7. Übung zur VL Betriebs- und Kommunikationssysteme

Tutor: Thomas Tegethoff

Bearbeiter: Etienne Jentzsch, Carola Bothe

1a)

Directory Traversal

Trickst ein schwaches Programm aus, sodass es Zugang zu einer geschützten/inneren Datei gewährt indem es den Verzeichnisbaum hoch und dann runter zur Passwort datei geht. Als Verteidigungsmaßnahme sichert/verschlüsselt man die Passwortdateien und erlaubt web servern keinen vollen Zugriff auf Dateisysteme. (VL Folie 7.29, Mitschrift)

Buffer Overflow

Bezeichnet man, wenn ein Programm Daten über die Grenzen eines Puffers auf benachbarten Speicherplatz schreibt. Dadurch kann bösartiger Code auf diesen benachbarten Speicherplatz geschrieben und später ausgeführt werden. (https://en.wikipedia.org/wiki/Buffer\_overflow)

Trapdoor/Backdoor

Ursprünglich als Tool zum debuggen und testen gedacht, erlauben Hintertüren den Zugang zu einer Datei/einem Programm ohne den üblichen Sicherheitsprozess zu durchlaufen. Die Türwird durch ein Stück Software implementiert (dazu werden im Negativfall z.B. Geräte beim Transport abgefangen) und kann vom Betriebssystem nur schwer kontrolliert werden. (VL Folie 7.35, Mitschrift)

Logic Bomb

Gehört zu den ältesten Schädlingen und ist ebenfalls Teil eines Programms. Sie 'explodiert' wie der Name sagt, wenn eine bestimmte (logisch) Bedingung erfüllt ist. Die Folgen der Explosion können veränderte oder gelöschte Daten, ein Abstürzen des Systems oder anderes sein. (VL Folie 7.36, https://de.wikipedia.org/wiki/Logikbombe)

Trojan Horse

Angeblich nützliches Programm, dass die gewünschte Funktion ausführt aber zusätzlich eine bösartige Funktion hat. Beispiel wäre eine Taschenlampe Anwendung, die nebenbei Kontaktdaten übermittelt, was man hier zumindest mit der Ablehnung von Zugriffsrechten im Zaum halten kann. (VL Folie 7.37, Mitschrift)

Virus

Software, die nach einem Auslöser andere Software modifiziert und neben dem schädlichen Code auch Code zur Selbstreplikation enthält. Viren haben heutzutage lange Inkubationszeiten, damit sie auch auf etwaigen backups vertreten sind, und die Fähigkeit zur Mutation, sodass Virenprogramme an ihre Grenzen stoßen. (VL Folie 7.40, Mitschrift)

Worm

Sind wie Zombies unabhängig vom Gastbetriebssystem und sobald sie einmal aktiviert wurden, replizieren sie sich wie Viren, wobei sie aktiv nach weiteren Verbreitungsmöglichkeiten auf andere System und Netzwerke suchen. In Gegensatz zum Virus findet die Verbreitung ohne die Infektion von fremden Dateien oder Bootsektoren statt. (VL Folie 7.45, <https://web.archive.org/web/20101124010540/>http://service1.symantec.com/SUPPORT/nav.nsf/pfdocs/1999041209131106)

Bot (aka Zombie, Drone)

Ein Programm, dass heimlich andere am internet hängende Geräte übernimmt, von denen dann die Attacke gestartet wird. Besonders im Zeitalter des Internet of things stellen sie daher eine Bedrohung und man kann die Bots selten zu ihrem Ersteller zurückverfolgen. (VL Folie 7.48, Mitschrift)

Rootkit

Programme, die auf dem System root Zugang gewähren, indem sie die Standardfunktionalität verändern. Damit wird Zugang zu allen Funktionen und Diensten des Betriebssystems gewährt und der Angreifer hat die komplette Kontrolle des Systems. (VL Folie 7.49)

b)

BIOS steht für Basic Input Output System und UEFI für Unified Extensible Firmware Interface. Bei beiden handelt es sich um read only Code, der die Schnittstelle zwischen Firmware, Computer Komponenten und dem OS bildet also beim Systemstart u.A. den Speicher prüft und Treiber lädt. Während BIOS das booten aller bootloader (Treiber) erlaubt, erlaubt UEFI aus

Sicherheitsgründen nur signifizierte. Das UEFI ist im Gegensatz zum BIOS ein eigenes kleines Betriebssystem, sodass etwa Updates direkt über das UEFI geladen und installiert werden können.Mit UEFI kann man nur 64-Bit Systeme booten und außerdem mehr primäre Partitionen einer Festplatte einrichten und größere Speichermedien verarbeiten. Wir finden UEFI besser, da es durch seine Standards für mehr Sicherheit sorgt und leichter Updates ermöglicht.

(VL Folie 7.6 & 7.8, Mitschrift, <http://praxistipps.chip.de/bios-oder-uefi-das-sind-die-unterschiede_36099)>

c) 10 gut verstandene Begriffe: rings, scheduling algorithms, Process, swapping, fragmentation, partitioning, virtual memory, hierarchical file system, priorety inheritance, preemptive

weniger gut verstandene Begriffe: I/O Buffering, Daemons, dispatcher, countermeasures,