

## IT-Sicherheit in Netzwerken – Praktische Aufgaben 3

In den folgenden praktischen Aufgaben werden Gefahren, Schwachstellen, Schutzziele und speziell unterschiedliche Angriffsformen in Netzwerken untersucht. Dabei steht im Vordergrund die unterschiedlichen technischen Angriffsformen herauszuarbeiten, gegen die ein Netzwerk geschützt werden muss. Ihre Aufgabe ist jetzt schrittweise diese verschiedenen Angriffsformen zu untersuchen. Dabei insgesamt zu beantwortende Fragen sind:

- Welche Angriffsformen kennen Sie bereits?
- Welche weiteren Angriffsformen können Sie sich vorstellen?
- Welche sich wiederholenden Schema dieser Angriffe lassen sich ermitteln?
- Können solche Schemata auf andere Angriffsszenarien übertragen werden?
- In welcher Weise sind die Angriffsformen erweiterbar?

Als eine spezielle Angriffsform in verteilten Netzwerken werden Bot-Netze studiert.

Nach Durchführung des Praktikums können Sie zuordnen,

- welche Gefahren mit unterschiedlichen Angriffsformen verbunden sind und
- über welche Schwachstellen die Angreifer

sowohl Firmen- und Privatrechner als auch verteilte Netzwerkstrukturen, wie Cluster, angreifen.

### Gefahren, Schwachstellen, Schutzziele und Angriffsformen in Netzwerken

Um Datensicherheit (engl. safety), Informationsflusssicherheit (engl. security) und mit ergänzenden Konventionen technischen Datenschutz (engl. protection) zu garantieren, müssen die Gefahren, Schwachpunkte als auch Schutzziele analysiert bzw. bestimmt werden. Bekannte Gefahren und Schwachstellen sind gegeben durch:

- Sabotage und Vandalismus,
- Nichtbeachtung vereinbarter Konventionen,
- organisatorische und technische Lücken in der Realisierung von Netzwerken.

Folgende Schutzziele lassen sich im Rahmen der Untersuchung von Sicherheitsszenarien ableiten:

- Echtheit,
- Integrität,
- Identität,
- Vertrauenswürdigkeit,
- Verfügbarkeit,
- Nichtabstreitbarkeit und
- Anonymität.

Um schließlich Gefahren abwehren zu können und Schwachstellen konkret für ein System zu ermitteln, müssen die konkreten technisch initiierten Angriffe studiert werden. Bisher wurden einige Computerviren, -würmer und so genannte Trojaner untersucht, allerdings nicht den bereits ermittelten Formen von Gefahren und Schwachstellen zugeordnet, über die Computerviren, -würmer und Trojaner in IT-Systeme eindringen können. Aus dieser Analyse von Schwachstellen und der Wirkung von Angriffen auf ein IT-System lassen sich wiederum gewisse sich wiederholende Formen von Angriffe ableiten, wie

- Verweigerung eines Dienstes / denial of service
- Ausschnüffeln / snooping
- Verschleiern / Spoofing
- Angriff über die Mitte einer Verbindung / man of the middle attack

Die genannten Angriffsformen werden auf einzelne Firmen- oder Privatrechner gefahren. In einem verteilten Rechnersystem bzw. einem Verbund von mehreren Rechnernetzen besteht die Möglichkeit weitere Formen von Angriffen zu implementieren. Dazu gehören z.B.

- Vergiftungen von Adressräumen (engl. Stichwort: Address Resolution Protocol Poison / ARP Poison),
- die speziellen Angriffe auf Internetdienste, die diese Dienste zum Absturz bringen sollen (engl. Stichwort Internet Information Services crash / IIS crash) oder auch
- die Erzeugung von übermäßig viel Interverkehr (engl. Stichwort smurf attack) sowie
- so genannte Bot-Netze.

