Internet Security

Prüfung am 23.1.2003

Kennzahl _____ Matrikelnummer _____ Name _____

- Bitte füllen Sie die Angaben mit dokumentenechtem Schreibmaterial aus.
- Es sind keine Unterlagen erlaubt.
- Die Arbeitszeit beträgt 90 Minuten.

1. Geben Sie die grundlegenden Methoden an, um eine Attacke durchzuführen. Nennen sie für jede Methode ein Beispiel.
[5 Punkte]

   1.

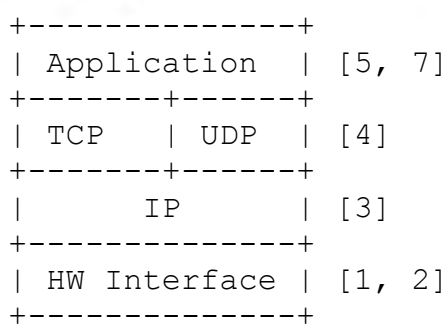
   2. Das kann alles sein, jedenfalls bekomme ich von meinen ESSO INSO Folien da keine sinnvolle Antwort zusammen.

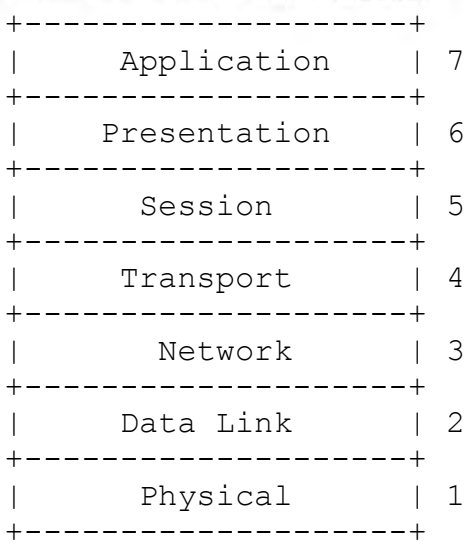
   3.

   4.

   5.

2. Stellen sie den TCP/IP Protokollstack dem OSI-Reference Modells graphisch gegenüber. Geben sie für die TCP/IP Layers auch die entsprechenden Protokolle an. Nennen Sie auch jene Schichten des OSI Reference Modells, die bei TCP/IP nicht implementiert sind.
[10 Punkte]





TCP/IP definiert weder das HW-Interface, das z.B. für ein Token-Ring Netz anders aussieht als für Ethernet, noch die Schichten ab 5. (HTTP, SSL, FTP, Telnet usw. usf)

3. Nennen sie die drei Aufgaben des Transport Layers im OSI Reference Modell.
[3 Punkte]

1. Den Aufbau eines Tunnels zwischen dem Ziel und dem Client.

2. Sicherung der Daten während der Übertragung, so z.B. Neuübertragung bei Verlust eines Segments.

3. Zusammensetzen der Segmente in der richtigen Reihenfolge.

4. Wofür ist *IP Fragmentierung* notwendig? Wo wird es durchgeführt? Wo findet *Reassembling* statt? Welche Datenfelder des IP Protokolls werden dafür benötigt, und was ist die Aufgabe jedes Feldes?
[7 Punkte]

Falls die MTU kleiner als das IP-Packet ist, muss es notwendigerweise fragmentiert werden da es ansonsten nicht gesendet werden kann. Dadurch wird die HW des Netzes transparent.

Durchgeführt wird es entweder schon beim Sender oder von einem Router am Weg. Reassembled wird entweder an einem Router oder beim Empfänger.
Datenfelder:

- Length
- Don't fragment Flag (könne ja vom Client aus verboten sein)
- Fragment Offset

5. Nennen Sie zwei Attacken, welche IP Datagram Fragmentierung benutzen und erklären Sie sie kurz.
[2 Punkte]

- IP Fragment Overlap-Attack: Das Setzen des Fragments dass Daten überschrieben werden wodurch beim Zusammensetzen der Packete neue Daten entstehen => Malicious-Daten einfügen.
- IP Fragment Overrun: Zusammengesetze Daten sind länger als laut Spezifikation möglich (65.532) ==> System-Crash

6. Vergleichen sie die beiden Routingprotokolle RIP und OSPF.
[5 Punkte]

RIP	OSPF
Router Information Protocol ist ein simples Protokoll dass das zyklische Senden von Daten über wen welcher Hop erreichbar ist verlangt. Wobei dabei die Hop-Anzahl für die Pfad-Findung eine Rolle spielt.	Ähnlich wie RIP verlangt das Open Shortest Path Protocol, dass zyklisch Informationen gesendet werden über wen welcher Hop zu welchen **Kosten** erreichbar ist, wobei die Kosten nicht über die Hop-Anzahl alleine sondern auch andere Faktoren wie den Traffic definiert werden ==> Load Balancing möglich. Zudem kennt ein Knoten nicht nur seine Nachbarn sondern das gesammte Netzwerk.

