

TECHNISCHE
UNIVERSITÄT
WIEN
VIENNA
UNIVERSITY OF
TECHNOLOGY

Abgabe 3

Internal Penetration Test

Version 1.2

Gruppenmitglieder:

0125638 Gerald Haider
0105011 Roman Vottner
0125850 Thomas Moser
0052189 Georg Glatz (Sprecher)

Dokumentenverlauf

Datum	Änderungen	Autor
25. Jän. 2006	Initialversion	Gerald Haider
28. Jän. 2006	Erweiterung	Gerald Haider
28. Jän. 2006	Erweiterung	Thomas Moser

Inhaltsverzeichnis

1	SCANNING	3
1.1	AUFFINDEN VON LAUFENDEN RECHNERN.....	3
1.2	PORTSCANS MIT NMAP.....	4
1.2.1	<i>Rechner 1 – Windows XP Client – 192.168.66.99</i>	4
1.2.2	<i>Rechner 2 – Domaincontroller – 192.168.66.100 = 192.168.67.1 = 192.168.68.1</i>	5
1.2.3	<i>Rechner 3 – Linux Server – 192.168.67.100</i>	5
1.2.4	<i>Rechner 4 – Datenbank Server – 192.168.68.100</i>	5
2	ENUMERATION.....	6
2.1	SMB NULL SESSIONS	6
3	VULNERABILITY ASSESSMENT.....	6
3.1	SCANNEN MITTELS NESSUS	6
4	PENETRATION	6
4.1	EINDRINGEN MIT HILFE VON METASPLOIT FRAMEWORK	6
4.1.1	<i>Rechner 1 – Windows XP Client – 192.168.66.99</i>	6
4.1.2	<i>Rechner 3 – Linux Server – 192.168.67.100</i>	7
5	COVER TRACKS AND BACKDOORS.....	7
5.1	INSTALLIEREN VON „ROOTKITS“	7
5.1.1	<i>rootkit für Windows XP Prof.</i>	7
5.1.2	<i>rootkit – Installation für Suse Linux 8.2</i>	7
6	SECURING THE SYSTEM.....	7
6.1.1	<i>Rechner 1 – Windows XP Client – 192.168.66.99</i>	7
6.1.2	<i>Rechner 3 – Linux Server – 192.168.67.100</i>	7
7	LISTE DER VERWENDETEN PROGRAMME.....	8

1 Scanning

Als erster Schritt des Penetration Testings haben wir versucht, uns ein Bild der vorhandenen Rechnerlandschaft zu machen. Dazu wurde zuerst eine Liste aller verfügbaren und damit angreifbaren Rechner ermittelt und dann jeder einzelne dieser Rechner auf Sicherheitslücken bzw. Angriffsmöglichkeiten überprüft.

1.1 Auffinden von laufenden Rechnern

Um herauszufinden welche Rechner im Netzwerk vorhanden sind, wurde mittels nmap ein Ping Scan durchgeführt:

