

### Angriffe gegen Netzwerkinfrastrukturen und Anwendungen Demonstration eines Angriffs auf einen Windows-Server

Projektarbeit vorgelegt von Lars Findorff und Stefan Humml im Fach „Netzwerksicherheit 1“

#### Einführung

Server, die wichtige Informationen enthalten, beispielsweise Web- oder Fileserver sind häufig Ziel von Angriffen. Dies gilt auch für Server, die nur innerhalb eines Intranets, also für einen eingeschränkten Kreis von Mitarbeitern, erreichbar sind. Verschiedenen Studien zufolge finden etwa zwei Drittel der IT-Angriffe gegen ein Unternehmen durch Mitarbeiter, also mit Hilfe des Intranets statt. Dennoch wird häufig argumentiert, im Intranet gäbe es wenig bis keine Gefahren. Ein schlechtes Absichern der Server und seltenes Einspielen von Sicherheitsupdates ist die Folge.

Die hier vorgestellten praktischen Beispiele zeigen den erfolgreichen Angriff auf einen Windows-Server durch Ausnutzen einer Sicherheitslücke im Betriebssystem. Nach erfolgreicher Kompromittierung wird ein sog. Rootkit installiert, das in der Lage ist, die Aktivitäten auf dem System vor dem Administrator zu verbergen.

Neben der Demonstration der Auswirkung einer solchen Schwachstelle zeigt das Beispiel das typische Vorgehen eines Angreifers und gibt einen Einblick in den Werkzeugkasten professioneller Hacker.

Die hierbei eingesetzten Programme sind im Internet kostenlos verfügbar. Auch diese Tatsache zeigt, dass viele Angriffe weder besonders tiefgehendes Know-How noch großes Budget erfordern.

#### Beschreibung des Versuchs

Die erste Phase eines Angriffs, wie er hier gezeigt wird, nennt man Reconnaissance oder Fingerprinting. Dabei wird der Server auf mögliche laufende Anwendungen, die Schwachstellen enthalten können,

geprüft. Zu diesem Zweck wird ein sog. Port-Scanner eingesetzt, der diese Funktionalität bietet und detailliert Aufschluß über Betriebssystem und laufende Applikationen gibt:

```
Starting Nmap 4.76 ( http://nmap.org )
Interesting ports on Server (192.168.239.137):
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
MAC Address: 00:0C:29:67:2A:3D (VMware)
Device type: general purpose
Running: Microsoft Windows XP!2003
OS details: Microsoft Windows XP Professional
```

Abb: Durchlauf eines Portscanners

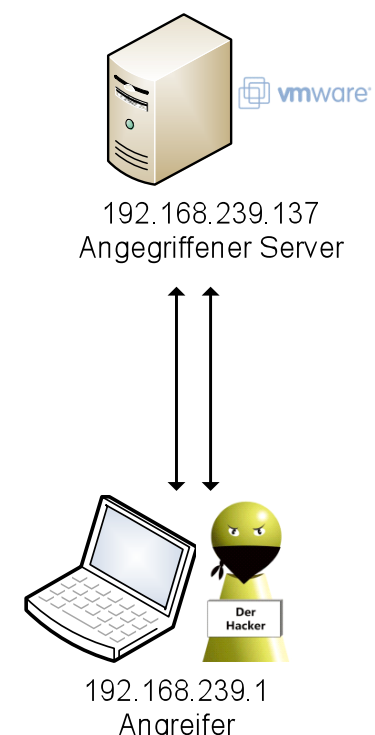
In dem gezeigten Beispiel wird ein Windows Server 2003 identifiziert. Geübten Angreifern bzw. Sicherheits-Interessierten ist bekannt, dass vor kurzem eine Schwachstelle in Windows gefunden wurde, die die vollständige Kompromittierung des Systems zulässt.

Dem Fingerprinting folgt das gezielte Angreifen vorhandener oder vermuteter Schwachstellen. In dem hier gezeigten Beispiel wird eine bekannte Sicherheitslücke ausgenutzt, die dem Angreifer hochprivilegierten Zugriff auf das System erlaubt. Nach der initialen Kompromittierung werden mit Hilfe der Kommandozeile auf dem angegriffenen System neue Benutzerdaten eingegeben und diesem Benutzer administrative Rechte eingeräumt.

Um weiterhin den Server erreichen zu können, installiert der Angreifer danach eine sog. Remote-Shell, die jederzeit Kontakt zu einer hochprivilegierten Kommandozeile über das Netzwerk ermöglicht. Da jedoch insbesondere Dateien, Prozesse und offene Ports von Administratoren überwacht werden, kommt ein sog. Rootkit zum Einsatz, das das Verstecken eben dieser Spuren ermöglicht.

#### Architektur des Versuchs

Der angegriffene Server befindet sich innerhalb einer virtuellen Maschine und ist über die IP-Adresse 192.168.239.137 bzw. den Alias *Server* zu erreichen. Die Angriffe erfolgen hierbei von dem Laptop aus, der auch den virtuellen Server zur Verfügung stellt, wobei die Kommunikation via IP genutzt wird:



#### Gegenmaßnahmen

Die wichtigste Maßnahme, die gegen solche Angriffe getroffen werden kann ist die zeitnahe Installation von Sicherheits-Updates.

Weiterhin können sensible Server auch innerhalb eines Firmennetzwerkes durch Firewalls und Intrusion Detection Systeme geschützt werden. Somit kann die Erreichbarkeit des Servers und daraus folgend die Anzahl potenzieller Angreifer eingeschränkt werden.