Zusammenfassung M184

Netzwerksicherheit realisieren

Emanuel Duss

2010-08-06

Informationen

Autor	Emanuel Duss
Erstellt am	2009-10-15
Bearbeitet am	2010-08-06
Erstellt mit	OpenOffice.org auf Ubuntu Linux

Lizenz

Bearbeitungsprotokoll

Datum	Version	Änderung
2009-11-10	0.1	Erstellt
2010-05-15	1	Final

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 IT-Sicherheit

1.1 Abstrakte IT-Güter / Bereiche der IT-Sicherheit

Kat.	IT-Gut	Massnahme	Bedrohung	Beispiele
Daten	Vertraulichkeit der Daten Nur berechtigte können Daten lesen.	VPN Datenträgerverschlüsselung Zugriffssteuerung (Sicherheitsgruppen und DACLs)	Sniffen Diebstahl von Datenträgern Identitätsklau Falsche Zugriffslisten	IPSec WLAN WPA2-PSK WLAN IEEE802.1X PayPal PGP / GPG TrueCrypt Host-Firewall
Daten	Integrität der Daten Daten können nicht unbemerkt verändert werden.	VPN Hashbildung auf Dateien Redundante Datenträger (RAID) Backup (und regelmässige Restore-Tests)	Man in the Middle Angriffe Verlust von Backup Verlust der Restore-Möglichkeit	IPSec WPA2-PSK WLAN IEEE802.1X PayPal PGP / GPG
System	Verfügbarkeit der Systeme Unberechtigte können die Verfügbarkeit nicht beeinflussen.	Hardening gegen SYN-Flood Angriffe Netzwerk IDS zur Auswertung von Angriffen Redundante Systeme Servervirtualisierung Passwortrichtlinien Anti-Malware-Software Betriebssystem und Anwendungen updaten	SYN-Flood Angriffe (D)DoS Technische Systemausfälle Naturereignisse Identitätsklau von Admin-Konten	IPSec WPA2-PSK WLAN IEEE802.1X PayPal PGP / GPG RAID
System	Schutz vor Missbrauch Nur berechtigte dürfen Systeme benutzen.	Netzwerk- und/oder Host-IDS Logs auswerten Dienste richtig konfigurieren Anti-Malware-Software Betriebssystem und Anwendungen updaten	Schlecht geschützte Systeme Schlecht geschützte Dienste (SMTP-Relaying nach Identitätsklau) Malware	IPSec WPA2-PSK WLAN IEEE802.1X PayPal PGP / GPG
Benutzer	Digitale Integrität Niemand kann sich als andere Person ausgeben.	Passwortrichtlinien Sicheres Authentifizierungsverfahren (IEEE 802.1X, CHAP, ...) Zweikomponenten-Authentifizierung: „etwas haben“ und „etwas wissen“ = SmartCard mit private Key + PIN)	Identitätsklau	Kerberos WLAN IEEE802.1X PayPal PGP / GPG
Benutzer	Nichabstreitbarkeit der Urheberschaft Die Urheberschaft steht zweifelsfrei und dauerhaft fest.	Digitale Signatur ermöglicht Nachweis der Urheberschaft und der Integrität (keine nachträgliche Änderungen ohne Wissen des Subscribers möglich).	Verfassen von anonymen Dokumenten	PayPal PGP / GPG

Keine Sicherheit: DNS-Abfrage auf dem Nameserver ns1.bluewin.ch; Anmeldung auf einem AD-Client.

1.2 IT-Security-Management-Prozess

Das Ziel ist die Ausarbeitung, die Implementierung und das Testen von Sicherheitsrichtlinien für Layer 1 – 8.

Schritt	Stichwort	Kurze Erklärung
1	IT-Asset erfassen	Inventarliste mit detaillierter Auflistung der Teilkomponenten
2	Bedrohung	Mögliche Bedrohungen feststellen
3	Risiko	Wie ist das Risiko der Bedrohungen Relative Bewertung: *Wahrscheinlichkeit * Schadensausmass* • Primär: Ausmass des Schadens, wenn ein Ereignis eingetroffen ist • Sekundär: Wahrscheinlichkeit für Schadensereignis
4	Sicherheitsrichtlinien	Ausarbeiten von Sicherheitsrichtlinien: • Verhalten / evtl. Schulungen • Checklisten für die Implementierung
5	Testen	1. Penetrationstests: Tests von Aussen (ohne Vorwissen) 2. Security-Audit: Tests von Innen (mit Vorwissen) 3. Auswertung der Logfiles (Firewall, Ressourcenüberwachung, IDS, SNMP-Systeme)

Tabelle 1: IT-Security-Management-Prozess

1.3 Beispiele

Asset-ID	Bezeichnung	Beschreibung	Bedrohung	Risiko
1	**FTP-Server**	**99.999% Verfügbarkeit**		
1.1	Server Hardware	HP DL120 1 CPU 1 GB RAM 120 GB RAID 5 1 NIC 100 Mbps	Manipulation am Server Klau des Datenträgers Ausfall von wichtigen Systemen	3*8=24
1.2	Betriebssystem	Debian Lenny 5.0	Verschiedene, künftige bekannt gewordene Vulnerabilities	6*8=48
1.3	FTP-Server	proftpd	TCP-Syn-Flood Angriff gegen Port 21 (FTP-Control-Port)	7*3=21
1.4	Host Firewall	Iptables		
1.5	Remote Verwaltung	SSH	Verschaffen eines Zugangs durch systematische Passwort-Hackerangriffe	6*10=60
1.6	Datenbank	MySQL 5.0		
2	**HTTPS-Server**			
2.1	Server Hardware	HP DL120; 1 GB RAM	Manipulation am Server Klau der Harddisk Serverausfall	1 * 9

