SoSe 2017

Prüfungsinhalte Praktische NW-Sicherheit (Wahlpflicht)

1 Allgemeine Hinweise

Wie zuvor besprochen sind zwei DIN A4 Seiten (d.h. ein Blatt mit Vor- und Rückseite oder zwei einzelne Blätter mit je einer beschrifteten Seite) mit handschriftlichen Aufzeichnungen als Hilfsmittel bei der Klausur zugelassen. Einige wenige Grafiken dürfen ausgedruckt sein.

Die Klausur wird über 90 Minuten geschrieben, die Fragen teilen sich auf in verschiedene Arten, von der Abfrage bestimmter Schlüsselfakten – also konkretem Wissen, auch mit Hilfe von Tabellen oder Multiple Choice – bis hin zu einem angemessenen Verständnis von Zusammenhängen und Grundsätzen, die in der Vorlesung behandelt wurden.

Von der insgesamt 100 Punkte entfallen 50% auf Wiedergabe konkreten Wissens (Typ A), 25% auf die Wiedergabe von Konzepten sowie Zusammenhängen (Typ B) und 25% auf das Verständnis und die Einordnung der behandelten Konzepte (Typ C). Bei den Fragen wird die zu erzielende Punktezahl und die Klasse der Frage jeweils angegeben, der Unterschied zwischen Typ B und C kann fließend sein.

Rechtschreibfehler und Grammatik gehen nicht in die Notengebung ein, wenn allerdings die Antwort unleserlich ist, kann dies sehr wohl das Ergebnis negativ beeinflussen. Es werden keine Minuspunkte geben, d.h. entweder die Antwort ist korrekt, dann gibt es Punkte, oder sie ist falsch, dann gibt es entsprechend auch keine Punkte. Als falsch werden Teile von Antworten auch dann gewertet, wenn sich die Aussagen widersprechen – also quasi sowohl mit „Ja“ als auch mit „Nein“ geantwortet wird.

Jeder Täuschungsversuch – ob mit IT oder ohne – führt zum Einzug der Klausur und die Bewertung als „nicht bestanden“!

2 Prüfungsinhalte

Die Inhalte werden im weiteren pro Foliensatz (PNSW-yy-xxx_v1.pdf, die Überschriften entsprechen der Benennung der Dateien) stichwortartig ohne weitere Angabe der genauen Seitenzahlen aufgeschlüsselt. Die Reihenfolge der Darstellung kann dabei in wenigen Fällen von der konkreten Vorstellungsreihenfolge abweichen.

Die Fragen der Klausur beziehen sich immer auf konkrete Inhalte, die in den Foliensätzen auch behandelt wurden. Für die Mehrzahl der Inhalte sollte die Detaillierung innerhalb des Foliensatzes ausreichen, die Fragen angemessen beantworten zu können. Allerdings sei darauf hingewiesen, dass für das Lernen weitere Literatur verwendet werden sollten, da die Kürze eines Foliensatzes nie ausreicht, die für ein Verständnis notwendigen Kontext- und Hintergrundinformationen zu geben. Dies betrifft insbesondere diejenigen Studentinnen und Studenten, die die Vorlesungen nicht persönlich verfolgt haben.

2.1 Firewall

- **Begriffe und ihre Bedeutung, Zusammenhänge**
  - Kompartmentalisierung → Separation of Concerns
  - Minimalisierung von Vertrauensbeziehungen und möglicher Kommunikation → Least Privileges
  - Nicht nur eine Maßnahmen → Defense in Depth
- **Architekturkomponenten und Definitionen**
  - Firewall
  - Intrusion Detection System : Host und Network
  - Honeypot
  - Network Monitoring
  - Log-Server
- **Funktionsweise und -prinzipien**
  - Packet Screens
  - Stateful Inspection
  - Proxy Server (incl. Virus Filter, URL Checker)
  - DMZ und deren Aufbau, Grundprinzipien für deren Konfiguration
    - Auftrennung von Kommunikationsströmen
    - Z.B. am Beispiel SMTP
  - Kontrolle von Firewalls durch Network Monitoring, Honeypots, etc.
    - Konflikt mit den Zielen der Firewall
  - Verbleibende Probleme

2.2 DDoS

- **Schutzziele**
  - Confidentiality, Integrity, Availability
- **Angriffe auf die Verfügbarkeit**
  - Ziele für unterschiedliche Angriffsformen und -ansätze
- **Möglichkeiten, einen DoS-Angriff durchzuführen**
  - Programmschwachstellen

- Protokollschwachstellen
- Prozessschwachstellen
- Resourcenauslastung
- slashdot-Effekt

- Angriffstypen
  - Flood
    - SYN-Flood
    - UDP-Flood
  - Reflection mit oder ohne Amplification
    - z.B. DNS, NTP oder SNMP
  - Angriffe auf Server und Infrastrukturkomponenten
  - SPAM als Sonderform von DoS-Angriffen
  - Einzelne Pakete
    - z.B. Ping of Death oder Smurf
- **Botnetze**
  - Einsatzmöglichkeiten von Bot-Netzen
- **(D)DoS-Mitigation und Architekturmöglichkeiten**
  - Eigene Möglichkeiten
    - mit Bordmitteln (z.B. Firewall etc.)
    - mit DoS-Mitigationslösung
  - Durch Dienstleister
    - beim ISP
    - beim Dienstleister in der Cloud
- **Überlast trotz Mitigation**

2.3 VPN

- **Schutzziele Vertraulichkeit / Integrität**
- **Architekturen**
  - LAN-to-LAN
  - Host-to-LAN

