

Übung, Teil 3: **Internal Penetration Test**

Typ: **GRUPPENARBEIT in 4er Gruppen**

Deadline Bericht: **28.01.2006 23:55**

Abgabegespräch: **inkl. Endprüfung 31.01.2006**

Für diesen Teil der Übung kommt ein eigens entwickeltes Penetration-Testing-Labor zum Einsatz. Dieses wird am IFS gehostet und bildet ein internes Netzwerk eines Klienten nach. Ziel ist, das praxisnahe Hacken in einer gesicherten Umgebung zu ermöglichen, um so die benötigten Skills und Tools zu erlernen.

Dabei werden unterschiedliche Gebiete berücksichtigt, wie etwa Scanning, Vulnerability Assessment, Enumeration, Hacking into Linux and Windows sowie Security, um ein möglichst breites Übungs- und Lerngebiet zu bieten.

Um dies zu bewerkstelligen, stehen über ein VPN und VNC zwei Attack-Workstations zur Verfügung, sodass paralleles Arbeiten zu zweit möglich ist. Diese beiden Workstations sind mittels SSH auf 192.168.66.10 resp. 20 erreichbar. Es laufen bereits VNC Sessions auf 192.168.66.10:4 und 192.168.66.20:1. Das Passwort für alle Verbindungen auf diesen Maschinen ist „h4ckm3“. Natürlich können weitere Attack-Workstations auch direkt im inneren Netzwerk erobert werden ;)

Dazu bekommt jede 4er Gruppe einen Timeslot von 12:00 Mittags bis 8:00 am nächsten Morgen (Hacker arbeiten meistens nachts ;) zur Verfügung gestellt. Die meisten Tools werden als Komfortbonus bereits auf den Attack-Workstations vorinstalliert sein, eine Internet-Verbindung ist jedoch über einen Proxy (192.168.66.1:8080) vorhanden, um Tools oder Exploit Code nachzuladen.

Aufgabenstellung:

- Bildung einer 4er Gruppe, Zuteilung eines Timeslots inkl. entsprechender Zugangsdaten. Installation und Test der VPN-Verbindung.
- Durchführung eines internen Penetration-Tests anhand der üblichen, in der VO vorgestellten, Methodologie.
- Erstellen eines detaillierten Berichts mit allen durchgeführten Tätigkeiten und gefundenen Sicherheitslücken inklusive Lösungs- respektive Penetrationsweg, Links zu externen Seiten, die im Zuge der Lösung in Anspruch genommen wurden, Screenshots von relevanten Inhalten, sowie detaillierten Vorschlägen zur Absicherung gegen die erkannten Lücken.

Deliverables:

Elektronisch über Moodle bis 28.01.2006

- Lösungsbericht: Beschreibung der Lösung und des Vorgehens bezüglich der Bearbeitung der Angabe, Erklärung, was warum wie gemacht wurde und welche Sicherheitsrisiken sich daraus ergeben. Links zu eventuell verwendeten externen Seiten und Programmen angeben, Screenshots von wichtigen Details, sowie detaillierte Vorschläge zur Absicherung gegen die erkannten Lücken.

- Bitte verwenden Sie die gleiche Nummerierung und Reihenfolge wie im Fragenkatalog, um eine Zuordnung zu erleichtern.
- Format: .pdf

Abgabegespräch:

31.01.2006

- Beim Abgabegespräch müssen Sie Ihre Lösungswege erklären können sowie über die entsprechenden Grundlagen Bescheid wissen. Was bedeuten die aufgezeigten Sicherheitsprobleme für Sie als Administrator/CSO?
 - o Beispielfragen: „Wie haben sie Aufgabe xyz gelöst?“ – „Was versteht man unter Arp Spoofing? Wie geht man vor, falls man einen Service auf seine Version hin untersuchen möchte“ – „Welche Probleme ergeben sich aus Windows Null Sessions? Beispiele? Was sollten Admins (bzw. User) daher beachten?“
 - o NICHT: „Wie lauten sämtliche Command Line Switches von nc.exe?“ – „Wie funktioniert Sequence Number Prediction für Windows Server 2003 SP1 im letzten Patchstand?“
- Falls Sie eine besonders elegante / ungewöhnliche Lösung gefunden haben, weisen Sie bitte darauf hin.
- Bringen Sie bitte einen Ausdruck Ihres Berichts zum Abgabegespräch mit!

Punkteschema:

Insgesamt gibt es **20** Punkte zu erreichen. Da die verschiedenen Aufgaben sehr unterschiedliche Schwierigkeitsgrade aufweisen, wird zur besseren Gewichtung mit 100 Prozentpunkten gerechnet.

Die Endpunktezahlgibt sich dann z.B. folgendermaßen:

- 75 Prozentpunkte erreicht (siehe Fragenkatalog für Verteilung)
- 75% von **20** Punkten entsprechen **15**
- Aufrunden auf halbe Punkte → Endpunktezahlg = **15** Punkte

Wie im echten Leben sollten Sie versuchen, die Systeme, die Sie hacken, nicht zu töten oder zum Abstürzen zu bringen! **Ein Restart bzw. Restore** ist auf Mailrequest an den Tutor (andreas@furtenbacher.com mit cc an tomek@ifs.tuwien.ac.at) möglich, kostet Sie jedoch **20% der erreichten Punkte**. **Des Weiteren kann dies je nach Zeitpunkt einige Zeit dauern bzw. überhaupt einen Folgetermin bedeuten.** Eine detaillierte Aufschlüsselung der Prozentpunkte findet sich nachfolgend.