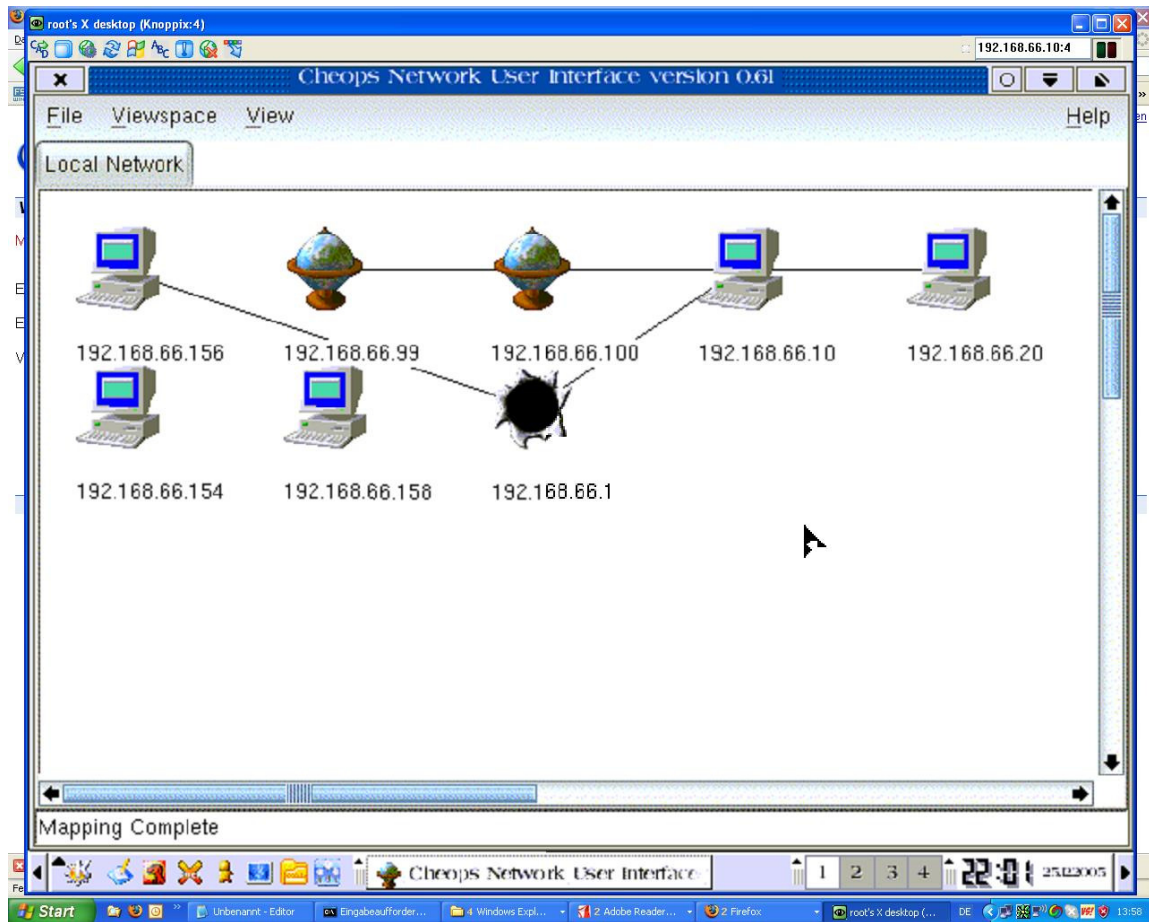
```
root@pentest2:~# nmap -sP 192.168.*.*

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-12-25 21:32 EST
Host 192.168.66.0 seems to be a subnet broadcast address (returned 1 extra pings).
Host 192.168.66.10 appears to be up.
MAC Address: 00:0C:29:5A:E8:EE (VMware)
Host 192.168.66.20 appears to be up.
Host 192.168.66.99 appears to be up.
MAC Address: 00:0C:29:75:AE:21 (VMware)
Host 192.168.66.100 appears to be up.
MAC Address: 00:0C:29:9D:16:E5 (VMware)
Host 192.168.66.255 seems to be a subnet broadcast address (returned 1 extra pings).
Host 192.168.67.1 appears to be up.
Host app.simcorp.com (192.168.67.100) appears to be up.
Host 192.168.68.1 appears to be up.
Host db.simcorp.com (192.168.68.100) appears to be up.
Nmap run completed -- 65536 IP addresses (11 hosts up) scanned in 1789.382 seconds
```

Wie man aus oben angegebenen Listing ersehen kann, scheint es im gescannten Netzbe-
reich 6 laufende Rechner zu geben (wie sich später herausstellte, waren es in Wirklichkeit
nur 4).

