

# Hackproofing von IIS6 Web Servern

ERNW GmbH



# Agenda



- Grundprinzipien
- Lokales Härten
- IIS6 Konfiguration Best Practices
- ASP.NET
- Logging und Log-Analyse
- Sichere Remote Administration



# Grundprinzipien



- Segregation of Duties
- Minimal Machine
- Patch-Level
- Least Privilege
- Defense in Depth
- Secure the Weakest Link
- Strong Authentication



# Anforderungen an einen typischen Web Server



- HTTP Dienste
- Datenbank-Zugriff
- Remote Verwaltung
- Datei-Transfer



# Lokales Härten



- Verringern der Angriffsfläche
- Abschalten von nicht benutzten Features
  - Dienste
  - Protokolle
  - Sub Systeme
  
- Port-Filterung
- Setzen von ACLs
- Robustes Logging



# Lokales Härten



- Ein standard Windows Server 2003 (Anwendungs-Server Rolle) hat
  - 3 Protokoll Bindungen
  - 7 geöffnete Ports
  - 20 laufende Prozesse
  - 37 laufende Dienste



# Was kann man abschalten?



- Netzwerk-Protokolle
  - Microsoft Netzwerk Client
  - Datei- und Drucker-Freigabe
  - NetBIOS über TCP/IP (CIFS)



# Was kann man abschalten?



- Automatisch startende Dienste
  - Computer Browser, DHCP Client, Distributed File System Distributed Link Tracking Client, Distributed Transaction Coordinator, Error Reporting Service, Help and Support, Print Spooler, Remote Registry, Secondary Logon, Server, TCP/IP NetBIOS Helper, Wireless Configuration, Workstation



# Was kann man abschalten?



- Manuelle Dienste
  - Application Management, File Replication, Portable Media Serial Number Service, Remote Access Auto Connection Manager, Remote Access Connection Manager, Remote Desktop Help Session Manager, Resultant Set of Policy Provider, Smart Card, Special Administration Console Helper, Telephony, Upload Manager, Windows Installer, WinHTTP Web Proxy Auto-Discovery Service



# Was kann man nicht abschalten?



- Windows lässt nicht die Deaktivierung von RPC zu (TCP/135 und hohe Ports)
- Müssen immer von einer Firewall geblockt werden
- Zusätzlich lokale Paket-Filterung dringend empfohlen



# Lokale Paket-Filter



- Internet Connection Firewall
  - Stateful Inspection
  - Regelt nur eingehenden Verkehr
  
- IPSEC Policies
  - Regelt ein- und ausgehende Verkehr
  - Quell/Ziel IP-Adressen und Port-Limitierung möglich
  
- Kombination aus beidem ist sehr mächtig



# Paket-Filter Vorgehensweise



- Zuerst über ICF die generell über das Netzwerk angebotenen Dienste freigeben
  - HTTP und HTTPS (TCP/80 und TCP/443)
  - Terminal Services (TCP/3389)
  
