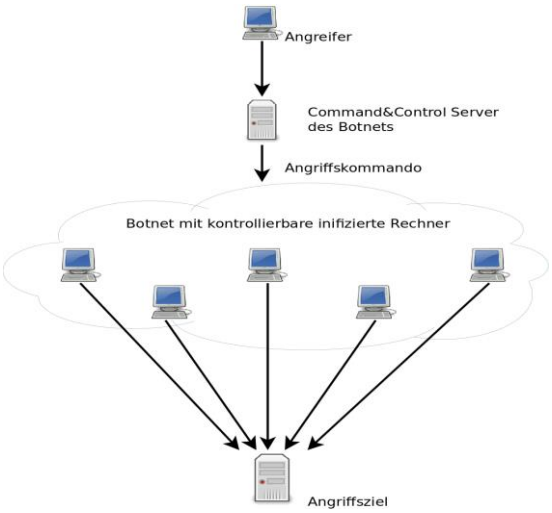
DoS und DDoS Angriffe (1/2)

Denial-**o**f-**S**ervice

- Angriff mit dem Ziel der Störung der Verfügbarkeit eines Dienstes (Service)

Distributed **D**enial-**o**f-**S**ervice

- Denial-of-Service-Angriff, der mithilfe zahlreicher Angreifer ausgeführt wird, z.B. mittels eines Botnets



DoS und DDoS Angriffe (2/2)

Beispiele:

- **Low Orbit Ion Cannon (LOIC)** – Software für Netzwerk-Tests
  - Eigentlich dazu gedacht, zu prüfen ob Netzwerk ausreichend resistent gegen DoS-Angriffe ist
  - Kann aber auch für echte DoS-Angriffe missbraucht werden
- **Operation „Avenge Assange"**
  - DDoS-Angriffe auf MasterCard, Visa und andere Web Seiten
  - Grund für den Angriff war die politische Entscheidung, die Bearbeitung von WikiLeaks-Spenden zu unterbrechen

Malware – Viren, Würmer & Co. (1/2)

Malware

- **Mal**icious Soft**ware** – Bezeichnung für Schadsoftware, also für bösartige Software, wie z.B. Viren, Würmer, Trojaner, …

Beispiele (1/2):

- **Viren**
  Zerstörerische Mini-Programme, die meist mit „verseuchten" Anwendungen kommen
- **Würmer**
  Schadsoftware, die sich automatisch über offene Netzwerkverbindungen verteilen
- …

Malware – Viren, Würmer & Co. (2/2)

Malware

- **Mal**icious Soft**ware** – Bezeichnung für Schadsoftware, also für bösartigen Software wie z.B. Viren, Würmer, Trojaner, …

Beispiele (2/2):

- **Trojaner**
  - Malware, die oft ungewollt durch einen naiven Benutzer auf dem Computersystem installiert wird
  - Funktionalität unterscheidet sich von der Funktionalität, die der Benutzer erwartet, z.B. Hintertür oder Aufzeichnen der Passwörter im Hintergrund
  - Beispiel: „**Bundestrojaner**" entwickelt von der Polizei zum Abhören der VoIP-Software
- Weitere Beispiele werden im weiteren Kursverlauf vorgestellt

Spoofing und Phishing (1/2)

Spoofing

- Angreifer sendet Nachrichten mit einer gefälschten Absenderadresse, z.B. gefälschte IP-Adresse oder Email-Adresse

Spoofing wird oft verwendet im Zusammenhang mit:

Phishing

- Mit Methoden des „Social-Engineering" werden Nutzer aufgefordert, z.B. ihre Passwörter zu verraten
- Angreifer nutzen dazu gefälschte Emails, SMS, Anrufe, …

Spoofing und Phishing (2/2)

Beispiel:

- Email mit gefälschter Absender-Adresse (**Spoofing**) fordert Benutzer auf, eine verfälschte Web-Seite zu öffnen, die eine starke Ähnlichkeit hat zur echten Web-Seite , z.B. mit Facebook oder Online-Bank
- Dann erfolgt Aufforderung, die eigenen Benutzerdaten, z.B. Nutzernamen, Passwort, Kreditkartennummer, usw. (**Phishing**) einzugeben …

Defacement (1/2)

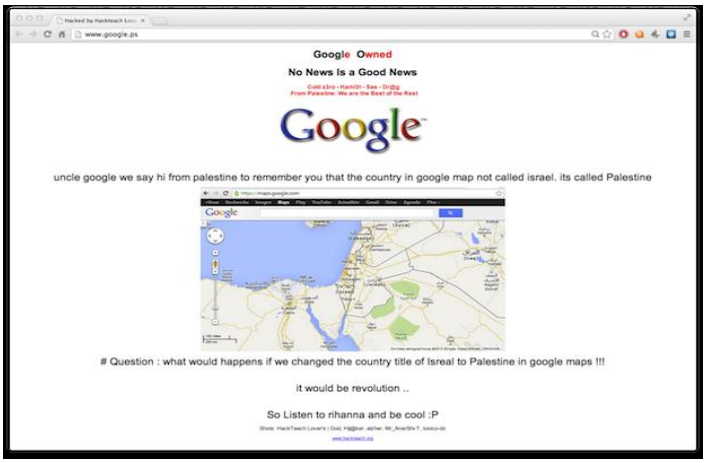
Angriff auf Web Seite oder Web Server, mit dem Ziel, diese inhaltlich zu verändern (De-face = Änderung des Gesichts)

Angewendet für

- **Phishing von Benutzer-Daten**:
  - Benutzer können nicht wissen, dass die Änderungen auf der Seite unberechtigte Verfälschungen sind
  - Angreifer können sensible Identitätsdaten erlangen, wie z.B. Passwörter, Kreditkartennummern, …
- Eigenwerbung von Hacking Gruppen
- Angriff auf die Verfügbarkeit

Defacement (2/2)

Beispiel: Google Website für Palästina



Quelle: ZDnet

Sniffing und Eavesdropping

Sniffing ist Methode, die für Netzwerk-Diagnostik entwickelt wurde und den vollständigen Datenverkehr im Netzwerk „mitzuhören" kann

- Systemadministratoren können damit, Fehler im Netzwerkverkehr erkennen und analysieren, z.B. mit der Sniffing-Software: *Wireshark*

Eavesdropping bezeichnet unberechtigtes „Abhören" von Datenpaketen auf ihrem Weg durch Netzwerk

- Angreifer verbindet sich mit Netzwerk des Opfers, sammelt und analysiert dort IP-Pakete mit dem Ziel, Identitätsdaten oder andere vertrauliche private Daten zu extrahieren
- Angreifer können unverschlüsselten Datenverkehr mitlesen:
  - alle ungesichert über das Web versandte Anfragen
  - Chat-Nachrichten, usw.

Weitere Angriffe auf IT-Systeme

- Unberechtigter physischer Zugang zu Computer System, z.B.
  - Laptop-Diebstahl, Handy-Diebstahl, …
  - Einbruch in Serverraum
- Social Engineering Attacken
  - ... nicht nur, um Passwörter zu stehlen, wie im Phishing-Beispiel
- Angriff zur Entschlüsselung von Identitätsdaten
  - Password Cracking
  - Password Guessing
- …

Weitere Angriffe auf IT-Systeme

- Unberechtigter physischer Zugang zu Computer System, z.B.
  - Laptop-Diebstahl, Handy-Diebstahl, …
  - Einbruch in Serverraum
- Social Engineering Attacken
  - ... nicht nur, um Passwörter zu stehlen, wie im Phishing-Beispiel
- Angriff zur Entschlüsselung von Identitätsdaten
  - Password Cracking
  - Password Guessing
- …

Verbreitete Angriffe | Sicherheit im Internet | Prof. Dr. Christoph Meinel 11