2.2	Betriebssystem	Windows 2008 R2	Diverse Vulnerabilities & Exploits	5 * 8
2.3	Webserver (mit SSL)	Microsoft IIS	Diverse Vulnerabilities & Exploits Directory Traversal-Attacken Ungültiges / Flasches Zertifikat	7 * 5
2.4	Datenbank	MS SQL Server 2008	Diverse Vulnerabilities & Exploits Absetzen von Befehlen über MS SQL	5 * 9
2.5	Groupware-SW	Sharepoint-Server	Diverse Vulnerabilities & Exploits Cross-Side-Scripting SQL-Injection	4 * 7
3	**Notebook**			
3.1	Notebook Hardware	Lenovo ThinkPad T400s	Kann gestohlen werden.	
3.2	Betriebssystem	Windows 7 Professional	Aktuelle Sicherheitslücken und Exploits.	
3.3	Filesystem	256 GB ssD HDD	Beim Diebstahl könnten Daten gestohlen werden	
4	**WLAN**	**802.11g-Karte**	**Beim Einwählen in Fremde Netze kann der Notebook angegriffen werden**	
5	**VPN**	**IPSec VPN**		
6	**USB-Stick**	**Emtec 8 GB**	**Verlust oder Diebstahl offenbart**	
7	**IIS mit DB**	**Basierter**	**Webapplikation**	
7.1	Server-Hardware	HP DL120; 1 GB RAM	Technisch bedingte Ausfälle	
7.2	OS	W2k3 R2	(D)DoS-Angriff Diverse Vulnerabilities & Exploits Übernahme von Adminrechten und Berechtigungen durch Hacker	7 * 7 = 49
7.3	Adminkonto	Digitale Identität des Administrators	Identitätsklau durch Passwort-Hacking	5 * 9 = 45
7.4	Webserver	IIS 6	Diverse vulnerabilities & Exploits	
7.5	Framework	ASP.NET-Framework	Diverse vulnerabilities & Exploits	
7.6	Anwendung	ASP.NET-Anwendung	Sicherheitsmängel in der Webanwendung (SQL-Injection, Css)	
8	**Firewall**			
8.1	Firewall SW	Cisco IOS	Fehlkonfiguration Diverse Vulnerabilities & Exploits	5 * 9 = 45
8.2	Zugang	Administrativer zugang via SSH	Schwaches Passwort vom WAN her erreichbar	5 * 5 = 25

Tabelle 2: Beispiel Master Table

1.3.1 Initiale Massnahmen

- OS nur von sicheren Quellen und in sicherer Umgebungen installieren
- Rechnungszentrum Zutrittsbeschränkung mit SmartCards
- Windows-Updates durchführen
- Redundante Systemteile (RAID, USV)
- Vulnerability-Scanner-Analyse
- TCP/IP-Stack gegen SYN-Flood schützen
- Berechtigungen setzen
- Berechtigungen in Datenbanken richtig setzen
- Sicheres Zertifikat verwenden (Ohne MD5 im Zertifikat)
- SQL-Server sicher installieren und konfigurieren
- Berechtigungen auf Relationen setzen!
- Updates installieren; Eigenen Module sauber programmieren, damit keine SQL-Injections oder Cross-Side-Scripting möglich ist.
- User schulen, damit sie vorsichtig mit dem Gerät umgehen
- Spezielle Gruppenrichtlinien
- Festplatte verschlüsseln
- USB-Stick verschlüsseln
- WLAN-Authentifizierung mit 802.1X-Standard (WPA-Enterprise)
- Windows-Passwort sicher wählen
- Updates installieren
- Anti-Malware-Software
- Hostfirewall
- BIOS-Passwort
- Preboot-Authentication (PBA)
- Name vom Administratorkonto ändern
- Passwort vom Administratorkonto sicher auswählen
- Passwortrichtlinien
  - Chronik
  - Regelmässiges wechseln
  - Komplexität
- Bildschirmschonerpasswort verwenden
- Nur die nötigen Rechte vergeben
- NTFS-Filesystem
- Updates
- Firewall aktivieren
- Virenscanner
- Verschlüsselung
- Bios-PWD
- Bitlocker mit TPM

1.3.2 Permanent

- Überprüfen der Security-Massnahmen
- Wer hat wann den Serverraum betreten
- Mitarbeiter schulen und sensibilisieren
- Logfiles auswerten (Z.B. Sind SQL-Injections an der URL erkennbar)
- Fehlerhafte Logins überprüfen

- Sich über neue Updates, Vulnerabilities und Exploits informieren (CERT, Microsoft-Publikationen)
- Applikationen und OS updaten
- Penetrationstest und Security-Audit für das eingesetzte Produkt
- Anwendung des Microsof Security Base Line Analyzers
- Firewallkonfiguration OK?
- Firewallregeln richtig?
- Firewall mit Tools testen.
- Security-News lesen
- Herstellerinformationen abonnieren
- Firmware-Updates installieren

1.4 Einen Computer / Server angreifen

- Arbeitsplatz nach Hinweisen auf Passwort durchsuchen (Doku, PostIt)
- Social Engineering (Mit Personen sprechen...)
- Footprinting
- Manueller Bruteforce (admin, just4us, only4us, hesunda20_, usw...)
- Bootreihenfolge überprüfen
- Wenn möglich von CD booten
  - OphCrack booten und Passwort 'knacken'
  - Trinity Linux Windows PWD zurücksetzen
  - Mit Linux-Live-CD booten und Daten auslesen (wenn nicht verschlüselt)
- Von USB-Stick statt von CD booten
- Exploit ausnutzen (Milw0rm.com)
  - Local-Exploit: Hilfsmanager um cmd.exe austauschen
  - Remote-Expoit: SMB-Lücke (z.B. Windows Vista)
- Bios-Passwort resetten
- HD ausbauen, mit Adapter an einen anderen PC anhängen
- Wenn verschlüsselt: Wie verschlüsselt
  - XOR: *(-1) ist schlecht
  - Sicherheitslücke in Verschlüsselung
  - Schlechte implementierung?

    - Sonst: keine Chance
- Unverschlüsseltes Backup?
- Daten einer öffentlichen Freigabe sichtbar?