Im Nachhinein betrachtet muss auch festgestellt werden dass diese Art des Scannens
nach Angriffspfern, nicht gerade die leiseste Variante darstellte, und somit mit ziemlicher
Sicherheit von IDS Systemen detektiert worden wäre. Eine mögliche leisere Variante um
an die Adressen der Hosts zu kommen wäre eine genauere Inspektion des laufenden DNS
Servers gewesen (DNS Zone Transfer).

1.2 Topologie des Netzwerks



1.3 Portscans mit nmap

Nachdem die Hosts ermittelt waren wurden die einzelnen Rechner wiederum mit nmap auf offene Ports gescannt:

1.3.1 Rechner 1 – Windows XP Client – 192.168.66.99

```
root@pentest2:/# nmap -O 192.168.66.99
Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-12-25 23:01 EST
Interesting ports on 192.168.66.99:
(The 1657 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
3389/tcp  open  ms-term-serv
5000/tcp  open  UPnP
MAC Address: 00:0C:29:75:AE:21 (VMware)
Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Pro or Advanced Server, or Windows XP, Microsoft Windows XP SP1
Nmap run completed -- 1 IP address (1 host up) scanned in 2.194 seconds
```

Da der Port für „Remote Desktop“ offen war, versuchten wir uns mit einem RDP Client auf die Maschine zu verbinden, was uns die Erkenntnis brachte das es sich um eine „Windows XP Professional“ Client, namens „Minniemaus“ handelte, welcher in der Domäne „simcorp“ betrieben wurde.

1.3.2 Rechner 2 – Domaincontroller – 192.168.66.100 = 192.168.67.1 = 192.168.68.1

```
root@pentest2:/# nmap -O 192.168.66.100
Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-12-25 22:23 EST
Interesting ports on 192.168.66.100:
(The 1649 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1026/tcp  open  LSA-or-nterm
1029/tcp  open  ms-lsa
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-term-serv
MAC Address: 00:0C:29:9D:16:E5 (VMware)
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scanned in 8.581 seconds
```

Da der Port für „Remote Desktop“ offen war, versuchten wir uns mit einem RDP Client auf die Maschine zu verbinden, was uns die Erkenntnis brachte das es sich um einen Rechner mit „Windows 2000 Server“ handelte, welcher als Domaincontroller für die Domäne „simcorp“ betrieben wurde. Aufgrund der Portscans und der Testverbindungen auf die offenen RDP Ports konnten wir feststellen das dieser Rechner über 3 IP Adressen (Netzwerkarten) ansprechbar ist: 192.168.66.100 = 192.168.67.1 = 192.168.68.1
Somit reduzierte sich die Anzahl der anzugreifenden Rechner auf 4 Stück.

1.3.3 Rechner 3 – Linux Server – 192.168.67.100

```
root@pentest2:/# nmap -O 192.168.67.100
Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-12-25 21:55 EST
Interesting ports on app.simcorp.com (192.168.67.100):
(The 1657 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
113/tcp   closed auth
139/tcp   open  netbios-ssn
143/tcp   open  imap
3128/tcp  open  squid-http
Device type: general purpose
Running: Linux 2.4.X
OS details: Linux 2.4.19 - 2.4.20, Linux 2.4.21 (x86)
Nmap run completed -- 1 IP address (1 host up) scanned in 22.753 seconds
```

Aufgrund der offenen Ports und des OS Fingerprints von nmap kann davon ausgegangen werden das es sich hier um einen Linux Server handelt.

1.3.4 Rechner 4 – Datenbank Server – 192.168.68.100

```
root@pentest2:/# nmap -O 192.168.68.100
Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-12-25 21:54 EST
```

```
Interesting ports on db.simcorp.com (192.168.68.100):
(The 1659 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
1025/tcp  open  NFS-or-IIS
1027/tcp  open  IIS
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scanned in 8.280 seconds
```

2 Enumeration

2.1 SMB Null Sessions

Versuchen Sie Userlisten inkl. Passwörter, Rechte, Netzwerkdienste und deren Versionen usw. herauszufinden und beschreiben Sie diese inkl. der verwendeten Tools, Methoden und Begründungen für deren Benutzung.

