Prof. Dr. Andreas Hanemann, 05.05.2016

Aufgabensammlung zur Klausurvorbereitung für das Modul „Sicherheitstechniken in Kommunikationsnetzen“ bzw. für den MOOC „Netzwerksicherheit“

Kapitel 2: Angriffe aus dem Internet

1) Erklären Sie die Begriffe Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit und Nicht-Abstreitbarkeit. Geben Sie typische Maßnahmen an, mit denen diese Aspekte abgesichert werden können.
2) Gibt es einen Unterschied zwischen den Begriffen Authentifizierung und Autorisierung?
3) Welche Arten von Angreifern kann man unterscheiden?
4) Geben Sie Beispiele für Angriffe auf verschiedenen OSI-Schichten an.
5) Was versteht man unter dem Begriff „Spoofing“? Welche Arten kann man unterscheiden? Wie ist der Ablauf beim „ARP Spoofing“?
6) Wie funktioniert ein „Replay“-Angriff?
7) Was versteht man unter dem Promiscous Mode?
8) Sie verwenden Online-Banking, wobei Ihre Bank Transaktionsnummern per Mobilfunk versendet. Sie können die TAN entweder über ein älteres Mobiltelefon (kein Smartphone) per GSM empfangen oder über ein Smartphone mittels UMTS oder LTE. Welche Variante würden Sie als sicherer einschätzen?
9) Welche Angriffsmöglichkeiten bestehen im Zusammenhang mit ICMP-Nachrichten (Echo, Redirect, Destination Unreachable, Source Quench, Fragment Reassembly Time Exceeded)?
10) Welche Risiken bestehen im Zusammenhang mit BGP? Beachten Sie dabei die Longest-Prefix-Matching-Regel.
11) Welche Angriffsmöglichkeiten gibt es im Zusammenhang mit DHCP?
12) Was versteht man unter einem Port Scan? Ist der Port Scan schon der eigentliche Angriff?
13) Wie kann ein Port Scan durchgeführt werden, so dass die Adresse des Angreifers nicht sichtbar wird?
14) Wie funktioniert eine Betriebssystemerkennung, ohne dass man ein zugelassener Benutzer auf einer Maschine ist?
15) Erklären Sie den typischen Ablauf eines DDoS-Angriffs.
16) Wie kann der TCP-Verbindungsaufbau zu einem Denial-of-Service-Angriff genutzt werden?
17) Wie kann das DNS oder NTP zu einem DDoS-Angriff missbraucht werden?
18) Warum besteht bei der HTTP-Methode „Persistent HTTP“ eine Anfälligkeit gegenüber DoS-Angriffen?
19) Was versteht man unter den Begriffen „Bot“ und „Botnetz“? Wie können Botnetze heutzutage organisiert sein?
20) Wie erfolgt die Passwortübertragung bei älteren Protokollen wie Telnet, FTP oder SNMPv1/SNMPv2?
21) Was versteht man unter einen „Wörterbuch“-Angriff?
22) Wie unterscheiden sich die Schadsoftware-Varianten Virus, Wurm, Trojanisches Pferd und Ransomware?
23) Was versteht man unter einem „Zero-Day-Exploit“ und unter einem „Drive-by-Exploit“?

24) Erklären Sie, was man unter einem „Buffer Overflow“ versteht und welche Auswirkungen ein solcher haben kann.
25) Erklären Sie, wie eine SQL-Injection funktioniert.
26) Wie funktioniert die Cross-Site Scripting-Variante „Persistent XSS“?
27) Welches sind die möglichen Folgen, wenn bei einem Nutzer die Einstellung des zu verwendenden DNS Servers manipuliert ist?
28) Beinhaltet das E-Mail-System bereits eine Verschlüsselung?
29) Welche Risiken bezogen auf die IT-Sicherheit bestehen bei der Vernetzung von Fahrzeugen?
30) Welche Bedeutung haben Keylogger Hardware, manipulierte USB-Sticks und Caller ID Spoofing beim Social Engineering?

Kapitel 3: Abwehr von Angriffen

1) Welche drei Varianten von VLANs kann man unterscheiden?
2) Warum ergibt sich nur ein geringer Sicherheitsgewinn, wenn man bei WLAN die zugelassenen MAC-Adressen einschränkt oder die SSID unterdrückt?
3) Welche Konfigurationsmöglichkeiten von Network Access Control kann man unterscheiden?
4) Wie unterscheiden sich statische Paketfilter, dynamische Paketfilter und Proxies?
5) Erklären Sie, wie die Regeln in einer Paketfilter-Firewall aufgebaut sind.
6) Aus einem internen Netz (10.0.1.0/24) soll es möglich sein, beliebige Webserver im Internet mit HTTP auf TCP-Port 80 anzusprechen. Diesen soll es auch erlaubt werden zu antworten. Geben Sie Regeln für eine Paketfilter-Firewall in geeigneter Weise an. Wie lautet eine sinnvolle Default-Firewall-Regel?
7) Wie wird entschieden, welche Firewall-Regel verwendet wird, wenn mehrere zu der aktuell zu untersuchenden Dateneinheit passen?
8) Ein Unternehmen bietet Dienste im Internet an, die auf mehreren Servern laufen, und hat außerdem eine Reihe von weiteren Rechnern, die keine öffentlichen Dienste anbieten. Machen Sie eine Zeichnung, die die typische Konfiguration einer DMZ in diesem Szenario zeigt.
9) Wenn man ein inneres Netz und eine DMZ hat und diese mit dem Internet verbunden sind, welche generellen Firewall-Regeln für den Zugriff zwischen den Bereichen sind dann sinnvoll?
10) Sollten Server in einem Firmennetz so eingestellt werden, dass diese auf ICMP Echo Requests antworten? Was wären Vor- und Nachteile?
11) Inwiefern gibt es einen Zusammenhang zwischen einer Firewall und ARP Spoofing?
12) Wie sollten eine Firewall und ein „Bastion Host“ konfiguriert sein?
13) Welche Schutzmöglichkeiten gegen „SYN Flooding“-Angriffe gibt es?
14) Erklären Sie den Unterschied zwischen den Begriffen „Identity Provider“ und „Service Provider“ im Zusammenhang mit dem Identity Management.
15) Wie unterscheiden sich NIDS und HIDS?
16) Wieso benötigt man zusätzlich zum Einsatz von Firewalls noch Intrusion Detection Systeme?
17) Was versteht man im Zusammenhang mit IDS unter Signaturen?
18) Fertigen Sie eine Zeichnung eines Netzes mit DMZ an und zeigen Sie, wo NIDS und HIDS installiert werden können.
19) Was versteht man unter einem Honeypot? Welchen Zweck erfüllen solche Systeme heutzutage?
20) Welche Arten von Virenscannern kann man unterscheiden?
21) Diskutieren Sie den Aufwand für und die Sicherheitsverbesserungen durch DNSSEC.

