Windows-Sicherheitslücken & Social Engineering

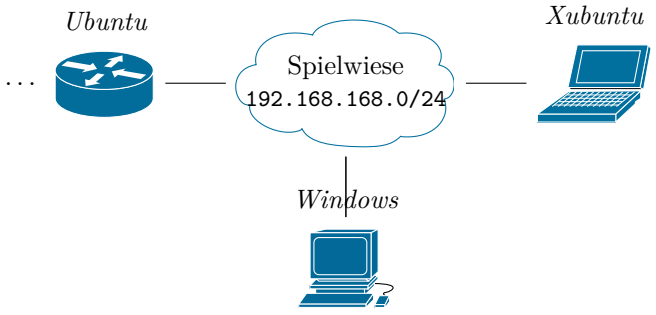
Lösen Sie die nachfolgenden Aufgaben und bereiten Sie diese bis zum nächsten Lehrveranstaltungstermin vor.

01.

a) Laden Sie *Adobe Flash Player* Version 15.0.0.167 von `https://helpx.adobe.com/flash-player/kb/archived-flash-player-versions.html` auf Ihren **Host**-Rechner herunter und installieren Sie die reguläre (d.h. nicht die Debug-) Version für *ActiveX* (für *Internet Explorer*) in der *Windows*-VM. Überprüfen Sie den Erfolg der Installation, indem Sie *Internet Explorer* starten und im Menü *Tools* unter *Manage Add-ons* bei *Show* die Option *Run without permission* (später *All add-ons*) auswählen, wo anschließend *Shockwave Flash Object* in der Liste erscheinen sollte. Diskutieren Sie die Sicherheitsimplikationen der Installation unter Berücksichtigung des in der Grafik unten dargestellten Netzwerkes.

b) Starten Sie *Metasploit* auf der *Xubuntu*-VM und wechseln Sie in das Modul `auxiliary/server/browser_autopwn2`. Setzen Sie die Option `MaxExploitCount` auf 100 und starten Sie das Modul. Verschicken Sie den ausgegebenen Serverlink per Email (z.B. mit dem Befehl `sendmail` in einer separaten SSH-Sitzung) an `victoria.victim@<Domänenname>` (z.B. `victoria.victim@spielwiese-unterweger.tld`). Rufen Sie die Email in der *Windows*-VM ab (z.B. mit *Thunderbird*) und klicken Sie auf den Link. Diskutieren Sie die Ausgabe des *Metasploit*-Moduls in der *Xubuntu*-VM nach Anklicken des Links.

c) Brechen Sie den Angriffsversuch ab und wiederholen Sie ihn erneut. Verwenden Sie dabei einen Emailtext, der das Anklicken des Links im Allgemeinen wahrscheinlicher macht und passen Sie den URI über die Moduloptionen derart an, dass dieser zum Emailtext passt. Gestalten Sie außerdem die Startseite des Serverlinks über die Option `HTMLContent` so, dass der Benutzer möglichst lange auf der Seite verweilt und diskutieren Sie, warum das bei einem Angriff praktisch relevant ist.



02.

a) Setzen Sie den Angriff aus der vorherigen Aufgabe fort, indem Sie eine der geöffneten *meterpreter*-Sitzungen interaktiv öffnen und mit dem Befehl `screenshot` einen Screenshot des angegriffenen Rechners anfertigen. Betrachten Sie diesen in der *Xubuntu*-VM und erläutern Sie die Sicherheitsimplikationen. Diskutieren Sie darüber hinaus die weiteren Informationsbeschaffungsmöglichkeiten, die z.B. mit dem Befehl `help` aufgelistet werden können.
Hinweis: Brechen Sie mit `jobs -K` den laufenden Server ab, bevor Sie weitere Angriffe durchführen – diese benötigen oft bestimmte Ports, die sonst durch den Server belegt wären.

b) Wenden Sie den Exploit aus dem Modul `exploit/windows/local/ms15_051_client_copy_image` unter Verwendung der aktiven *meterpreter*-Sitzung an, um Administratorrechte zu erlangen. Verifizieren Sie diese mit dem Befehl `getuid` in der neu geöffneten *meterpreter*-Sitzung. Diskutieren Sie, wie das Erlangen erweiterter Rechte nach dem initialen Angriff hätte verhindert werden können.

c) Installieren Sie mit dem Befehl `run persistence -U` in der *meterpreter*-Sitzung mit Administatorrechten eine Hintertür (engl. *Backdoor*). Starten Sie anschließend mit dem Befehl `reboot` die *Windows*-VM neu und bestätigen Sie die Ausführung des *VB*-Skriptes in der *Windows*-VM. Diskutieren Sie die Sicherheitsimplikationen dieser Aktion und Vermeidungsstrategien. Erläutern Sie außerdem die langfristigen Implikationen einer Hintertür und die Notwendigkeit weiterer browserbasierter Angriffe.

03.

a) Verwenden Sie in *Metasploit* das Modul `exploit/multi/handler`, um sich unter Zuhilfenahme der zuvor installierten Hintertür auf die *Windows*-VM zu verbinden. Überprüfen Sie in der geöffneten Sitzung, ob Sie Administratorrechte besitzen und erlangen Sie – falls notwendig – ebendiese.

b) Verwenden Sie das Modul `post/windows/gather/smart_hashdump`, um (gehashte) Passwörter von der *Windows*-VM zu kopieren. Versuchen Sie, diese mit *John the Ripper* unter Verwendung des Formatparameters `--format=NT` (max. 15 Minuten) zu knacken, d.h. als Klartext zu rekonstruieren. Diskutieren Sie – unabhängig vom Erfolg dieses Angriffes – die Sicherheit der Passwörter anhand der kopierten Datei mit Passworthashes. Erläutern Sie konkret, welche Implikationen das Knacken des Passwortes eines einzigen Benutzers hätte.

c) Installieren Sie eine neue(re) Version von *Adobe Flash Player* auf der *Windows*-VM und stellen Sie sicher, dass die durchgeführen Angriffe nicht mehr funktionieren. Diskutieren Sie außerdem den Einfluss der aktualisierten Software auf die installierte Hintertür.