1.5 Penetrationstests

1.5.1 Klassifikationen eines Penetrationstests?

- Informationsbasis
- Aggressivität
- Umfang
- Vorgehensweise
- Technik
- Ausgangspunkt

Phase	Bezeichnung/ Zielsetzung	Tools
1	Anforderungen Bekanntgabe der zu überprüfenden Adressen und Prozesse	
2	Footprinting Informationsbeschaffung (Information-Gathering) mittels Systemtools	Publikationen der Firma (z.B. Homepage) Social Engineering DNS-Einträge zur Firmen-Domäne
3	Ist-Aufnahme Mit Scans sollen benutzte IP-Adressen, Betriebssysteme von Hosts und Netzwerkgeräten, Produkte und Versionen von wichtigen Diensten in Erfahrung gebracht werden	Netzwerkscanner (nmap)
4	Analyse Einsatz von Schachstellen-Analysatoren (Vulnerabilty Scanner); Einsatz von Passwort-Cracker gegen Netzwerkgeräte und Serversysteme	Vulnerability Scanner (Nessus); Spezielle Vulnerability-Toolsammlungen (BOss vom BSI)
5	Report Berichterstattung über die Ergebnisse des Penetrationstests Massnahmen zur Ausmerzung der erkannten Schwachstellen vorschlagen	

Tabelle 3: Penetrationstests

2 Angriffsformen

2.1 Sicherheitsqualität

2.1.1 Sicherheitsqualität der Protokolle

Layer	Keine Sicherheitsfunktionen	Sicherheitsfunktionen
Layer 8	Mensch	Traue-Niemandem-Mensch
Layer 7	HTTP, FTP, Telnet, pop3, smtp, dhcp, SNMPv1/2, DNS	HTTPS, SFTP, SSH, CIFS (mit PKI), EFS, DNssec, SNMPv3
Layer 6		
Layer 5	PPP-Authentifizierungsprotokoll PAP (LAN-Manager Passwort Hashes in Windows-Systemen)	SSL, Kerberos v5, EAP bei IEEE 802.1x, SSL, CHAP
Layer 4	UDP, TCP (mit Session-ID ein gewissen Schutz gegen Hijacking)	EAP
Layer 3	IP, ICMP, ARP	IPSec
Layer 2	Ethernet, TokenRing, WLAN IEEE802.11	WPA, WPA2, Macfilter, VLAN IEEE 802.1Q
Layer 1	Kabel am Boden	Kabel in Chuck Norris Bart eingeflechten

Tabelle 4: Sicherheitsfunktionen

2.1.2 Sicherheitsqualität von Software

Buffer Overflow	Ein Programm wird geschrieben mit einer Eingabe die länger als gedacht ist. So werden andere Speicherbereiche überschrieben. Somit wird die Rücksprung-adresse auf dem Stack überschrieben und z.B. eine Root-Shell geöffnet.
Vulnerabilities	Verwundbarkeit / Schwachstelle der Software, die für Angriff benutzt werden kann; werden auf CERT-Servern veröffentlicht (http://www.cert.org)
Exploit	Konkreter Angriff, aufgrund bekannt gewordenen Schwachstelle
Directory-Tra-versal	Durch manipulieren von Pfadangaben auf beliebige Verzeichnisse des Filesystems zugreifen.
CERT	Computer Emergency Response Team / Entdeckt Vulnerabilities in offen gelegtem Code; Registrieren von konkreten Exploits; Publikation von Warnmeldungen und Bekanntmachen von Gegenmassnahmen
Bot-Netz	Virtuelles Netzwerk, das aus kompromitierten Systemen besteht.

Tabelle 5: Sicherheitsqualität von Software

2.2 Bedrohung durch Malware

Quelle: http://de.wikipedia.org/wiki/Malware

Malware	Eine Malware (Schadprogramm) ist eine unerwünschte Software, die unerwünschte oder schädliche Funktionen ausführt.
Virus	Kopiert sich in Programme, Dokumente, Datenträger weiter.
Wurm	Verbreitet sich über das Internet und versucht in andere Computer einzudringen.
Trojaner	Ein (manchmal nützliches) Programm, welches im Hintergrund noch ein weiteres Programm ausführt (z.B. Backdoor, Keylogger). Verbreitet sich nicht von alleine und wird durch den Benutzer installiert.
Backdoor	Öffnet einen Zugang („Hintertür“) zu einem Dritten. Wird durch Viren, Trojaner oder Würmer eingeschleust. Damit können DDOS-Attacken gemacht werden oder Spam verschickt werden.
Spyware	Sammeln Benutzerinformationen und leiten diese an Dritte weiter.
Adware	Zeigt ungewünschte Inhalte dem Benutzer an (z.B. Werbung)
Scareware	Verunsichert den Benutzer damit er z.B. Für ein unerwünschtes Produkt bezahlt (falsche Virenmeldung).
Dialer	Eigendlich keine Malware; Führen einwahlen auf teure Nummern durch.
Rootkits	Wird auf einem angegriffenen System installiert um künftige Logins, Prozesse und Dateien zu verdecken.

Tabelle 6: Malware Arten

2.3 Angriffsformen

2.3.1 Auf dem TCP/IP-Stack

Spoofing (Verschleierung)	Vortäuschen einer anderen Identität: Fälschen von MAC-Adressen, IP-Adressen, FQDN, E-Mail-Nachrichten, Replayangriffe mit Authentifizierungspaketen
DoS	Durch Überlastung einer Netzwerkkomponente deren Service gezielt arbeitsunfähig machen.
DDoS	Wenn der Angrif koordiniert von mehreren, verteilten Systemen erfolgt, spricht man von einem DDoS
Portscanning	Scannen, welcher Port auf einem System offen ist
Man-in-the-Middle	Sich dazwischenhängen und die Verbindung übernehmen
PingSweep	Ping-Suchlauf auf laufende Hosts
Banner-Grabbing	Schauen, welcher Webserver dahinter steckt z.B. über Abfrage des HTTP-Headers
Hijacking	Ein System übernehmen

Tabelle 7: Angriffsformen

2.3.2 Layer 8 – der Mensch

Social Engineering	Den Mensch beeinflussen, damit man an Daten oder Dienste kommt.
Phishing	Eine täuschen echte Seite wird per Mail versendet mit der Aufforderung seine Daten einzugeben.