- Danach mit IPSEC Policies diese Regeln verfeinern



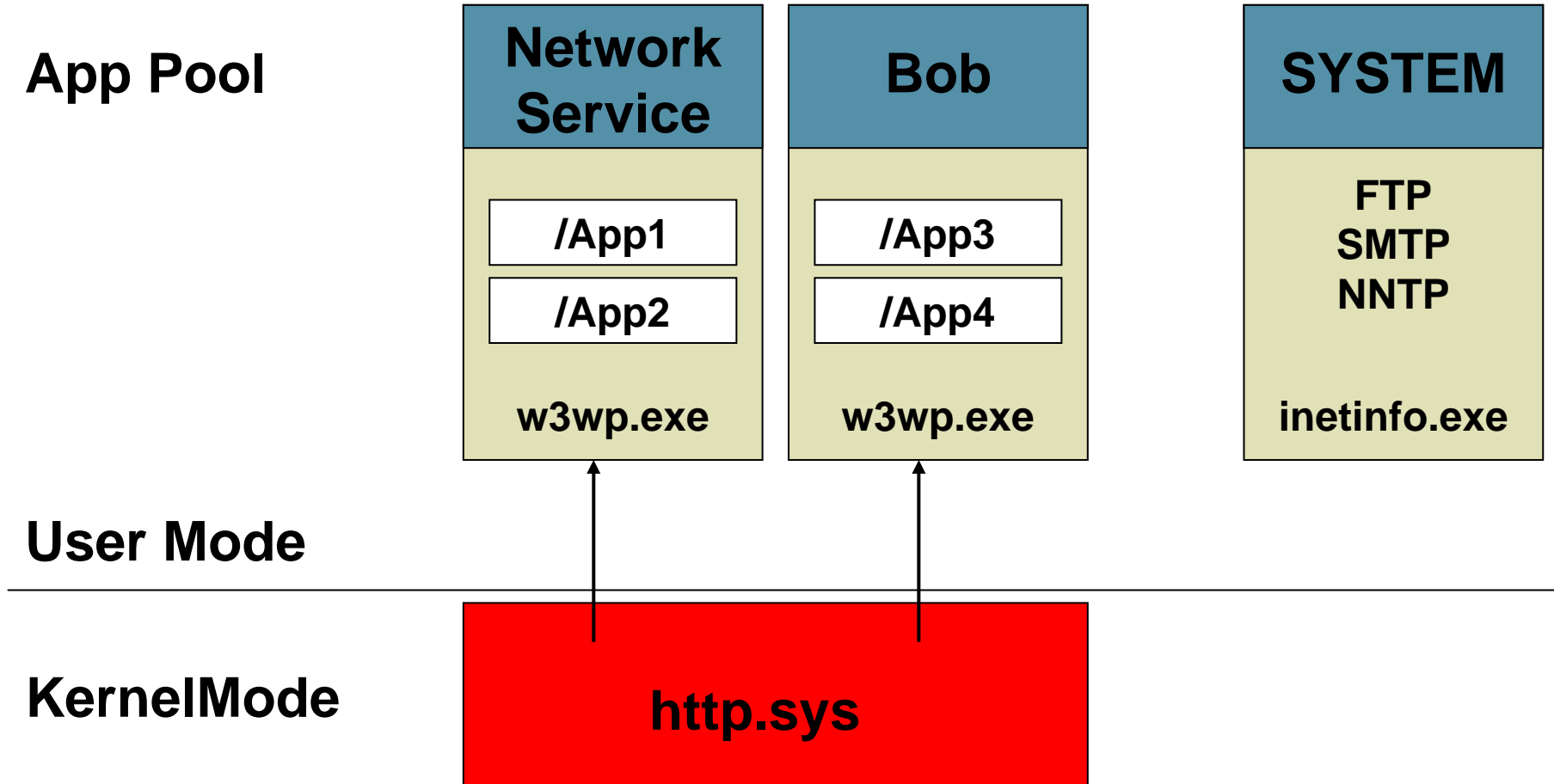
# IIS6 Konfiguration



- IIS6 Architektur
- Web Service Extensions
- AppPools
- IIS6 vs URLScan
- ACLs
  
- Shared Hosting Überlegungen



# IIS6 Architektur



# IIS6 Architektur



- Requests werden von http.sys normalisiert und validiert
  - HKLM\System\CurrentControlSet\Services\HTTP\Parameters
  
  - AllowRestrictedChars
  - MaxFieldLength
  - MaxRequestBytes
  
- Abgewiesene Requests werden in httperr.log gespeichert



# URLScan



- Kann noch granularer in Requests eingreifen
  - Erlaubte und verbotene Verbs
  - Erlaubte und verbotene Endungen
  - Manipulation des Server Headers
  - Filtern von speziellen Zeichenfolgen



# ASP.NET



- Natürlich bringt die beste Server-Konfiguration nichts, wenn die Web Anwendungen buggy sind
  - SQL Injection
  - Cross Site Scripting
  - Canonicalization Errors
  - Directory Traversal



# Top ASP.NET Probleme

- ValidateRequest und <%00script>
  - Authorization von nicht-.NET Dateien
  - ASP.NET Authorization Vulnerability
  - Tracing und Zugriff auf .axd Dateien
  - Cookieless Sessions
  - ViewState MAC Schutz
- 
- Full Trust Anwendungen



# Full Trust ASP.NET



- Full Trust ist der Standard
  
- Dies ermöglicht es Anwendungen
  - Beliebigen Unmanaged Code aufzurufen
  - Starten von neuen Prozessen
  - Lesen von Einträgen in der IIS Metabase
  - Lesen und Impersonieren von Windows Tokens von anderen Web Anwendungen
  - Lesen und Ausführen des Codes von anderen Web Anwendungen



# Robustes Logging



- Logs sollten zentral abgelegt werden
- Erleichtert die etwaige Analyse
- System-Zeit sollte von einer NTP Quelle stammen
  
- Windows Event Log Pfad ändern
  - HKLM\System\CurrentControlSet\Services\EventLog



# Log-Analyse mit LogParser



- Eingabe-Formate
  - IIS Logs
  - Windows Event Logs
  - URLSCAN Logs
  - IIS6 HTTPERR Logs
  - CSV Dateien
- Ausgabe-Formate
  - Text
  - XML
  - SQL
  - Grafisch