### Einfache Angriffe auf Firmen- und Privatrechner

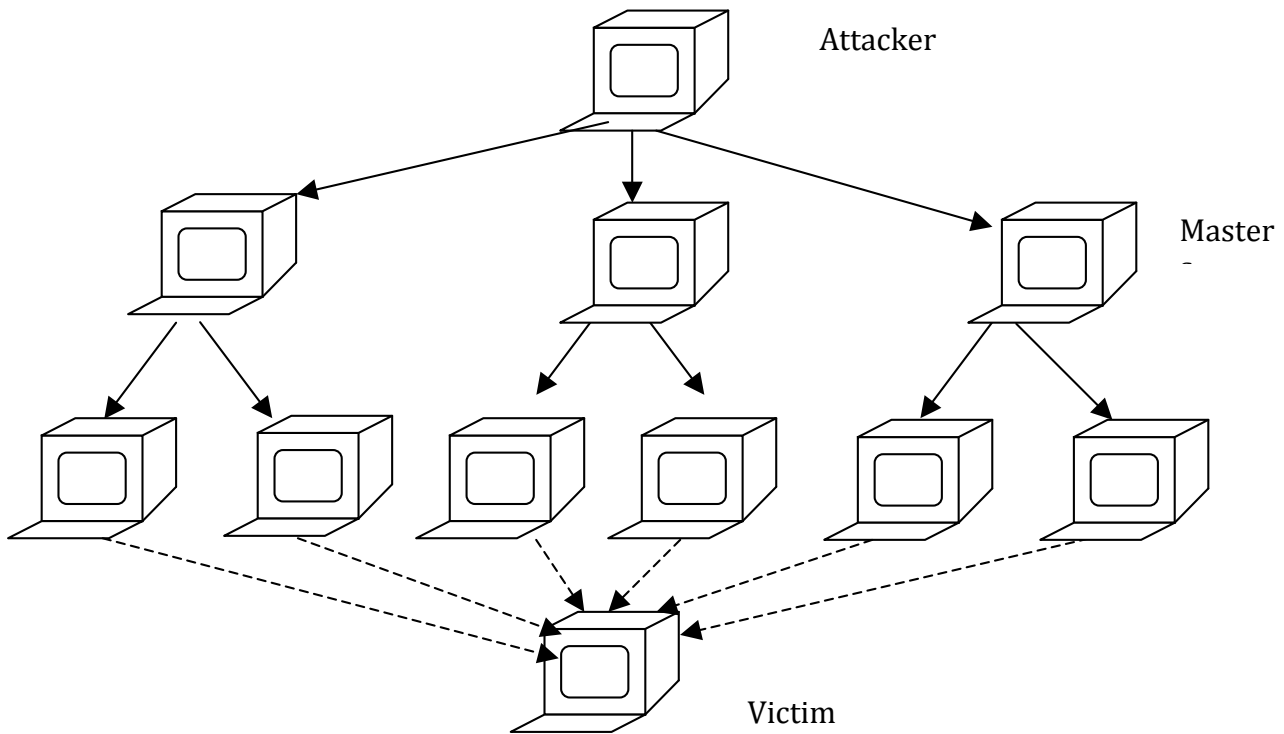
Wir haben bereits die folgenden Angriffsformen unterschieden. Betrachten Sie dazu die Schemata, die auf Folie 122 gegeben sind. Wir unterscheiden hier: snooping, man-in-the-middle attack, denial-of-service und spoofing. Dabei möchte jemand am Rechner A mit jemanden am Rechner B kommunizieren. Von Rechner C soll der Angreifer kommen. Diese Schemata können auf die bereits vorgestellten Angriffe durch Computerviren, würmer und Trojaner angewendet werden.

1. Untersuchen Sie die Beispiele erneut und machen Sie eine Ergebnistabelle mit
  - a. Bezeichnung des Angriffs,
  - b. Form des Angriffs gemäß Schemata (mehrfach Nennungen sind möglich),
  - c. Beschreibung des Ablaufs (welche Elemente gehören in die Initialphase, welche Elemente gehören in die Schadensphase?)
  - d. Gefahren,
  - e. Verletzte Schutzziele und
  - f. Möglichen Abwehrmechanismen
2. Überlegen Sie sich welche Angriffsformen bisher unberücksichtigt sind?

### Verteilte Angriffe auf Netzwerke

Bisher sind "einfache" Verweigerungen von Diensten untersucht worden.