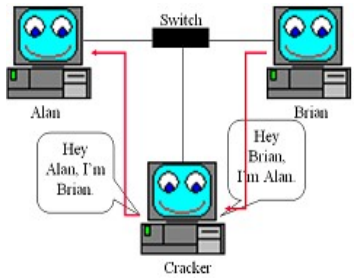
2.3.3 Beispiele

IP-Spoofing

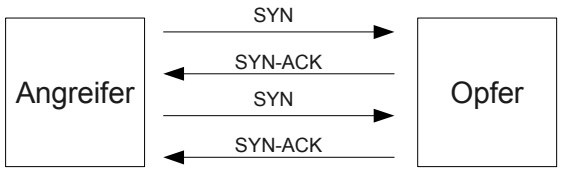
Definition	Versenden von falschen IP-Paketen mit gefälschter Absender-IP-Adresse. Die Identität wird dadurch verschleiert. http://de.wikipedia.org/wiki/IP-Spoofing
Tool	Ettercap (http://ettercap.sourceforge.net/), netcat
Zweck	Identität von einem Angriff verbergen
Massnahme	Paketfilter; TCP-Segmentnummerierung hilft ein wenig

ARP-Spoofing / ARP-Request-Poisoning

Definition	Versenden von falschen ARP-Paketen mit gefälschter Absender-MACAdresse. http://de.wikipedia.org/wiki/ARP-Spoofing

Prinzip	 Quelle: http://www.irongeek.com/images/mim.png
Tool	Arpspoof (aus dem Dsniff-Paket), Ettercap (http://ettercap.sourceforge.net/)
Zweck	Man-in-the-Middle; Mitlesen von Datenverkehr
Massnahme	Static ARP, Nach „gültigen“ Anfragen und Antworten suchen mit ARPWatch Mit VLANs die MAC-Broadcastdomänen einschränken.

SYN-Flood ((D)DOS)

Definition	Bei der SYN-Flood-Attacke wird die ACK-Nachricht nicht gesendet. Das Opfer wartet auf die Antwort vom Angreifer. Die Verbindung ist noch halb offen, also noch nicht ganz abgeschlossen. Der Speicherbereich im Netzwerkstack bleibt aber weiterhin reserviert. Wenn man sehr viele Verbindungsanfragen stellt, ohne diese zu bestätigen überläuft schlussendlich der Speicher vom Opfer.
Prinzip	
Tool	Ettercap (http://ettercap.sourceforge.net/), netcat
Zweck	Bei erfolgreicher Attacke sind Dienste oder ganze Computer in einem Netzwerk nicht mehr erreichbar. DOS-Attacken haben das Ziel, das Zielsystem zu überlasten.
Massnahme	Als Gegenmassnahme können SYN-Cookies oder Firewalls dienen.

3 Firewall

Eine Firewalll stellt ein trennendes Glied zwischen mindestens zwei Netzen dar. Sie unterbindet den ungehinderten Austausch von Informationen zwischen den Rechnern der beiden Netze. Es muss darauf geachtet werden, dass keine zweite Verbindung zwischen den beiden Netzen existiert, die eine Umgehung der Firewall möglich machen.

Es gibt verschiedenen Techniken, eine Firewall zu implementieren. Die am weitesten verbreiteten Techniken sind

- Filter auf OSI-Layer 3 und 4 (Paketfilter-Firewalls)
- Filter für die Anwendungsprotokolle (Proxys) (Application-Firewalls)

3.1 Vor was schützt eine Firewall?

Schützt vor	Schützt nicht vor
Firewalls können den Netzwerkverkehr auf gewissen Ports blockieren, können festlegen in welche Richtungen was für Verbindungen aufgebaut werden dürfen (z.B. vom internen LAN darf man in auf das Internet zugreifen, aber nicht umgekehrt). Intelligentere Firewalls können auch SYN-Flood oder Spoofingattacken erkennen.	Firewalls könne allerdings nicht vor Viren oder ähnlichen Schadprogrammen schützen. Auch ist eine Firewall noch kein ausreichender Schutz, dass überhaupt keine unerlaubten Verbindungen aufgebaut werden können. So kann, zum Beispiel über Port 80, auch ein Tunnel (mittels VPN oder SSH) gemacht werden, und eine Firewall so umgangen werden. Vor SPAM schützen sie meistens nicht. Schütz vor internen Angriffen nicht. Schütz nicht vor Wireless LAN.

3.2 Paketfilterung

3.2.1 Informationen zu Paketfilter-Firewalls

- Arbeitet auf Layer 3 und 4
- Das gesamte Netzwerk kann an einem zentralen Ort gegen aussen geschützt werden.
- Die Clients benötigen keine Anpassung und die User keine Schulung (=Transparent)
- Paketfilterungen ist in vielen Hard- und Software erhältlich.
- Auch Betriebssysteme verfügen über eigene Host-Firewalls (Personal-Firewalls).

3.2.2 Anfnorderungen

- Filterregeln pro Interface
- Filterregeln getrennt für ein- und ausgehende Pakete
- Filterregeln Meldungsspezifisch für ICMP
- Filterregeln getrennt für Quell- und Zieladresse / Netzwerke

- Reihenfolge der Abarbeitung vom Administrator festlegbar
- TCP-Verbindungsaufbau muss erkennbar sein: Stateful-Firewall
- Source Routing[1] standardmässig ignorieren
- Logs können an interne Hosts gesendet werden

3.2.3 Arten der Paketfilterung

Statische Paketfilterung

- Zustandslos: Es wird keine Zustandstabelle (Verbindungstabelle) erstellt.
- Erkennt kein Zusammenhang zwischen den verschiedenen zusammengehörende Datagrammen
- Daher weiss die Firewall nicht, welches Paket eine Antwort zu einer bestehenden Verbindung (die mittels 3-Way-Handshake hergestellt wurde) dazugehört.
- Jedes Paket wird die Filterregel durchlaufen.

Stateful Paketfilterung

- Zustandsorientiert: Es wird eine Zustandstabelle (Verbindungstabelle) erstellt.
- Nur das erste Paket einer neuen (!) Verbindung durchläuft die Filterregeln. Weitere Pakete einer zugelassenen Verbindung (auch Antworten in die Gegenrichtung) werden automatisch zugelassen.
- Die Firewall ändert Regeln während der Laufzeit
- Bei TCP ist das sehr einfach, da dort der 3-Way-Handshake stattfindet und die Antworten TCP-ETABLISHED sind.
- Bei UDP ist es schwieriger, da dort anhand der IP-Adressen, Port-Nr, Zeitstempel eine Zustandstabelle gemacht werden muss und keine Flags auf eine bestehende Verbindung hinweisen.

