

Integrität und Rootkits

Christoph Hermann

Sicherheit in komplexen DV-Systemen · Integrität und Rootkits Christoph Hermann

Integrität und Rootkits

- Rootkits
 - Vorstellung von Rootkits
 - Normale Rootkits
 - LKM Rootkits
 - Full Stealth Rootkits
- Gegenmaßnahmen
 - Tools
- IDS
 - NIDS, NNIDS, HIDS, ABIDS, dIDS
 - Tripwire
- Honeynet Forensic Challenge

Sicherheit in komplexen DV-Systemen · Integrität und Rootkits Christoph Hermann



Rootkits

- **Sammlung von Tools**

- Sniffer
 - Scripte die Logs säubern
 - Trojanisierte Binaries
- Zweck:
- Weitere Angriffe planen
 - Aktivitäten und Einbruchsspuren verschleiern
 - Weiteren Remote-Zugriff auf das kompromittierte System ermöglichen
 - Tarnung

– Drei verschiedene Arten von Rootkits

- „normale“ Rootkits
- Loadable Kernel Module Rootkits
- Full Stealth Rootkits (LKM auf TCP/IP Layer Ebene)



„Normale“ Rootkits

- **Tools**

– Scripte oder Programme die Log-Files säubern

- z2
- wted

=> wtmp, utmp, lastlog werden gesäubert

- Binaries die ersetzt werden
- Sniffer
- Späteren Remote-Zugriff ermöglichen





„Normale“ Rootkits

- Tools
- Binaries die ersetzt werden
 - ls, du, find
 - ps, top, pidof
 - netstat
 - killall
 - ifconfig
 - crontab
 - tcpd
 - syslogd
 - fix
- Sniffer
- Späteren Remote-Zugriff ermöglichen



„Normale“ Rootkits

- Tools
- Binaries die ersetzt werden
- Sniffer
 - PROMISC-Modus
 - Weitere Informationen ausspionieren
- Späteren Remote-Zugriff ermöglichen





„Normale“ Rootkits

- Tools
- Binaries die ersetzt werden
- Sniffer
- Späteren Remote-Zugriff ermöglichen
 - Infektion von
 - Lokalen Programmen
 - chfn, chsh, login, passwd
 - Netzwerk Daemonen
 - sshd, telnetd
 - bindshell



Generelles Vorgehen

- Scan-Vorgang
- Ausnutzen eines Exploits
- Feststellen wer eingeloggt ist (who)
- Rootkit herunterladen und installieren
 - Logs säubern / löschen
 - Binaries ersetzen / Trojaner installieren
 - Weitere Programme installieren (Eggdrops/Bouncer)





t0rnkit

- Einfach zu konfigurieren
- Installiert sich vollautomatisch
 - Deaktiviert syslogd
 - Ersetzt Programme (du, ls, etc...)
 - Installiert einen trojanisierten sshd
 - Startet einen Sniffer
 - Aktiviert telnetd, rsh, finger in inetd.conf
- Erkennung
 - Alle installierten Dateien sind 31336 Bytes groß
 - Meist in /usr/src/.puta installiert
 - Port 47017 ist nach außen geöffnet



LKM-Rootkits

- Loadable Kernel Module Rootkits
 - Laden sich als Modul in den Kernel
 - Modifizieren Systemaufrufe wie open()
 - Kernel Systemcalls werden verändert
 - sys_getdents (liest Verzeichnisse aus)
 - Modifiziert die Tabelle mit den Adressen der Systemcalls
 - Ersetzt vorhandenen Code durch eigenen
 - Verzweigt den Aufruf zu eigenem Code
- Erkennung
 - Vergleich der Systemcall Adressen mit der „System.map“





Adore

- Bekanntes LKM Rootkit
- Modifizierte Systemaufrufe:
 - sys_getdents
 - sys_write, sys_close, sys_kill, sys_fork, sys_clone, sys_sysmlink
 - sys_execve
- Versteckt Dateien, Prozesse und Services
 - Tarnt sich selbst
 - Ist nicht mittels „lsmod“ oder „cat /proc/modules“ erkennbar
- Kann beliebige Programme aufrufen
- Ist mittels „ava“ kontrollierbar
- Kann fast nicht entfernt werden



Full Stealth Rootkits

- Rootkits auf TCP-Layer Ebene
- Ziel: Bestmögliche Tarnung
- TCP/IP Stack wird modifiziert
 - Protokolle registrieren ihre Handler Routine im
 - *inet_protocol_base Pointer und im
 - *inet_protos[MAX_INET_PROTOS] Hash
 - Beim Systemstart werden dort alle Protokolle und deren Verarbeitungsroutine registriert
 - FSR verändern die normalen Handler Routinen
 - Überprüfen ankommender Pakete
 - Entpacken und ggf. ausführen des enthaltenen Befehls
- Gespoofte Pakete können verwendet werden





KIS von Optyx

- Kernel Intrusion System
 - Funktioniert sogar bei statisch kompiliertem Kernel
 - Ausgereiftestes existierendes Rootkit
 - Verändert nicht die Kernel-Systemaufrufe sondern schreibt direkt in den RAM
 - Verwendet „Kernel-memory-patching“
 - Keine Unterstützung für LKMs notwendig, nur Schreibzugriff auf Teile des RAMs (/dev/kmem)



Gegenmaßnahmen

- Wie finde ich Rootkits
- Tools zur Vorbeugung und Entdeckung
 - chkrootkit
 - checkps
 - KSTAT
 - Samhain Integritätschecker