# LogParser und das Windows Event Log



- Fehlgeschlagene Anmelde-Versuche
  - logparser "select distinct SID from Security where EventID IN (529; 530; 531; 532; 533; 534; 535; 537; 539)"
  
- Auflösen von SIDs
  - logparser "select distinct SID, RESOLVE\_SID(SID) as Username from Security where EventID IN (529; 530; 531; 532; 533; 534; 535; 537; 539)"



# LogParser und das Windows Event Log



- Die häufigsten Nachrichten im Event Log, sortiert nach Schweregrad
  - logparser "select distinct EventID, EventTypeName, Message, Count(\*) as Entries from System group by EventID, Message, EventTypeName order by EventTypeName, Entries DESC" -i:EVT -o:DATAGRID



# LogParser und IIS



- Top 10 der abgewiesenen Requests
  - logparser "SELECT TOP 10 src-ip, s-reason, Count(\*) as Hits FROM HTTPERR group by src-ip, s-reason order by Hits DESC"
- Verschiedene User Agents
  - logparser "select distinct cs(User-Agent) from ex\*.log order by cs(User-Agent)"
- User-Agent, dazugehörige IPs und #Hits
  - logparser "SELECT distinct c-ip AS Client, cs(User-Agent), COUNT(\*) as Hits FROM ex\*.log group by cs(User-Agent), Client order by cs(User-Agent), Hits DESC"



# LogParser und IIS



- Ungewöhnlich viele Hits auf die gleiche Seite von der gleichen IP Adresse
  - logparser "SELECT DISTINCT date, cs-uri-stem, c-ip, Count(\*) AS Hits FROM ex\*.log GROUP BY date, c-ip, cs-uri-stem HAVING Hits>50 ORDER BY Hits Desc"
- Status-Codes pro Seite
  - logparser "SELECT cs-uri-stem, sc-status, Count(\*) AS Total FROM ex\*.log WHERE TO\_LOWERCASE(cs-uri-stem) LIKE '%.aspx%' GROUP BY cs-uri-stem, sc-status ORDER BY cs-uri-stem, sc-status" -rtp:-1



# Remote Administration



- Terminal Services
  - In Windows enthalten
  - Grafisches Terminal / Datei-Transfer
  - Schlüssel-basierte Authentifizierung nur in Domänen Umgebungen
- SSH
  - Standard / Datei-Transfer mit SCP
  - Text-basiert und damit geringe Bandbreite
  - Starke Verschlüsselung
  - Schlüssel und (Einmal-) Passwort Authentifizierung
  - Erlaubt das Tunneln beliebiger TCP Verbindungen



# Fragen?



- Web Seite
  - <http://www.ernw.de>
  
- Blog
  - <http://www.leastprivilege.com>



# Links



- Securing Windows Server for the Internet
  - <http://www.oreilly.com/catalog/securwinserv/index.html>
- Windows 2003 Services Reference
  - <http://www.microsoft.com/downloads/details.aspx?FamilyID=b38a0682-2997-4678-9d9e-a07cc66a3bba&displaylang=en>
- Managing System Services
  - <http://www.microsoft.com/downloads/details.aspx?FamilyID=a70b06cb-b0f2-4800-997b-2a27ce8fcdc2&DisplayLang=en>



# Links



- NMAP
  - <http://www.insecure.org/nmap>
- Open Web Application Security Project
  - <http://www.owasp.org/software/dotnet.html>
- LogParser
  - <http://www.microsoft.com/downloads/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&DisplayLang=en>
  - <http://www.leastprivilege.com/default.aspx?date=2004-06-26>



# Links



- IIS6 makes URLScan almost obsolete
  - <http://www.winnetmag.com/Article/ArticleID/39979/39979.html>
- IIS6 Operations Guide
  - <http://www.microsoft.com/resources/documentation/iis/6/all/proddocs/en-us/default.msp>
- Full Trust ASP.NET
  - <http://www.leastprivilege.com/default.aspx?date=2004-09-28>
- Metabase ACLs
  - <http://support.microsoft.com/default.aspx?scid=kb;EN-US;267904>



# Links



- IIS6 Security
  - <http://www.securityfocus.com/infocus/1765>
- HTTP.SYS Konfiguration
  - <http://support.microsoft.com/default.aspx?scid=kb;en-us;820129>
- Ports used by Microsoft Servers
  - <http://www.leastprivilege.com/default.aspx?date=2004-06-18>
- Tunnel von TCP über SSH
  - <http://www.leastprivilege.com/default.aspx?date=2004-08-04>