7. Was ist OS Fingerprinting und warum kann es für einen Angreifer nützlich sein? Nennen sie typische Scans und deren Erkennungsmerkmale.
[5 Punkte]

OS Fingerprinting ist ein Überbegriff für Verfahren die das Ermitteln des Betriebssystems eines bestimmten Host zum Ziel haben.
Alle Verfahren haben gemeinsam, dass Kenngrößen bei Heade-Antworten bzw. die Antwort selbst geprüft werden, wie z.B. folgende Punkte:
- Wie groß ist die TTL? (IP Header)
- Wie groß ist die Window Größe
- Was passiert beim No Fragment Flag?
- Christmas-Tree Pakete senden (Einfach alle Flags setzen.)

8. Wie funktioniert TCP Hijacking? Beschreiben sie die Voraussetzungen und den Vorgang. Warum kommt es dabei zu ACK-Storms und wie können diese verhindert werden?
[8 Punkte]

Basis ist das Erraten der Initial-SYN Nummer.
Der Angreifer sendet das Paket mit gespoofder IP an den Server, dieser antwortet mit SYN+ACK an den Client.
Fangen wir nun dieses Paket nicht ab, mukiert sich der Client über die falsche SYN-Nummer und schickt seinerseits ein Paket zurück, der Server möge ihm ermöglichen die Verbindung neu aufzubauen. Was wiederum ACKnowledged werden muss ==> ACK storm.
Um das zu verhindern, könnte das Opfer offline genommen (DOS-Attacken) oder umgeleitet (ARP-Spoofing) werden.

9. Was ist DNS, wie ist der *namespace* organisiert und welche Protokolle werden dafür eingesetzt? Welche DNS-Servertypen gibt es?
[7 Punkte]

Domain Name Service ist eine Service um Namen auf IP-Addr. abzubilden.
Der namespace is wie ein Baum aufgebaut, wobei es bei der Top Level Domain beginnt und sich immer weiter herunterhangelt. DNS baut auf UDP auf, wobei der Standard auch TCP erlaubt.
Es gibt Root-Server die wiederum auf andere Name-Server verweisen um das System aufzubauen.

10. Warum ist NIS nicht sicher (worauf basiert es)? Nennen sie mindestens drei Gründe dafür.
[3 Punkte]

1 Es basiert auf UDP wodurch es zustandlose "Verbindungen" besitzt.

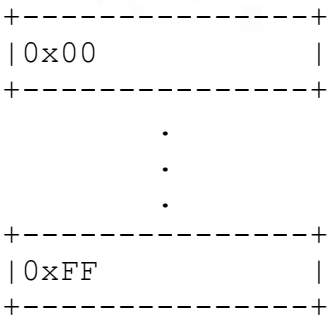
2 Es kennt keine Verschlüsselung wodurch Sniffen sehr leicht ist.

3 Abgesehen von der fehlenden Verschlüsselung werden Username u. Passwort nicht einmal gehashed => Daten noch leichter abhörbar

11. Erklären den Vorgang der Unix-Passwort Authentifizierung im Detail – welche Rolle hat insbesondere das 12-bit *salt*?
[7 Punkte]

Das ursprüngliche Verfahren sieht folgendes vor:
- User wählt Passwort.
- Passwort wird mit Salt-Wert vermischt.
- Das Ergebnis wird nun gehashed. Alte Implementation nehmen dazu einen auf DES basierenden Algorithmus der in einer Schleife 25 mal jeweils das Ergebnis hashed.
- Das Salz hat den Nutzen um den Wert weiter weg zu bringen vom ursprünglichen Passwort was wiederum die Kollisionswahrscheinlichkeit verringert und auch das Erraten schwerer macht.

12. Was sind Stack/Buffer Overflows? Erklären sie die Vor- und Nachteile dieser Attacke. Skizzieren Sie den Aufbau des Stacks und erklären Sie was beim Buffer Overflow genau passiert.
[12 Punkte]



Der Stapelspeicher wächst nach unten wodurch es sehr wahrscheinlich ist, dass unter dem aktuellen Programmcode weiterer Code oder Daten liegen.
Ziel ist es nun eigenen Code einzuschleusen indem über die Grenzen des eigenen (Unter-)Programms hinausgeschrieben wird und so späterer Code der ausgeführt werden soll, überschrieben wird.
Vorteile:
- Bei unsicheren Programmcode einfach durch geschickte Parameter möglich.
- Bei Erfolg Übernahme des aktuellen Programms möglich.

Nachteile:
- Erkennung von OS relativ leicht.
- Viele Tools, auch schon zur Compile-Zeit, erhältlich um dagegen anzugehen.
- Möglich einfach nur Programm abzuschießen obwohl Übernahme beabsichtigt war.

13. Welche Stack Overflow Schutzmechanismen gibt es? Nennen sie vier Möglichkeiten.
[4 Punkte]

1 Ausweichen auf Hochsprachen wie C# oder Java. (Z.B. sind dort Strings immutable Referenztypen wodurch Adresskopiererein für Strings unmöglich sind.

2 Stack Protection Mechanisms, z.B. Zufallsvalue vor Rücksprungadr. einfügen. Ist sie vor Zurückspringen anders => Attacke!

3 Run Time Defense, Kernel-Module die das Speichermanagement verändern wodurch sich der Adressbereich ändert. => Schwer zu erraten

4 Address Space Randomization, das Programm lädt die Daten nicht sequentiel auf den Stack sondern zufällig. D.h. wieder wird das gezielte Einfügen von Schadcode schwerer.