Klassenarbeit

1. TCP:
   Ein initiierender Host sendet die Sequenznummer 335 und hat das SYN-Flag gesetzt.
   a) Er empfängt eine Nachricht mit der Sequenznummer 785 und einer Acknowledgment-Nummer 336 sowie gesetztem ACK-Flag. Wie ist auf der initiierenden Seite die Antwort zu interpretieren? (Begründung!)

   b) Er empfängt eine Nachricht mit der Sequenznummer 785 und einer Acknowledgment-Nummer 200 sowie nicht gesetztem ACK-Flag.
   Wie ist auf der initiierenden Seite die Antwort zu interpretieren? (Begründung!)

   c) Welche Art von Angriffen lassen sich darauf aufbauen? Beschreiben Sie das Prinzip!

2. Welcher Nachteil besteht bei PAP gegenüber CHAP!
   Erklären Sie zunächst die Begriffe PAP und CHAP!

3. a) Wo wird das PPP-Protokoll im wesentlichen eingesetzt?
   b) Welche Unterprotokolle kennt PPP?
   c) Zu welchem Unterprotokoll des PPP gehört PAP?

4. In der Linux-Datei **inetd.conf** können Dienste aktiviert/ deaktiviert werden. Sie finden folgenden Dienst:

   # ftp stream tcp nowait root /usr/sbin/tcpd in.telnetd

   a) Ist der Dienst aktiv (wenn nein, wie kann er aktiviert werden, wenn ja, wie deaktiviert man ihn?
   b) Beurteilen Sie die Sicherheit des Rechners, falls der Dienst aktiv ist.

5. Stellen Sie symmetrische und asymmetrische Verschlüsselung gegenüber!

6. Unterscheiden Sie die Schadenswirkung von Trojaner und Viren!

7. Klassifizieren Sie Anforderungen an Paßwörter?

8. Ihnen stehen 4 Festplatten zur Verfügung.
   RAID 0: Alle werden benutzt. Eine Festplatte fällt aus! Beurteilen Sie die Datensicherheit! Worin liegt der Vorteil von RAID 0?

9. Einem Angreifer gelingt es, die Zuordnung zwischen einem Rechner-Namen und der zugehörigen IP-Adresse zu fälschen, d.h. daß ein Name in eine falsche IP-Adresse und umgekehrt umgewandelt wird.
   a) Welcher Dienst ist normalerweise für diese Zuordnung zuständig?
   b) Wie heißt die Angriffsart, die auf dieser Fälschung beruht?

10. a) Welches Gremium innerhalb eines Betriebes ist für die Organisation der IT-Sicherheit letztendlich verantwortlich?
    b) Beschreiben Sie das Spannungsfeld in dem alle organisatorischen IT-Sicherheitsmaßnahmen abzuwägen sind!

Philipp Iatrou ITFO 93% 15 1 [illegible]

(2) * Bei PAP wird das Passwort unverschlüsselt über das Netz geschickt, während es bei Chap nicht übertragen wird.
* Pap ist ein Password Authentifications Protokoll, das genutzt wird um sich an einer Gegenstation zu identifizieren.
Chap ist ein Challenge Handshake Authentification Protocol.

10

(3) a) eine Punkt zu Punkt Verbindung wird genutzt, wenn ~~[illegible]~~ Rechner ~~[illegible]~~ eines Netzes keine direkte Verbindung zum Internet haben. Eine Einwahl (PPP Verbindung) zu einem entsprechenden Gateway geschieht dann meistens per Modem.
Weitere Gründe für PPP-Verbindungen:
- ~~Rechner~~ Verbindung ~~wird nicht~~ existiert nicht permanent sondern wird bei Bedarf aufgebaut
-

b) Unterprotokolle von PPP:
- LCP (Link Control Protocol)
- NCP (Network Control Protocol)

10

c) LCP

(4) a) Der Dienst ist nicht aktiv, durch löschen des #-Zeichens wird er aktiv gesetzt. Eine weitere Möglichkeit führt über das Yast-Tool.

b) In der Grundkonfiguration ist unter Linux zunächst kein Zugriff erlaubt. Allerdings bietet jeder zusätzlich ~~[illegible]~~ geöffnete Port eine Angriffsmöglichkeit.
8
Momentan hat lediglich der Root Zugriff auf die Remoteservices, ~~d~~ entsprechende User müssen noch [illegible] werden.

