.180.5	123/tcp	
Missing Secure Attribute SSL Cookie Information Disclosure Vulnerability	6.4 (Mittel)	134.130.180.6	443/tcp	
http TRACE XSS attack	5.8 (Mittel)	134.130.180.5	80/tcp	
http TRACE XSS attack	5.8 (Mittel)	134.130.180.5	443/tcp	
http TRACE XSS attack	5.8 (Mittel)	134.130.180.5	3128/tcp	

Erste Ergebnisse im Dez. u. Jan.

- **Stichtag 18. Januar:**
  - → 2255 IP-Nummern haben eine Freischaltung in der ext. Firewall
  - → 1443 lieferten beim Scannen einen Report
  - → 170 hatten schwerwiegende Schwachstellen -> Handlungsbedarf
  - → 631 hatten mittelschwere Schwachstellen



Bewertung von Servern mit Zugang aus dem Internet

Ziel: Mehr Grün, weniger Rot

Weitere Planung

- **Regelmäßiger Scan aller Server mit Freischaltung in der Firewall in ca. monatlichem Rhythmus**
- **Bereitstellung der Ergebnisse an die verantwortlichen Administratoren**
- **Ausweitung der Scans auf „kritische Infrastruktur“**

- **Fragen?**

Metrik CVSS

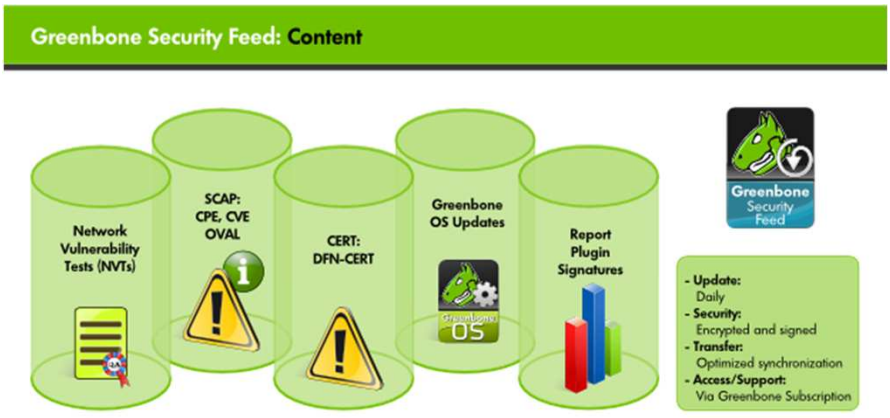
- **Berechnung Basis-CVSS**
  - → Verwertbarkeit der Schwachstelle
    - →Zugangsvektor (Physikalischer Zugang, Broadcast Domain, Internet)
    - →Komplexität in der Ausnutzung (Low, Medium, High)
    - →Authentifizierung erforderlich
  - → Auswirkungen (None, Partial, Complete)
    - →Vertraulichkeit
    - →Integrität
    - →Verfügbarkeit

Greenbone Applicance

- **Schwachstellenmanagement**
  - → Wo sind Schwachstellen? Welche Schwachstellen haben wir? Wie kann man sie schließen?
- **Übersicht**
  - → Wo stehen wir? Wird es besser oder schlechter?

Mehrwert im Abo…

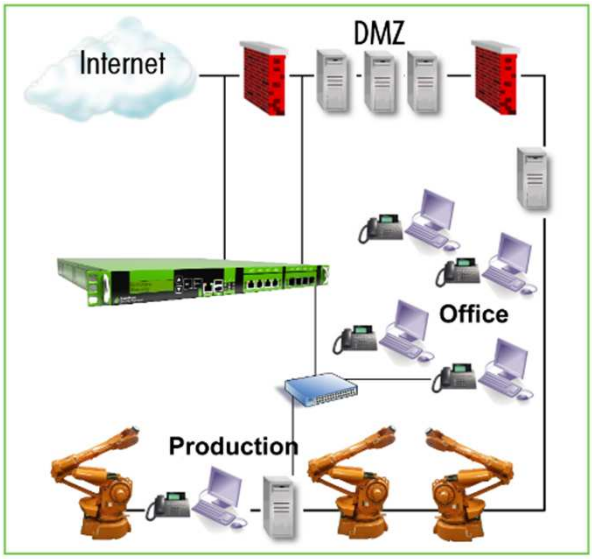
- **Details über mehr als 40.000 Schwachstellen:**