1. Können Sie sich solche Angriffe in verteilten Netzstrukturen vorstellen, so genannte „distributed denial-of-service attacks“ (DDoS attacks)? Schauen Sie sich dazu das folgende Schema an und überlegen Sie anhand der folgenden zu untersuchenden Angriffen, welche Abläufe bei Angriffen stattfinden, wie
  - a. ARP Poison
  - b. IIS Crash und
  - c. Smurf attack



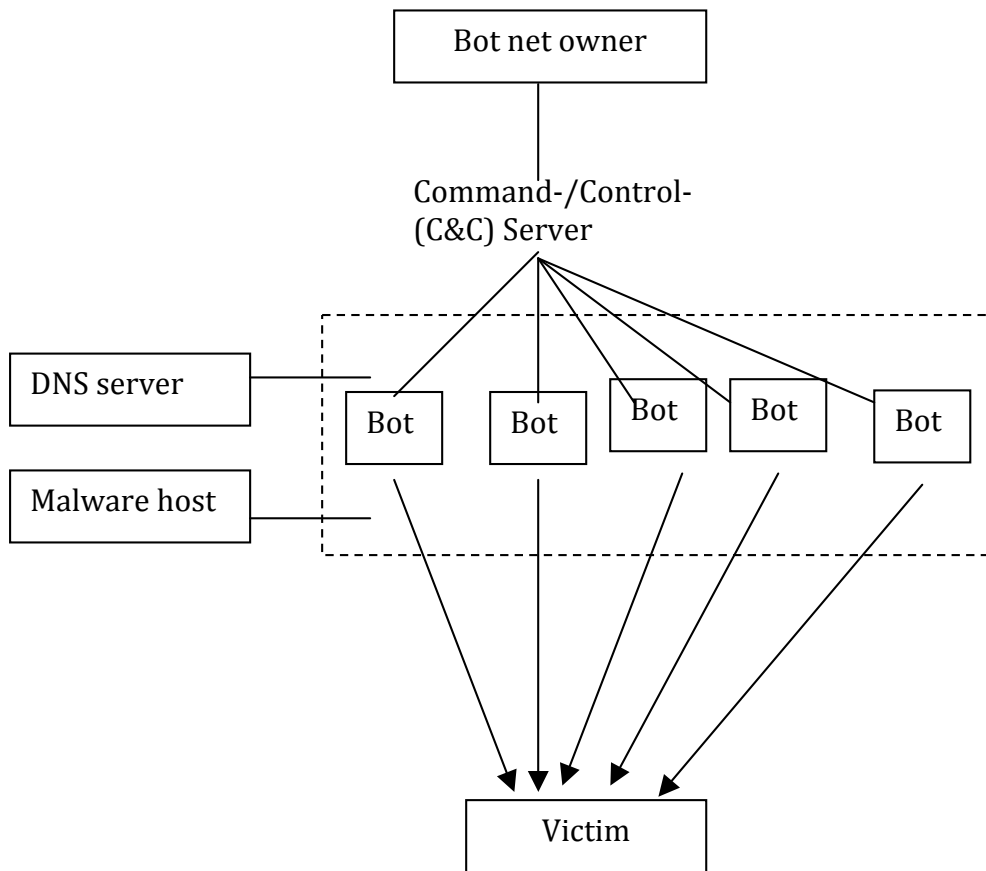
2. Welche Eigenschaften haben verteilte Angriffe zusätzlich zu einer „einfachen“ Verweigerung von Diensten? Listen Sie solche Eigenschaften auf und erklären Sie die gefundenen Eigenschaften.
  - a. Wie wird ein verteilter DDoS-Angriff gestartet? Denken über mögliche Teilphasen nach, wenn ein Netzwerk infiziert worden ist.
  - b. Wie wird eine Schadensphase bei einem DDoS-Angriff gestartet?
  - c. Beschreiben Sie den Ablauf eines DDoS-Angriffs mit eigenen Worten.
3. Ergänzen Sie ggf. das gegebene Schema um notwendige Details.
4. Schließen Sie, wie ein solcher DDoS-Angriff vermieden oder auch abgewehrt werden kann.