10

(5)

Symmetrische Verfahren	Asymmetrische Verfahren
- Gleicher Schlüssel bei Ver- und Entschlüsselung (Private Key Verfahren) - hohe Geschwindigkeit - aufwendiges/störanfälliges Schlüsselmanagement	- Zweiteiliger Schlüssel, ein öffentlicher und ein privater der nicht voneinander ableitbar sind. - Nur der öffentliche Schlüssel ist bekannt - Der Private Schlüssel wird nur von Eigentümer benutzt (Decoffierung)

10

(6) Trojaner sind funktionsfähige Programme, die eine bestimmte Aufgabe kontrolliert ausführen. Wodurch die Programmierung wird erst durch spezifische Aktivierung ausgelöst.
~~Der Nutzer merkt davon nichts, da~~ ein Beispiel für die Wirkung von Trojanern ist das übermitteln von sicherheitsrelevanten Daten oder Fernsteuerfunktionen des Clients.

Viren sind Programmteile, die auf unkontrollierten Weg (in Programmen, angehängten Dateien etc.) auf den Rechner gelangen und meist eine Rechnerschädigung zum Ziel haben. Viren pflanzen sich fort. Es gibt Boot-, Datei-, Makro-, Link- und Quellcode/Makro Viren

10

(7) Passwörter müssen sicher, also ~~nicht~~ nur mit möglichst hohem Aufwand zu knacken sein. Sie müssen eine ~~bei~~ bestimmte Mindestlänge haben (Groß-, Kleinbuchstaben und Zahlen bestehen. ~~Sie~~ Es Leicht zu erratene Passwörter dürfen nicht verwendet werden (Bsp. Geburtstag, Name der Freundin etc.)

8

Philipp Tatrau   ITC.   15.12.00

(8) Die Datensicherheit von RAID 0 liegt, wie der Name schon sagt bei 0. Fällt eine Platte aus hilft nur noch das Einspielen eines hoffentlich vorhandenen Backups. Die Daten werden ohne Parity auf die 4 Festplatten verteilt (Blockweise) und bieten somit in Sachen Ausfallsicherheit keine Lösung. (Datastriping)
Der Vorteil ~~ist~~ von RAID 0 liegt ~~nicht~~ im ~~[illegible]~~ Zugriff auf die Platten, d.h. ~~das Anwendungen die~~ ~~viel Lesen~~ [illegible] Anwendungen mit hohen Geschwindigkeitsanforderungen.
(hoher Durchsatz bei großen Datenzugriffen)   10

(9) a) Für die Zuordnung ist normalerweise der DHCP-Dienst zuständig ?   8
b) Diese Angriffsart nennt man IP-Spoofing.

(10) a) Verantwortlich für die Sicherheit ist das ~~IT-Sicherheit~~ IT-Sicherheitsmanagement. Dieses besteht aus Mitgliedern des Managements, dem IT-Koordinierungsausschuss und dem IT-Sicherheitsmanagement sowie diversen Sicherheitsbeauftragten.

b) Sicherheit hat zwei paar Schuhe, zum einen gibt es keine totale Sicherheit, zum anderen darf durch die Sicherheit nicht die Produktivität des Unternehmens beeinträchtigt werden. Man muss berücksichtigen, das manche Mitarbeiter diese Sicherheitsbarrieren umgehen müssen, z.B. um sich auf Kundenrechner aufzuschalten, Updates von FTP Servern zu ziehen usw. Eine Sicherheitskonzept muss immer genügend Spielraum lassen um die Moral der Mitarbeiter nicht in den Keller wandern zu lassen. Wenn bei den Usern jegliches Surfen im Internet unterbunden wird sinkt die Stimmung ... garantiert.   10

(1) a) Der Host hat eine Anfrage gestellt und über
wird das SYN-Flag übergeben, dass ein Verbindungsaufbauwunsch
besteht, der vom gegenüber quittiert werden muss
Das gegenüber wiederum antwortet mit einem gesetzten Ack-Flag,
das bedeutet das die übermittelte Quittierungsnummer gültig ist. ✓

b) Die Quittungsnummer ist nicht gültig, Verbindung kann
nicht zu stande

Begründung: FRAGEN SIE DOCH DIE ZACHER !!!
Was kann denn der Zacher dafür?
Die Aufgabe ist von mir! 7

c) SYN-Flooding ✓