Rootkits entdecken

- Feststellen der Kompromittierung
 - Anormales Verhalten von Befehlen
 - fehlende Parameter durch falsche Version
 - Veränderung / Anstieg des Netzwerktraffics
 - Scans von eigenen Systemen aus
 - Warez Verbreitung
 - Offene Ports
 - Unterschiede zwischen der Ausgabe von netstat und einem Portscan



chkrootkit

- Sammlung von 7 kleinen Tools
 - chkrootkit
 - ifpromisc
 - chklastlog
 - chkwtmp
 - check_wtmpx
 - chkproc
 - Strings





checkps

- Überprüft die Ausgabe von „ps“
 - Generiert eine eigene Prozessliste mittels
 - Informationen aus /proc
 - Testen aller Prozessnummern mittels kill()-Systemaufrufs
- Benachrichtigungsarten
 - syslogd
 - Log-File
 - E-Mail



KSTAT

- Kernel Security Therapy Anti-Trolls
 - Spürt LKMs auf
 - Überprüft den Speicher (/dev/kmem)
 - Vergleicht Adressen der Systemcalls mit der „System.map“
 - Lädt sich als LKM in den Kernel
 - Neue Version verlässt sich nicht mehr auf die „System.map“, muss genau wie der Kernel immer neukompiliert werden
 - Parameter „-m“ durchsucht Speicheradressen nach Kernelmodulen



Samhain Integritätschecker

- Ähnlich wie KSTAT
 - Vergleicht die Systemcall Adressen mit der „System.map“
- Kann Checksummen von Dateien überprüfen
- spürt abnormale SUIDs auf
- Läuft in einem „Stealth-Modus“
- Logging
 - Signieren der Log-Files
 - Zentrale Speicherung per MySQL/postgresQL



IDS

- Intrusion Detection Systeme
 - NIDS (Network Intrusion Detection Systems)
 - NNIDS (Network Node Intrusion Detection Systems)
 - HIDS (Host-Based Intrusion Detection Systems)
 - ABIDS (Anomaly-Based Intrusion Detection Systems)
 - dIDS (distributed Intrusion Detection Systems)
- Bsp. eines IDS: Tripwire





NIDS

- Network Intrusion Detection Systems
 - Breitband-Erkennungssystem
 - Erkennen Angriffe gegen Teilnetzwerke
 - Überwachung von nichtkritischen Systemen
 - Einsatz auf Routern zwischen Subnetzwerken oder auf Switches / Hubs, generell an Punkten an denen Subnetze aufeinander treffen



NNIDS

- Network Node Intrusion Detection Systems
 - Einsatz auf kritischen Systemen
 - Datenbank
 - Backup-Server
 - Keine Betrachtung von anderen Netzteilnehmern
 - Genaue Feststellung von Änderungen auf speziellen Hosts





HIDS

- **Host-Based Intrusion Detection Systems**
 - Keine Netzwerküberwachung
 - Kontinuierliche Überwachung von Systemdateien
 - Verschiedene Aspekte von Dateien werden überprüft
 - Vergleich mit gespeicherten Daten in einer Datenbank
 - Alarmierung des Administrators bei Veränderungen
 - Einsatzort:
 - kritische Workstations
 - Server mit extra Sicherheitsbedürfnissen



ABIDS

- **Anomaly Based Intrusion Detection Systems**
 - Relativ neue Entwicklung
 - Festlegung einer Art „normaler Aktivität“ von Netzwerktraffic
 - Abweichung von den Standardwerten werden überprüft und gemeldet
 - Wichtig zur Erkennung von Angriffen „von innen“
 - Erkennen/Überprüfen wer Zugriff auf welche Ressourcen hat und wer nicht
 - Filtern nur „abweichenden“ Traffic
 - Einsatz an Stellen (wie bei NIDS) an denen Subnetzwerke zusammentreffen (Router etc...)



dIDS

- **Distributed Intrusion Detection Systems**
 - Sammeln und aggregieren Logs von verschiedenen IDS Systemen
 - Bewerten und kategorisieren die entdeckten Angriffe
 - Zentrale Speicherung und Filterung von Log-Files
 - Erkennung von über das gesamte Netzwerk verteilten Angriffen
 - Zeigt Angriffsstrategien auf das gesamte Netzwerk auf



Tripwire

- **Zwei Versionen**
 - Opensource (HIDS)
 - Überwachung von Systemattributen (Checksummen)
 - Kommerzielle Version
 - Bietet HIDS & NIDS Fähigkeiten
 - Flexibel konfigurierbar
 - Kann bei Veränderung beliebige Befehle ausführen
 - Verschiedenste Log-Fähigkeiten
 - Ist in sechs Teile unterteilt



Tripwire

- Tripwire Manager
 - Verschiedene Benachrichtigungsmöglichkeiten
 - Sichere Verbindung (SSL) zu den Clients für den Befehls- und Datenaustausch
- Information Infrastructure Monitoring
 - Digitaler Schnappschuss des gesamten Systems
- Intrusion Detection
 - Unerlaubte Zugriffe werden protokolliert
- System-Konfigurations-Management
 - Überwachung von Systemattributen und Veränderungen
- System Lockdown
 - Überwachung von unbefugten Neuinstallationen
- Damage Assessment and Recovery
 - Kann automatisch den Schaden einschätzen und klassifizieren, und dann einen Bericht zur Schadensbehebung erstellen
 - Kann automatisch Dateien aus einem Backup wiederherstellen



HoneyNet Forensic Challenge

- Unwissenheit über Angriffe
- Wettbewerb
 - Wenige Informationen (über ein angegriffenes System)
 - Wenige Zeilen Log-Files
 - Disk-Images
 - Informationsgewinnung über den Angriff
 - Veröffentlichung zum Nutzen aller
- Spaß & Lerneffekt