Stateful Inspection Paketfilterung

- Standardmässig stellt ein Client von einem unprivilegierten Port eine Verbindung zum Server auf einen privilegierten Port her.
- Bei FTP läuft das nicht so. Der Client eröffnet von einem unprivilegierten Port eine Verbindung zu Port 21 (FTP Control Port) auf dem Server. Will der Server Daten an den Client übertragen, stellt er vom privilegierten Port 20 eine Verbindung zu einem unprivilegierten Port beim Client her (das nennt man aktives FTP, da der Server die aktive Rolle einnimmt).
- Eine Stateful Inspection Firewall schaut in die Pakete rein (auch Layer 7 Eigenschaften) und analysiert, welche Ports genutzt werden und ändert anhand diesen Informationen die Firewall-Regeln.

1 Source Routing: Der Sender kann die vollständige Wegsequenz zum Zielhost bestimmen.

- Eine Firewall ohne Stateful Inspection müsste alle unprivilegierten Ports zur Clientseite öffnen, was ein fatales Sicherheitsrisiko wäre.

3.2.4 Funktionsweise

Eine Paketfirewall kann in IP-Pakete rein schauen und anhand der Optionen entscheiden, was mit dem Paket geschehen soll. Folgende Optionen sind Nützlich:

IP-Header

IHL	IHL muss <= 5x32 Bit sein, weil sonst der Option Teil nicht leer ist. Könnte Router-IP-Adresse enthalten für Source- oder Destination Routing (mögliche Angriffe).
Protocol	Das IP-Datagramm enthält neben dem Header den Payload. Von welchem Typ der Payload ist, steht im Feld Protocol.
SRC/DST IP-Addr	Keine RFC-1918-IP-Addresse am WAN-Seitigen Interface hereinlassen (3 Regeln für die Supernetze).

TCP-Header

SRC / DST Port	Eine Firewall kann nur bestimmte Ports zulassen
Control-Bits (Flats)	Verbindungsaufbau mit 3-Way-Handshake (SYN- und ACK-Flag)

UDP-Header

SRC / DST Port	Eine Firewall kann nur bestimmte Ports zulassen

Der Verbindungsaufbau ist deshalb nicht an einem SYN-Flag erkennbar.

3.2.5 Beispiel von Firewall-Regeln

Das Gesicht darf dabei nicht einschlafen!!!! ^ ^

1. Mailserver (SMTP) in DMZ
2. HTTP-Server in DMZ
3. HTTPS-Server in DMZ
4. Nameserver in DMZ (für Anfragen von aussen)
5. Nameserver in DMZ (für Client-Anfragen von innen nach aussen weiterzuleiten (rekursive DNS-Abfragen))
6. Nameserver AXFR / IXFR Notify-Verfahren Zonenübertragung in HMZ (Über TCP statt wie bei DNS normal UDP)
7. Nameserver AXFR / IXFR Slave-Hol-Vervahren Zonenübertragung in HMZ (Über TCP statt wie bei DNS normal UDP)

Nr.	Richtung	SF / SFI	L4 Proto	SRC-IP-Addr	SRC-Port / Proto	DST-IP-Addr	DST-Port / Proto	Action	Descr
1.1	WAN-DMZ	SF	IP	ANY	> 1023 / TCP	$SMTP_SRV	SMTP (25) / TCP	ALLOW	Mail: WAN SMTP IN
1.2	DMZ-WAN	SF	IP	$SMTP_SRV	> 1023 / TCP	ANY	SMTP (25) / TCP	ALLOW	Mail: DMZ SMTP OUT
2	WAN-DMZ	SF	IP	ANY	> 1023 / TCP	$HTTP_SRV	HTTP (80) / TCP	ALLOW	Web: WAN HTTP OUT
3	WAN-DMZ	SF	IP	ANY	> 1023 / TCP	$HTTPS_SRV	HTTPS (443) / TCP	ALLOW	Web: WAN HTTPS OUT
4	WAN-DMZ	SF	IP	ANY	> 1023 / UDP	$DNS_SRV	DNS (53) / UDP	ALLOW	DNS: WAN DNS Query IN
5	DMZ-WAN	SF	IP	$DNS_SRV	> 1023 / UDP	ANY	DNS (53) / UDP	ALLOW	DNS: DMZ DNS Query OUT
6	DMZ-HSZ	SF	IP	$DNS_SRV1	> 1023 / TCP	$DNS-SRV2	DNS (53) / TCP	ALLOW	DNS: Notify AXFR / IXFR Zonentransfer
7	HSZ-DMZ	SF	IP	$DNS_SRV1	> 1023 / TCP	$DNS-SRV2	DNS (53) / TCP	ALLOW	DNS: Slave-Hol AXFR / IXFR Zonentransfer

Tabelle 8: Firewall Master Table

- ANY = Beliebige IP-Addr / TCP- oder UDP-Port
- > 1023: Port-Nr. grösser als 1023 (Typisch für Client-Prozesse)
- $FOOBAR: Bitte durch die jeweilige IP-Adresse ersetzen. Danke. Säuberli mäihen.

3.2.6 Firewallregeln für FTP

Quellen: http://www.alenfelder.com/Informatik/pass-akt-ftp.html

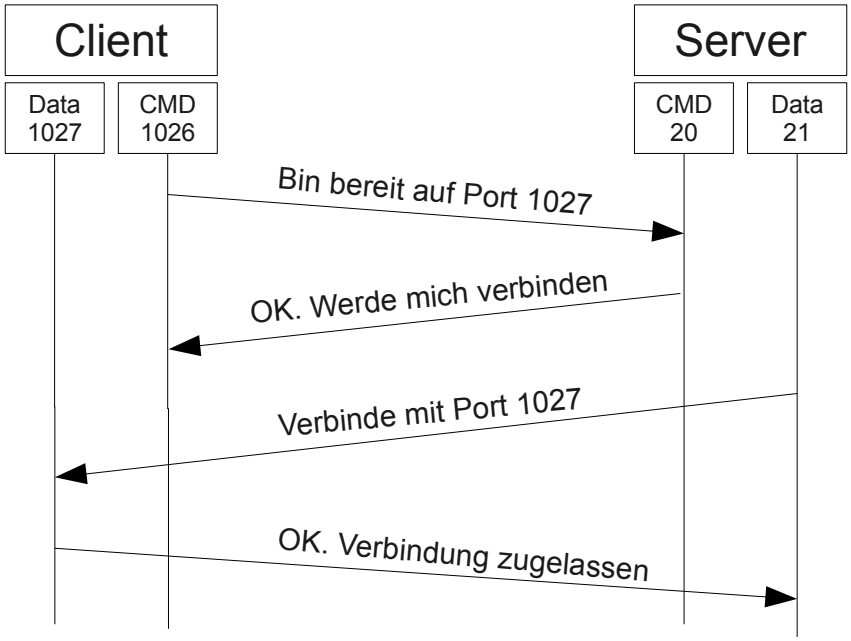
Aktives FTP (active mode)

Der Server verbindet sich nach der Client-Anfrage mit dem Client.

