Master-Projekt
Wintersemester 2016/17

Hack Grid

Komplexe
Softwaresysteme

HSB
Hochschule Bremen
City University
of Applied Sciences

MALWARE

Das Opfer Rudi Sorglos ist ein normaler PC-Endanwender. Zuerst wird Rudi in diesem Projekt mit zwei verschiedenen Formen von Malware über das Infektionsmedium E-Mail konfrontiert. Durch sein Antivirusprogramm und die Meldung „Ihr PC ist geschützt“ fühlt sich Rudi gut gesichert. Deshalb wird gezeigt, dass ein Antivirusprogramm niemals einen vollständigen Schutz garantieren kann. Zusätzlich demonstriert das Projekt, welchen Schaden eine Malware-Infektion mit sich bringen kann. Die Ergebnisse dieses Projektes sollen zur Anwendersensibilisierung eingesetzt werden.

BOTNETZE

In diesem Teilprojekt geht es darum ein Bot-Netz aufzubauen und auf seine Möglichkeiten zu untersuchen. Während der Bot aktiv ist, werden verschiedene Methoden des Ausspähens (aktive Suche nach Passwörtern, herunterladen weiterer Schadsoftware) untersucht.
Im weiteren Verlauf soll die Gewinnung von neuen Bots mittels des "Man-in-the-Tab" Prinzips erfolgen. Hierbei wird JavaScript Code bei der Verwendung eines Proxy-Servers in angeforderten Code injiziert. Die so infizierten Rechner werden Teil des oben beschriebenen Bot-Netzes.
Besonderes Ziel ist es das Bewusstsein für die Entstehung eines solchen Netzes zu fördern und Möglichkeiten zur Verhinderung aufzuzeigen.

SOCIAL ENGINEERING

Im ersten Szenario wird ein Angriff über Mittel des Social Engineerings auf eine fiktive Person Max Mustermann durchgeführt. Das Ziel ist dabei, seine Identität über Phishing Mails zu stehlen und auch über eine HID-USB Attacke anzugreifen.
Im zweiten Schritt werden einige der Angriffe bei realen Personen getestet und der Erfolg geprüft.
Das Phishing wird über eine gefälschte E-Mail umgesetzt. Die Mail imitiert mittels einer falschen Absender Adresse und authentischen Inhalts eine scheinbar wichtige Nachricht, die den Benutzer auf eine gefälschte Webseite locken soll.
Die USB-HID Attacke wird über einen präparierten USB-Stick durchgeführt. Sobald der Stick über einen USB Port an einen Rechner angeschlossen ist, soll dieser eine Konsole öffnen und dabei das System kompromittieren.

HARDWARE HACKING

In der Industrie sind Speicherprogrammierbare Steuereinheiten zu finden (SPS). Viele dieser SPSen sind über 20 Jahre alt und über Sicherheit wurde damals nicht ausführlich nachgedacht. So wollen wir in unserem Projekt eine SPS über ein Netzwerk angreifen und manipulieren. Als erstes sind die offenen Ports ausfindig zu machen und sich daraus ergebende Angriffszenarien zu evaluieren. Mögliche Szenarien wären das aufspüren von einer Backdoor und einen DDOS-Angriff.Um die SPS über einen Rechner im Netzwerk anzugreifen, wird ein Angriff mit Hilfe eines USB-Devices entwickelt. Dazu soll der "USB-Stick" wie eine Tastatur funktionieren und Befehle ausführen und über ein Programm das Verhalten der SPS verändern.

INTRUSION DETECTION

Nach dem IT-Grundschutz gilt der IDS-Einsatz als ein wichtiger Bestandteil einer Informationssicherheit-Maßnahme und auch eine Erweiterung zu einem bestehenden Firewall-System. IDS ermöglicht die Überwachung des Netzwerkverkehrs, damit Angriffe und Sicherheitsverletzungen zeitnah erkannt werden können. In diesem Projekt wird eine Open-Source IDS „SNORT“ aufgebaut. Nach der Implementierung des IDS und vom IDS benötigen Werkzeuge werden verschiedene Angriffe durchgeführt.
Als Zusammenarbeit mit anderen Projekt-Gruppen (Malware, Botnetze) wird versucht, Malware und Botnetze zu erkennen.
Ein "normales" Angriffs-Szenario (Portscann, Brute-force...) wird auch getestet.

TEILNEHMER

Julian Scheichel,
Philipp Kathmann,
Tobias Wenzig,
Marco Bronner,
Andreas Rattner,
Jelto Wodstrcil,
Yassir Dliaa,
Merle Labusch,
Eda Tasdelen,
Daniel Wiese,
Betreuer: Prof. Dr. Sethmann