SVS | Übung 1

Task 1

Zur Übernahme der Kontrolle über ein Netzwerkgerät werden im Allgemeinen folgende Aktivitäten unternommen:

The following activities are usually performed to take control over a network device:

Aktivität / Activity	Ziele / Goals	Schutzmechanismen / Defence mechanisms
1. Netzwerkanalyse / Network analysis	Auffindung möglicher Angriffsziele / Finding potential attack targets,…	Ping-Antworten verbieten / Forbid ping responses,…
2. Zielsystemscanning / Target system scanning		
3. Einbruch / Break-in		
4. Ausnutzung / Exploitation		

Vervollständigen Sie die Tabelle, indem Sie die folgenden Fragen beantworten:

- Was sind die Ziele der einzelnen Aktivitäten?
- Welche Schutzmechanismen kennen Sie gegen diese Aktivitäten?

Complete the above table by answering the following questions:

- What are the goals of single activities?
- What are the defense mechanisms against them?

Task 2

Welche IT-Objekte können zum Ziel eines Angriffs werden? Nennen Sie Beispiele für Angriffe. Füllen Sie die untenstehende Tabelle aus.

Which IT entities can become a target of attack? Name examples for attacks. Fill in the following table.

Klasse / Class	Objekte / Objects	Beispiele / Examples
Netzwerkinfrastruktur / Network infrastructure	Verbindungen / Connections,…	Kabelbruch / Cable breach
Endgeräte / End devices		
Betriebssysteme / Operation systems		
Anwendungen und Dienste / Applications and services		
Benutzer / Users		

Task 3

Machen Sie sich mit dem Werkzeug *nmap*[1] vertraut. Beantworten Sie die folgenden Fragen:

- Finden Sie die Namen aller Rechner heraus, deren IP-Adressen sich im Bereich *134.109.193.0/24* befinden[2]. Welche Rechner sind gerade aktiv?
- Welche Dienste laufen auf dem Rechner *tan.informatik.tu-chemnitz.de*?
- Welches Betriebssystem ist auf dem Rechner *pauline.informatik.tu-chemnitz.de* installiert?

Inform yourself about the *nmap*[1] tool. Answer the following questions:

- Find the names of all PCs[2] in the IP range *134.109.193.0/24.* Which of them are currently online?
- Which services run on the machine *tan.informatik.tu-chemnitz.de*?
- Which operating system is installed on *pauline.informatik.tu-chemnitz.de?*

Task 4

Welche Angriffe / Möglichkeiten zur Wiederherstellung von Passwörtern sind Ihnen bekannt? Finden Sie das Passwort von der Ressource http://pauline.informatik.tu-chemnitz.de/webdav_http_basic/secret.jpg heraus (Benutzername: *hello*), indem Sie folgende Techniken anwenden (mittels eines selbst-geschriebenen Programms):

a) Dictionary-Angriff (mittels des Vokabulars *passlist.txt*)
b) Bruteforce (auf 3 Buchstaben beschränkt)

Which attacks / possibilities to recover passwords do you know? Find out the password from the resource http://pauline.informatik.tu-chemnitz.de/webdav_http_basic/secret.jpg (username: *hello*) by applying the following techniques (a self-written program):

a) Distionary attack (using vocabulary passlist.txt)
b) Bruteforce (limited to 3 letters)

[1] http://nmap.org/ (cheat sheet: https://www.stationx.net/nmap-cheat-sheet/)
[2] Aus dem Uni-Netz bzw. über das VPN / From University network or using VPN