Der FTP-Client verbindet sich mit einem Port > 1024 mit dem Server Port 21.

Der Client wartet auf einem Port höher und sendet diesen Port an den Server.

Der Server verbindet sich mit diesem Port.



Problem (auf der Clientseite): Ohne Stateful Inspection müsste man alle TCP-Portnummern öffnen.

Router-Firewall 1 (Client)

Nr.	SF / SFI	L3, L4 Protokoll	Src-IP-Addr	SRC-Port	DST-IP-Addr	DST-Port	Beschreibung
1	SFI	IP, TCP	LAN	>=1023	ANY	21	Open FTP-Control FTP-Data per SFI

Router-Firewall 2 (Server)

Nr.	SF / SFI	L3, L4 Protokoll	Src-IP-Addr	SRC-Port	DST-IP-Addr	DST-Port	Beschreibung
1	SF	IP, TCP	ANY	>=1023	FTP-Srv	21	Open FTP-Control
2	SF	IP, TCP	FTP-Srv	20	ANY	>=1023	Open FTP-Data

Passives FTP (passive mode)

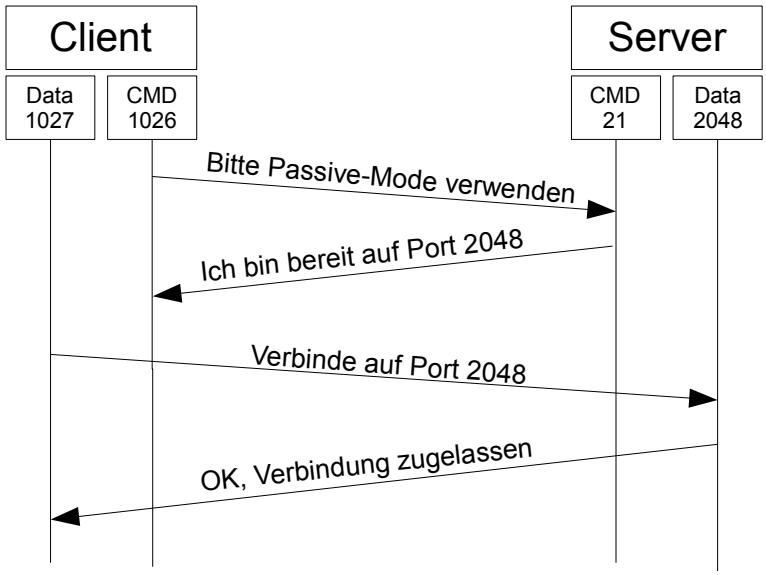
Der Client verbindet sich selber mit dem Server, nachdem er die Port-Nr vom Server bekommen hat.

Beim Passive-Mode muss der Server keine Verbindung aufbauen.

Dies erledigt der Client.
Der Client öffnet zwei Ports (N > 1024 und N+1).
Auf dem Port N kontaktiert der Client den Server, allerdings mit dem PASV-Kommando.

Dann öffnet der Server einen Dataport > 1024 und sendet den Port an den Client.

Der Client verbindet sich dann von seinem Datenport N+1 zum Data-Port der Servers.



Problem auf der Serverseite.

Router-Firewall 1 (Client)

Nr.	SF / SFI	L3, L4 Protokoll	Src-IP-Addr	SRC-Port	DST-IP-Addr	DST-Port	Beschreibung
1	SF	IP, TCP	LAN	>=1023	ANY	21	Open FTP-Control
2	SF	IP, TCP	LAN	>=1023	ANY	>=1023	Open FTP-Data

Optional Rule 1 mit SFI erweitern

Router-Firewall 2 (Server)

Nr.	SF / SFI	L3, L4 Protokoll	Src-IP-Addr	SRC-Port	DST-IP-Addr	DST-Port	Beschreibung
1	SFI	IP, TCP	ANY	>=1023	FTP-Srv	21	Open FTP-Control FTP-Data per SFI

3.3 Application Firewall

3.3.1 Beschreibung

- Auch bekannt unter Application Gateway oder Proxy
- Der Proxy trennt die direkte Kommunikationsbeziehung zwischen Client und Server und übernimmt als Stellvertreter die Kommunikation zum Zielrechner.
- Arbeitet qualis als Man in the Middle (Client-Proxy und Proxy-Server)
- Filterung von applikationsspezifischen Features (FTP Put, ...)
- Applikationserweiterungen wie Integration einer Authentisierung oder Aufzeichnung der

Zugriffspfade.

- Pro Applikation braucht es einen eigenen Proxy
- Gen**eris**che Proxies nehmen lediglich eine Verbindung entgegen und leiten diese weiter.