### Bot-Netze

Eine neuere Form von verteilten Angriffen sind so genannte Bot-Netze. Untersuchen Sie im Folgenden die Struktur von Bot-Netzen. Sie erhalten im Folgenden eine kurze Beschreibung, wie Bot-Netze funktionieren. Um diese Bot-Netze zu analysieren, ist die Funktionsweise genauer zu untersuchen.

1. Studieren Sie das folgende einfache Schema von Bot-Netzen.
2. Lesen Sie den beschreibenden folgenden Text zur Funktionsweise von Bot-Netzen.
3. Machen Sie dann eine genauere Analyse zur Funktionsweise von Bot-Netzen.

## Einfaches Schema von Bot-Netzen



## Kurze Beschreibung zur Funktionsweise von Bot-Netzen

Ein Bot-Netz ist ein Verbund (Cluster) von Computersystemen im Internet. Ein Bot-Netz ist auch ein Modell für einen Verbund von infizierten Rechnern, die Bots genannt werden. Bot steht dabei für eine Verkürzung von "robot". Bots arbeiten für und agieren in Teilnetzen des Internets. Bots werden durch Angreifer implementiert und kontrolliert. Nachdem ein Bot gestartet ist, verteilt er schadhafte Software im infizierten Teilnetz und versucht weitere Teilnetze – spezifiziert innerhalb des Angriffs oder durch den Angreifer selbst – zu schaden. Dabei verteilen Bots schadhafte Software selbständig. Ein Server für Schadenssoftware wird oftmals aktualisiert. Dabei wird eine Gruppe von Bots, die zu einem Bot-Netz zusammengefasst sind, durch einen so genannten Command- und Control Server (C&C Server) gesteuert. Wenn nun Aktionen von Bot-Netzen beobachtet werden, ist festzustellen, dass IRC Server zumeist als Wirte (hosts) genutzt werden. Dazu holt sich der Bot die URL des Opfers, des IRC Servers; d.h. um ein Bot-Netz zu installieren, ist das (erste) Zielsystem des Angriffs ein DNS Server, um IP Adressen anderer Zielsysteme zu erhalten.

## Weitere Analyse von Bot-Netzen

Um weitere Informationen zu Bot-Netzen zu erhalten, beantworten Sie bitte die folgenden Fragen:

- Warum ist ein IRC server als C&C Server in einem Bot-Netz anwendbar? Welche Funktionalität des IRC Servers wird benötigt, um eine Kommunikation zwischen den einzelnen Bots zu gewährleisten?
- Sind andere Mechanismen als ein IRC Server anwendbar, um ein Bot-Netz zu installieren und zu kontrollieren? Welche Schwachpunkte im Internet gibt es

noch, die sich angreifende Bot-Netze zu eigen machen können, um ein Netzwerk zu nutzen?

- c. Betrachten Sie die gegebene Bot-Netz Struktur. Wie können die Schwachstellen geschützt werden? Wie z.B. kann der IRC Server geschützt werden?
- d. Der Informationsfluss im Internet wird durch unterschiedlichste Protokolle realisiert. Welche Protokolle kommen noch in Frage, so dass Bot-Netze anwendbar sind? Insbesondere welche Protokolle eignen sich, um die Schadenssoftware bei einem laufenden Bot-Netz in ein angegriffenes Netz einzuschleusen?
- e. Denken Sie über die Administration von IP Adressen durch einen DNS Server nach. Wie kann ein Bot-Angriff auf den DNS Server erfolgen?
- f. In welchem Verhältnis steht ein Bot-Netz-Angriff zu anderen bereits studierten Angriffsformen? Können auch andere solcher Angriffsformen innerhalb eines Bot-Netzes implementiert werden? Wenn ja, welche Formen lassen sich wiederholen und wie? Was sind die gemeinsamen Eigenschaften dieser Angriffe?
- g. Fassen Sie Ihre Ergebnisse zusammen, indem Sie in ca. 10 Sätzen die Arbeitsprozesse von Bot-Netzen beschreiben.