UNIVERSITÄT SIEGEN

Lehstuhl IT-Sicherheitsmanagment
Prof. Dr. Kesdogan

Exercise 3: Net Weaver

An dieser Stelle ist es gegebenenfalls sinnvoll sich mit Bibliotheken wie `scapy` anzufreunden.

Why do my eyes hurt?

Sende ein Ethernetpacket mit Ethernet-Ziel-Adresse "FF:00:00:00:00:00" und deinem Nick (ASCII-Codiert) als Payload. Absender-Adresse ist ziemlich beliebig, auf Spielereien wie IP und ähnliches kannst du verzichten. Ziel ist es, dass dein Nick bei uns im Serverlog angezeigt wird.

Mr. Wizard. Get me the hell out of here.

Einige Leute brauchen ein Telefon um mit der anderen Seite der Matrix zu telefonieren. Der Eine benutzt die Matrix selbst. Was dem einen ein Hindernis, ist dem anderen ein Sprungbrett.

Dein Server befindet sich hinter einem NAT, dein Client ebenso. Der Client kennt die externe Adresse des Servers, und du kannst dir eine unbenutzte IP in den Weiten des Internet suchen. (Es muss nicht `3.3.3.3` sein.) Jetzt willst du, dass die beiden miteinander kommunizieren und die Magie der Matrix soll dir dabei helfen.

Fähige Hacker können TCP/IP aus dem Stegreif, aber echte Netzer kennen mindestens noch die Kontrollschicht, namentlich ICMP. Und das ist der Knackpunkt. Orientiere dich an der Beschreibung von `http://samy.pl/pwnat`. Zum Testen werden wir zu gegebener Zeit das NAT des VPN öffnen um das testen zu ermöglichen.

Welcome to Rivendel, Mr. Anderson

Bevor ihr eure Untergebenen in die Matrix entlassen könnt, müsst ihr ihnen einen Ort bieten an dem sie Unterschlupf finden und ihre Beute abliefern können. Selbst das BKA verwendet solche Command-and-Control Server. Wir machen es uns einfach und lauschen an einem beliebigen UDP-Port.

Implementiere eine kurze Kommandoliste, die Kommandolisten je nach Absender bereithält und entsprechend sendet, wenn dieser Absender dich anfunkt.

Never send a human to do a machine's job.

Dein erster Brückenkopf. Angenommen du findest einen Einstieg auf einem Linux-System, welches deinem zum verwechseln ähnlich sieht, schreibe ein Programmstück, welches du auf diesem System ablegen kannst, und welches als Daemon im Hintergrund Kontakt zu deinem eigenen CnC-Server aufnimmt.

Implementiere die Kommandos "LS" und "SYSTEM". Bonusaufgabe ist es eine Update-Funktion für deinen Dienst zu implementieren. Jetzt sorge dafür, dass dein Brückenkopf sich nach der Installation bei deinem CnC-Server meldet.

Kontakt: `fischer@wiwi.uni-siegen.de`