3.3.2 Anforderungen

- Benutzerspezifisch konfigurierbar (User und Gruppen)
- Anwendungsspezifische Einschränkungen
  - Gewisse FTP / SMTP Verbindungen verbieten
  - FTP-Dateizugriffe an Benutzer koppeln und nur eine Richtung durchlassen
  - Gewisse HTTP-Methoden durch Filter einschränken
  - Filterung der Nutzinformationen (Keywörter, Viren)
- Einige Dienste sollten nicht über eine Firewall hinaus genutzt werden
  - RPC, X11, NFS, NIS, TFTP, r-Dienste
- Logs an einen Internen Host senden
- Für Benutzeridentifikation eine starke Authentifizierungsmethode anbieten
- Für gewisse Applikationen muss Verschlüsselung möglich sein

3.3.3 Funktionen der FortiGate 500A

- Layer 7: Web-Content-Filter, Antimalware-Software, Antispam-Software, IDS, IPS, URL-Filtering
- Layer 5: SSL-VPN (OpenVPN), RADIUS
- Layer 4: Stateful-Inspection
- Layer 3: Stateful, IPSec, VoIP, NAT, Static und Dynamic Routing
- Layer 2: PPTP, L2TP

3.3.4 HTTP-Proxy Funktionen (z.B. Squid)

Normale Paketfilter stellen folgende Funktionen nicht zur Verfügung:

- URL-Filterung
- Daten filtern (alle mkv-Datein nicht zulassen)
- Inhalt filtern (nach Keyword suchen)
- Inhalt verändern (z.B. JavaScript filtern)
- Proxy kann Authentifizierung verlangen
- Benutzerbezogene Auswertung der Logfiles

- Dateien Scannen (Virensignaturen)

3.4 Architektur von Firewalls

Für die eigentlich Realisierung der Firewall, also das Zusammenspiel aus Paketfilter und Application Gateway, gibt es viele verschiedene Möglichkeiten. Die wichtigsten seien hier genannt :

3.4.1 Screening Router (Nur Packet-Filter)

Ein Screening Router ist ein Router, der zwei Netzwerke mittels Paketfilterung "sicher" verbindet. Er stellt die preiswerteste, aber auch die unsicherste Firewallarchitektur dar. Preiswert, weil ein Router bei jeder Netzwerkanbindung bereits vorhanden ist und auf jedem Router Access- und Deny-Listen zur Paketfilterung installiert werden können. Unsicher, weil Paketfilterung allein keine nennenswerte Hürde für einen Hacker darstellt.

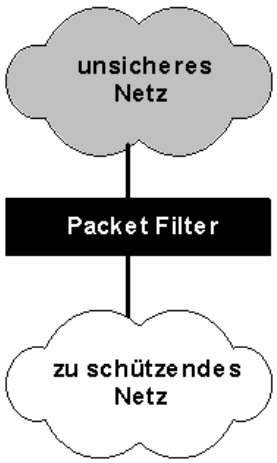
Vorteile

- leicht realisierbar, da die Funktionalität von vielen Routern geliefert wird
- leicht erweiterbar für neue Dienste

Nachteile

- IP-Spoofing möglich
- alle Dienste, die gestattet werden sollen, müssen auf allen Rechnern, die erreicht werden können, sicher sein
- komplexe Filterregeln
- keine Testmöglichkeiten, es ist insbesondere nicht möglich festzustellen, ob die Filterregeln in ihrer Reihenfolge verändert werden, was bei einigen Routern geschieht, um den Durchsatz zu steigern
- keine ausreichende Protokollierungsmöglichkeit

Der Einsatz von Paketfiltern ist unbedingt zu empfehlen, jedoch nicht ein ausschliesslicher Einsatz. Das Sicherheitsrisiko ist für Firmen und öffentliche Institutionen zu hoch.



Ausschlieslicher Einsatz eines Paketfilters

3.4.2 Dualhomed Gateway (Application Gateway)

Diese Anordnung besteht aus einem Application-Gateway mit zwei Netz-Interfaces, welches zwischen den beiden Teilnetzen eingesetzt wird. Es muss so konfiguriert werden, dass keine Pakete ungefiltert passieren können (IP-Forwarding abschalten).

Die Anwendung eines reinen Application Gateways zur Absicherung empfiehlt sich in nahezu keinem Fall. Eine Ausnahme wäre, den Application Gateway mit entsprechendem Cache-Speicher auszustatten, um damit z.B. HTML-Seiten zwischenzuspeichern. Jedoch kann man dann nicht von einer Absicherung des Netzes sprechen.

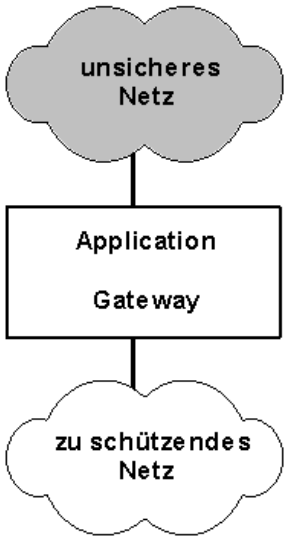
Vorteile

- Kein Paket kann ungefiltert passieren
- Umfangreiche Protokollierung möglich
- Interne Netzstruktur wird verdeckt

Nachteile

- Preis (Rechner mit zwei Netz-Interfaces)
- Keine Transparenz für den Benutzer
- Probleme bei neuen Diensten
- Die Übernahme des Application-Gateways durch den Angreifer führt zu einem vollständigen Verlust der Sicherheit

Ein zusätzlicher Schutz lässt sich durch den Einsatz eines Packet-Filters vor dem Gateway erreichen, wie z. B. durch einen vorhandenen Router. In diesem Fall müssten Router und Gateway durchbrochen werden, um Zugang zum zu schützenden Netz zu erhalten.



3.4.3 Three Homed Host

Ein Three Homed Host ist, analog zum Dual Homed Host, ein Rechner mit drei Netzwerkkarten. Auch hier sind alle Netzwerkinterfaces voneinander isoliert. Die dritte Netzwerkkarte dient dem Aufbau eines "Secure Server Network" (ssN). Das ssN dient dem Schutz von öffentlich zugänglichen Infoservern (z. B. WWW-Server). Will eine Institution einen WWW-Server installieren, kann das auf unterschiedliche Art geschehen. Sie kann den Server auf der externen Seite der Firewall im ungeschützten Netz plazieren. Damit ist der Server ungeschützt zugänglich für Attacken. Die andere Möglichkeit ist, den Server innerhalb des geschützten Netzes, also hinter der Firewall, zu plazieren. Damit müsste man aber einen sehr unsicheren Durchgang durch das Firewallsystem schaffen. Das Secure Server Network ist eine elegante Lösung für dieses Dilemma. Wird der WWW-Server in diesem Netz plaziert, dann ist er vollständig durch die Firewall geschützt, und auch für das interne Netz ergibt sich kein Sicherheitsloch. Aber auch hier hat man denselben Nachteil wie bei Dual Homed- und Screened Host.