- Common Platform Enumeration (CPE)
- Security Content Automation Protocol (SCAP)
- Common Vulnerabilities and Exposures (CVE)

Greenbone in der Gesamtarchitektur

- **Arbeitsschritte**
  - → Portscan
  - → Discovery
  - → Schwachstellen identifizieren
  - → Report erstellen
  - → Admin informieren
- **Verschiedene Views bzw. Perspektiven**



Konfiguration der Appliance

- **Leihgabe von TUDD / begrenzte Leistungsfähigkeit / Kein Support**
- **Bislang Einbindung der Appliance in ein eigenes „Scannernetz“**
- **Geplant sind „Beinchen“ in verschiedenen Netzen:**
  - → Vor der Firewall (Sicht des Außentäters)
  - → Im unpriviligierten Netz innerhalb der Hochschule (z.B. Eduroam / Sicht des Innentäters)
  - → Im NOC-Netz (weitgehend ungehinderter Zugang)
- **Bisher erworbene Skills: Scriptgesteuerte Einrichtung von Tests und Scriptgesteuerte Auswertung von Tests**
- **Erfahrung mit Nutzern in der RWTH war im Okt./Nov. 2014 positiv**

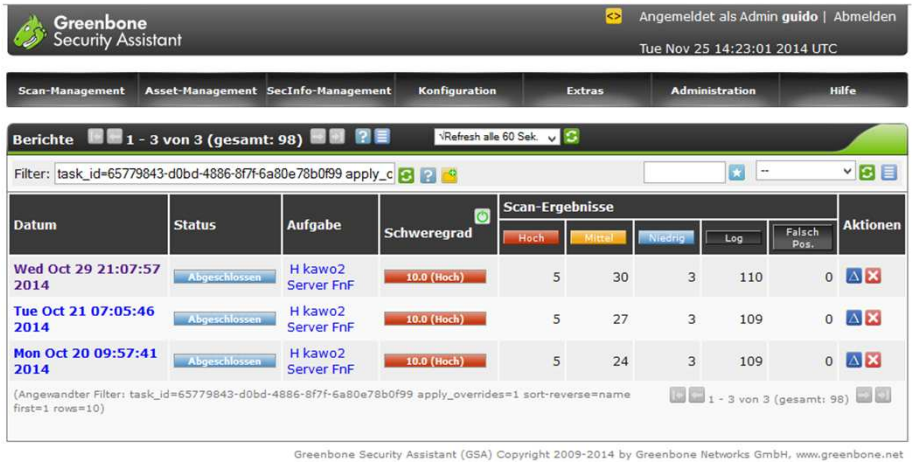
Einsatzszenarien

- **Initialer und dann regelmäßiger Schwachstellenscan für Geräte mit Freigaben in der Firewall**
  - → Verknüpfung mit Changemanagement (Lifecycle von Freigaben)
  - → Durchführung der Freigaben ev. an Scanergebnis gekoppelt
  - → Automatische Übermittlung von Schwachstellen an zuständige Admins / Verknüpfung mit Ansprechpartnern in Netzdatenbank/Verinice
- **Regelmäßiger Discovery-Scan des Hochschulnetzes von „außen“ um die Perspektive eines Angreifers einzunehmen.**
  - → Stimmt die Sicht mit der CMDB überein?
- **Regelmäßiger Discovery-Scan von schutzbedürftigen Netzen aus NOC-Perspektive**
  - → Scan nach Geräten, ev. nach Softwarepaketen
  - → Stimmt die Sicht mit der CMDB überein?

Einsatzszenarien 2

- **Verknüpfung von Scanergebnissen mit Nagios**
  - → Alarmierung ist etabliert
  - → Admins kennen und nutzen Nagios
- **Verknüpfung mit Verinice**
  - → Informationen über gefundene Schwachstellen und umgesetzte oder nicht umgesetzte Sicherheitsmaßnahmen gebündelt
- **Verknüpfung mit Webshop**
  - → Anforderung von Scans…

Beispiele 2 (Kawo)



Beispiele 3 (ZHV)