Detaillierte Aufschlüsselung der zu erreichenden Prozentpunkte je Aufgabe:

Step	Prozentpunkte
1 Scanning	5
2 Enumeration	10
3 Vulnerability Assessment	5
4 Penetration	50
5 Cover Tracks and Backdoors	10
6 Securing the System	20
	<u>100</u>

Rechtliche Anmerkungen:

Dieses Lab ist eine Übungsumgebung und wurde mit viel Aufwand für Übungszwecke aufgebaut. Wer die gelernten Methoden und Angriffe ohne förmliche

Autorisierung auf andere Netze als das Übungsnetzwerk oder seine eigenen Privatnetze anwendet, muss mit entsprechenden rechtlichen Folgen rechnen. Dies gilt insbesondere auch für alle Instituts- und Universitätssysteme ab und inklusive des VPN-Routers (192.168.66.1) auswärts. Bei unethischem Verhalten werden wir das Lab sofort stoppen und die entsprechenden Logfiles sowie alle IDS-Protokolle auf Detailebene untersuchen respektive eventuell auch rechtliche Schritte einleiten.

EINRICHTUNG DES VPN ZUGANGS

Der VPN Zugang ist ein IPSEC/L2TP Zugang. Die User lauten **vpn1-vpn4**, das Passwort wird Ihnen kurz vor Beginn der Übung zugeteilt. Unter Windows richten Sie die Verbindung wie folgt ein (Die Einrichtung unter Unix sollte mit den angegebenen Daten auch möglich sein, als Protokoll stehen MSCHap, MSChapv2 und Chap zur Verfügung):

Start-> Einstellungen/Systemsteuerung-> Netzwerkverbindungen-> Neue Netzwerkverbindungen erstellen -> Weiter -> Verbindung mit dem Netzwerk am Arbeitsplatz herstellen -> Weiter -> VPN-Verbindung -> Weiter -> Irgendeinen Namen ->Weiter -> (Je nach Bedarf Anfangsverbindung wählen -> Weiter ->) **128.131.167.192** ->Weiter ->Weiter -> Fertigstellen.

Eigenschaften anklicken:

Auf Reiter Sicherheit gehen.

IpSec Einstellungen

Der vorinstallierte Schlüssel lautet: „**PenTestLab2005**“

Bei Netzwerk **IpSec/L2TP** als VPN Typ auswählen

Fertig

Als Benutzer **vpn1**, bzw vpn2-4 eingeben

Das zugesendete Passwort eingeben

Nun sollten sie die Maschinen 192.168.66.10 und 20 pingen und sowie wie am Anfang beschrieben über SSH und VNC erreichen können. - Verwendet beim Einrichten neuer VNC Screens über SSH mit vncserver den geometry Parameter um angenehme Auflösungen einzustellen.

Alle Angriffe sollten von diesen oder nachfolgend eroberten Maschinen durchgeführt werden!

FRAGENKATALOG

Vorwort

Die verschiedenen Steps des Labs verfügen über sehr unterschiedliche Schwierigkeitsgrade, auch dieser Fragenkatalog setzt Schwerpunkte. Ob Sie die Abgabe strikt nach den Punkten oder chronologisch strukturieren, bleibt Ihnen

überlassen, jedoch ersuchen wir Sie, deutlich auf die Kategorie zu verweisen, um eine klare Zuordnung zu ermöglichen.

1 Scanning

Beschreiben Sie die verwendeten Tools, Methoden und Begründungen für deren Benutzung sowie die gewonnenen Erkenntnisse inkl. IPs, Funktion, Netzplan, offenen Ports usw. zum vorhandenen Netzwerk.

2 Enumeration

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.

3 Vulnerability Assessment

Untersuchen Sie alle gefundenen Systeme auf Schwachstellen und recherchieren Sie dafür erhältliche externe Exploits und Advisories. Beschreiben Sie die verwendeten Tools, Methoden und Begründungen für deren Benutzung sowie die gewonnenen Erkenntnisse.

4 Penetration

Nützen Sie die vorhandenen Sicherheitslücken aus, um neue Angriffsziele erreichen zu können. Versuchen Sie möglichst alle vorhandenen Angriffsvektoren zu erkennen und auszunützen. Beschreiben Sie die verwendeten Tools, Methoden und Begründungen für deren Benutzung sowie die gewonnenen Erkenntnisse. - Bitte hinterlasst auf jedem gehackten Rechner ein neu erstelltes Verzeichnis mit Namen OWNED im C:\ oder root Verzeichnis, in welchem eine Datei (nur admin/root solle sie lesen dürfen) details.txt liegt. Diese soll den Namen der Person(en) welche dies vollbracht haben, eine Kurzbeschreibung was gemacht wurde, Datum und Uhrzeit beinhalten um leichtere Nachvollziehbarkeit zu gewährleisten.

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.

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.

...4ND D0N'7 F0R637 70 H4V3 FUN! ;)