- **Konzept eines sicheren Tunnels**
- **Secure Shell**
  - Sicherheitszusicherungen
  - Einordnung im TCP/IP-Stack
  - Prinzip des TCP-Port-Forwardings
  - Positionierung von SSH-Servern
- **Möglichkeiten für die Einordnung im TCP/IP-Stack**
  - Schicht 1
  - Schicht 2
  - Schicht 3 // Erläuterungen zu Folie 60 beachten (siehe hinten)
  - Schicht 4
  - Schicht 7
  - Vergleich der Möglichkeiten

3 Hinweise zu Folie 60 / Kombination von AH und ESP

Zunächst einmal muss man AH und ESP einzeln betrachten, dann zusammen:

1. weder AH noch ESP: genauso wie IP ohne jede Sicherheit, alle Pakete lesbar und manipulierbar
2. AH alleine lässt die Daten unverschlüsselt (also für Angreifer lesbar), aber es können keine Pakete eingeschleust oder manipuliert werden
3. ESP verschlüsselt die Daten und dadurch kann ein Angreifer, der die Daten nicht lesen kann (kein Schlüssel für ihn verfügbar) diese auch nicht verändern (also entschlüsseln, dann verändern und daraufhin wieder „richtig“ verschlüsseln)
4. AH+ESP kombiniert die direkte Authentizierung von AH mit der Vertraulichkeit

Diese vier Möglichkeiten gibt es in großen Installationen mit zwei Standorten sowohl zwischen Client-Server als auch zwischen den Firewalls (oder den an den Standorten eingesetzten VPN-Gateways), d.h. es gibt 4x4 = 16 Kombinationen.

Client-Server	**Firewall-Firewall**	**Einordnung**
NULL	NULL	Die Firewall-Firewall-Lösung bestimmt das gesamte Sicherheitsniveau.
	AH	

Client-Server	**Firewall-Firewall**	**Einordnung**
	ESP	Innerhalb der beiden lokalen Netze wird das Sicherheitsniveau durch das VPN nicht verändert, d.h. lokal bleiben die Daten angreifbar.
	AH+ESP	
AH	NULL	Die Client-Server-Lösung bestimmt das gesamte Sicherheitsniveau.
	AH	Es können keine Pakete gefälscht werden, aber sowohl in den lokalen Netzen als auch im Internet bleiben die Daten lesbar. Da zwischen den Firewalls nur authentisierte Pakete ausgetauscht werden können, können durch das VPN auch keine gefälschten Pakete in die lokalen Netze gelangen.
	ESP	Es können keine Pakete gefälscht werden, aber in den lokalen Netzen bleiben die Daten lesbar. Zwischen den Firewalls sind die Daten verschlüsselt, d.h. ein Angreifer kann diese nicht lesen und erkennt so auch nicht, welche internen Systeme miteinander kommunizieren. Wegen der impliziten Authentisierung können durch das VPN auch keine gefälschten Pakete in die lokalen Netze gelangen.
	AH+ESP	Es können keine Pakete gefälscht werden, aber in den lokalen Netzen bleiben die Daten lesbar. Zwischen den Firewalls sind die Daten sowohl explizit verschlüsselt als auch explizit authentisiert, gefälschte Pakete haben keine Chance.
ESP	NULL	Die Client-Server-Lösung bestimmt das gesamte Sicherheitsniveau.
	AH	Die Client-Server-Verschlüsselung verhindert, dass die Daten mitgelesen werden können, sowohl in lokalen Netzen als auch im Internet. Damit wird indirekt auch die Authentisierung gelöst. Da zwischen den Firewalls nur authentisierte Pakete ausgetauscht werden können, können durch das VPN auch keine gefälschten Pakete in die lokalen Netze gelangen.

Client-Server	Firewall-Firewall	Einordnung
	ESP	Sowohl zwischen Client-Server als auch zwischen den Firewalls sind die Daten verschlüsselt, d.h. ein Angreifer im Internet oder in den lokalen Netzen kann diese nicht lesen und erkennt so auch nicht, welche internen Systeme miteinander kommunizieren. Wegen der impliziten Authentisierung können weder durch das VPN gefälschten Pakete in die lokalen Netze gelangen noch können dem Client oder dem Server gefälschte Pakete untergeschoben werden.
	AH+ESP	Die Client-Server-Verschlüsselung verhindert, dass die Daten in lokalen Netzen mitgelesen werden können. Damit wird indirekt auch die Authentisierung gelöst. Zwischen den Firewalls sind die Daten sowohl explizit verschlüsselt als auch explizit authentisiert, gefälschte Pakete haben keine Chance.
AH+ESP	NULL	Die Client-Server-Lösung bestimmt das gesamte Sicherheitsniveau.
	AH	Durch die Kombination bei der Client-Server-Lösung wird verhindert, dass die Daten mitgelesen oder manipuliert werden können, sowohl in lokalen Netzen als auch im Internet. Die Authentisierung wird direkt gelöst. Da zwischen den Firewalls nur authentisierte Pakete ausgetauscht werden können, können durch das VPN auch keine gefälschten Pakete in die lokalen Netze gelangen.
	ESP	Durch die Kombination bei der Client-Server-Lösung wird verhindert, dass die Daten mitgelesen oder manipuliert werden können. Zwischen den Firewalls sind die Daten verschlüsselt, d.h. ein Angreifer kann diese nicht lesen und erkennt so auch nicht, welche internen Systeme miteinander kommunizieren. Wegen der impliziten Authentisierung können durch das VPN auch keine gefälschten Pakete in die lokalen Netze gelangen.

Client-Server	Firewall-Firewall	Einordnung
	AH+ESP	Durch die Kombination bei der Client-Server-Lösung wird verhindert, dass die Daten mitgelesen oder manipuliert werden können. Zwischen den Firewalls sind die Daten sowohl explizit verschlüsselt als auch explizit authentisiert, gefälschte Pakete haben keine Chance.