Prof. Dr. Andreas Hanemann, 05.05.2016

Kapitel 4: Sicherheitsprotokolle

1) Welche VPN-Typen kann man unterscheiden?
2) Ordnen Sie die Protokolle IPsec, SSL/TLS und SSH in das OSI-Schichtenmodell ein.
3) Was unterscheidet asymmetrische von symmetrischen Verschlüsselungsverfahren? Was für Schlüssel gibt es?
4) Wie erfolgte die Standardisierung von AES? Hat sich dieses Verfahren bewährt?
5) Wie werden asymmetrische und symmetrische Verschlüsselung in der Praxis (z.B. bei IPsec und SSL/TLS) kombiniert?
6) Was versteht man unter einer kryptographischen Hash-Funktion? Welche Eigenschaften soll eine solche Funktion haben?
7) Erklären Sie, wie ein Message Authentication Code berechnet wird. Was wird durch die Verwendung bei der Kommunikation erreicht?
8) Wie ist der Zusammenhang zwischen digitalen Unterschriften und Public Key-Kryptographie?
9) Welche Inhalte hat ein digitales Zertifikat?
10) Was sind die Aufgaben einer Zertifizierungsstelle?
11) Wie kann man unterprüfen, ob ein digitales Zertifikat für ungültig erklärt wurde?
12) Erklären Sie den Ablauf eines Challenge-Response-Verfahrens. Warum wird dabei der Challenge zufällig gewählt?
13) Wozu dient der Standard WPA2?
14) Was kann man durch die Verwendung des Protokolls 802.1X erreichen?
15) Erklären Sie die Eigenschaften von AH und ESP bei IPsec sowie den Unterschied zwischen Transport- und Tunnel-Modus. Was versteht man in diesem Zusammenhang unter dem „tunneln“ von IP Paketen?
16) Welche Informationen sind in einer Security Association bei IPsec enthalten?
17) Wie wird ein Replay-Angriff bei IPsec verhindert?
18) Ein Unternehmen hat zwei Standorte, die über das Internet verbunden sind. Das Unternehmen möchte sicherstellen, dass die Daten beim Transport über das Internet nicht erfolgreich abgehört oder verfälscht werden können. Erklären Sie, wie dieses mit IPsec erreicht werden kann.
19) Welche Bedeutung hat es, wenn vor einer URL in der Browserzeile https statt http steht?
20) Welche Aufgaben übernimmt das Handshake-Protokoll von SSL/TLS?
21) Was ist der Unterschied zwischen einer Verbindung und einer Session bei SSL/TLS? Wie ist deren Beziehung?
22) Aus welchen Teilen besteht eine Cipher Suite bei SSL/TLS?
23) Vergleichen Sie IPsec mit SSL/TLS und zeigen Sie Gemeinsamkeiten und Unterschiede auf. Diskutieren Sie auch Vor- und Nachteile.
24) Ein Unternehmen beschäftigt Außendienstmitarbeiter, die oft Besprechungen bei Kunden haben. Während dieser Besprechungen müssen sie manchmal auf Server in der Firma zugreifen, wobei diese Daten über einen Browser abfragbar sind. Würden Sie in diesem Fall empfehlen, dass die Außendienstmitarbeiter per IPsec oder per SSL/TLS angebunden werden?
25) Welche Aufgaben hat das SSH-Protokoll?
26) Wie funktioniert das Port Forwarding mit SSH?
27) Warum erreicht man durch die Kombination der E-Mail-Protokolle SMTP, POP3/IMAP mit SSL/TLS nur einen partiellen Schutz bei der E-Mail-Übertragung?
28) Erklären Sie Gemeinsamkeiten und Unterschiede von PGP und S/MIME.

Prof. Dr. Andreas Hanemann, 05.05.2016

Kapitel 5: IT-Grundschutz und ISO/IEC 27000

1) Was versteht man unter einem Information Security Management System (ISMS)?
2) Wozu dienen die IT-Grundschutzkataloge des BSI?
3) Wie sind die Inhalte der IT-Grundschutzkataloge aufgebaut?
4) Wozu dient die Standardfamilie ISO/IEC 27000?
5) Wie ist der Zusammenhang von IT-Grundschutz mit ISO/IEC 27000?
6) Welche Zertifizierungsmöglichkeiten bestehen im Zusammenhang mit ISO/IEC 27000?