Georg wos habts ihr da gemacht?

3 Vulnerability Assessment

3.1 Scannen mittels Nessus

Das Scannen nach Schwachstellen auf den gefundenen Systemen erfolge größtenteils mittels Nessus. Hierzu wurde die aktuellste, von uns manuell installierte Version von Nessus, mit den Standardeinstellungen auf die Rechner losgelassen. Es wurde aber nur nach Schwachstellen gesucht, die das zu scannende System nicht zum Absturz bringen können.

Neben dem Scannen mit Nessus wurden die offenen Ports auch manuell untersucht. So wurde zum Beispiel festgestellt welche Webseiten der Webserver anbieten und ob hier etwas auf irgendwelche Verwundbarkeiten vorliegen.

4 Penetration

4.1 Eindringen mit Hilfe von Metasploit Framework

4.1.1 Rechner 1 – Windows XP Client – 192.168.66.99

Dieser Rechner wurde mittels des im Metasploit Framework integrierten „Microsoft ASN.1 Library Bitstring Heap Overflow“ Exploits übernommen. Als Payload wurde bei der ersten Attacke „add User“ gewählt um einen User anzulegen, um dann komfortabel über RDP auf den Rechner zugreifen zu können.

4.1.2 Rechner 3 – Linux Server – 192.168.67.100

Dieser Rechner wurde mittels des im Metasploit Framework integrierten „Samba trans2open Overflow“ Exploits übernommen. Als Payload wurde eine „reverse root shell“ gewählt, wodurch wir vollen root Zugriff auf den Rechner hatten

Die restlichen 2 Rechner konnten von uns leider nicht übernommen werden.

5 Cover Tracks and Backdoors

Versuchen Sie, die auf den eroberten Systemen verursachten Spuren zu verwischen und möglichst geheime Hintertüren zu installieren, welche einen dauerhaften Zugang ermöglichen. Beschreiben Sie die verwendeten Tools, Methoden und Begründungen für deren Benutzung sowie die gewonnenen Erkenntnisse.

5.1 Installieren von „rootkits“

5.1.1 rootkit für Windows XP Prof.

georg was hast du gemacht?

5.1.2 rootkit – Installation für Suse Linux 8.2

Die Installation eines rootkits auf dem Linux System wurde zwar versucht, scheiterte aber da wir in der kurzen Zeit kein rootkit finden konnten das sich korrekt installieren lies und auch funktionierte.

6 Securing the System

Was hätte man gegen jede einzelne gefundene Schwachstelle tun können, um Sie zu minimieren oder zu vermeiden? Beschreiben Sie für jede gefundene Angriffsmethode die zur Absicherung möglichen Tools, Methoden und Begründungen, sowie die gewonnenen Erkenntnisse.

6.1.1 Rechner 1 – Windows XP Client – 192.168.66.99

Um dieses System abzusichern müssten nur die aktuellsten Patches von Microsoft eingespielt werden, die auf dem System uns vorliegenden System ja eindeutig schon länger nicht mehr eingespielt worden sind. Der konkrete Angriff könnte jedoch auch über aktivieren der integrierten Firewall abgefangen werden.

6.1.2 Rechner 3 – Linux Server – 192.168.67.100

Auch auf diesem System sollten sofern noch verfügbar die aktuellen Patches von SUSE eingespielt werden, falls diese nicht mehr verfügbar sind, kann man die betroffenen Anwendungen entweder manuell updaten, oder über den Einsatz einer Firewalllösung nachdenken, welche den Angriff auch verhindert hätte.

7 Liste der verwendeten Programme

- VMWare Workstation
- Auditor Security Live CD
 - o Metasploit Framework (<http://www.metasploit.com/>)
 - o nmap (<http://www.insecure.org/nmap/>)
 - o Nessus Security Scanner (<http://www.nessus.org/>)