3.4.4 Screened-Subnet

Bei dieser Konstellation handelt es sich um den Einsatz von zwei Paketfiltern. Diese zwei Paketfilter sind jedoch so zusammengeschaltet, dass sich zwischen ihnen ein weiteres Netz bildet. Das sogenannte "Screened Subnet". Durch dieses Screened Subnet oder auch Grenznetz wird das zu schützende Netz vollkommen vom unsicheren Netz entkoppelt.

Im Screened Subnet wird mit Hilfe von den zwei Paketfiltern für die Kontrolle der Verbindung gesorgt.Das Screened Subnet wird auch "De-Militarised Zone" genannt (DMZ)

Vorteile

- Kein direkter Zugang zum Gateway möglich
- Die Struktur des internen Netzes wird verdeckt
- Vereinfachte Regeln für die Packet-Filter
- Zusätzliche Sicherheit durch zweiten Packet-Filter
- Durch den Einsatz mehrerer Gateways lässt sich die Verfügbarkeit steigern
- Umfangreiche Protokollierung möglich

Nachteile

- Wenn die Packet-Filter manipuliert werden, ist eine direkte Verbindung unter Umgehung des Gateways möglich. Dies kann evtl. auch eine gewünschte Funktionalität sein (z. B. bei neuen Diensten)
- Angriffe auf die Packet-Filter werden nicht protokolliert
- Preis (Rechner mit zwei Netz-Interfaces)
- Keine Transparenz für den Benutzer

3.4.5 Screened Subnet und ein dual-homed Application Gateway

Diese Konfiguration einer Firewall bietet einen sehr hohen Sicherheitsstandard an und garantiert auch ein Höchstmass an Sicherheit.

Die beiden Paketfilter werden so zusammengeschaltet, dass sich zwischen ihnen ein Screened Subnet bildet. Das Application Gateway, dass sich nun in der DMZ befindet und zwei Netzschnittstellen besitzt, kontrolliert nun jedes Datenpaket. Es ist sichergestellt, dass sich kein Datenpaket am Application Gateway "vorbeischleichen" kann.

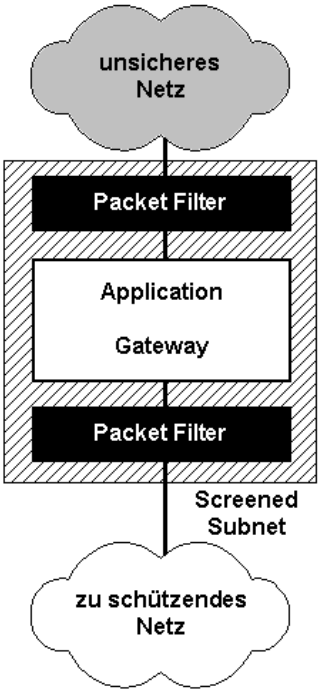
Vorteile

Die Vorteile einer solchen High-Security Konstellation sind

- Einfache Regeln, die Anordnung der Elemente ermöglicht eine einfache Definition der Regeln der einzelnen Firewall-Elemente
- Gegenseitiger Schutz, Die Paketfilter sorgen dafür, dass nicht jeder auf das Application Gateway zugreifen kann
- Geschachtelte Sicherheit, es wird nicht jede Sicherheitsanforderung an nur ein System gestellt

Durch den Einsatz von verschiedenen Betriebssystemen lässt sich das Schutzniveau nochmals eröhen. Denn dadurch schliessen sich unter Umständen Implementierungsfehler der verschiedenen Betriebssysteme gegenseitig aus.

Der Einsatz dieser Firewall eignet sich dann, wenn man wirklich von einem zu schützenden Netz (Firmennetz) und einem unsicheren Netz (Internet) sprechen kann. Das nicht einzuschätzende Sicherheitsniveau des Internets wird somit gesenkt.



4 Das Kerberos-Protokoll

Das Kerberos-Protokoll (Version5) dient zur Authentifizierung in einer AD DS-Umgebung. Hierbei wird nach erfolgreicher Authentifizierung ein TGT (Ticket Granting Ticket) als Nachweis für die Identität des betreffenden Benutzers in der Netzwerkumgebung ausgestellt. Dieses TGT wird durch das Schlüsselverteilungscenter KDC (Key Distribution Center) ausgestellt. Diese Kerberos-Tickets werden im Clientrechner in einem speziellen Speicherbereich des Arbeitsspeichers abgelegt und niemals in die Auslagerungsdatei übertragen.

Prä-Windows 2000 Versionen verstehen Kerberos nicht und können sich lediglich das alte LAN-Manager (LM) bzw. Das NT-LM Protokoll zur Authentifizierung. Der Windows Server 2008 ist jedoch abwärtskompatibel.

4.1 Merkmale von Kerberos v5 in AD

Folgendes sind die Hauptmerkmale von Kerberos:

- Gegenseitige Authentifizierung (Client / Benutzer / Gruppe gegenüber AD DC)
- Sichere Übertragung der Authentifizierungsdaten über das Daten über das Netzwerk (SSL)
- Das Kennwort wird niemals übertragen (Nur kombinierte Hash-Werte, wie bei CHAP)
- Ermöglicht Single Sign-On Authentifizierung

Weitere Merkmale sind:

- Schutz vor Wiederverwendung von gesendeten Authentizierungsdaten
  Erklärung: Dies wird mit einem Zeitstempel verhindert. Deshalb muss auch geachtet werden das die Zeit auf den DC nicht mehr als 5 Minuten auseinander sind.
- Delegierte Authentifizierung
- Kerberos V5 ist ein Industrie-Standard Protocol
- Interoperabilität (Von Windows System aus kann Authentifizierung auf UNIX-Realms)
- Ticket caching (Der Ticket Cache kann mit dem Kommandozeilen-Tool Klist.exe oder dem graphischen Tool Kerbtray.exe angezeigt werden. Diese beiden Tools befinden sich bei den Resource Kit Utilities.
- Zeitnahe Entscheidung: Zeitsynchronisation: Die verschiedenen Server müssen die selbe Zeit haben.

4.2 Komponenten von Kerberos

Wichtige Komponenten von Kerberos v5 im AD sind:

KDC	Key Distribution Center (Schlüsselverteilungscenter); auf jedem DC (existiert dafür ein SRV-RR in er DNS-Forword-Lookup Zone)
TGT	Ticket Granting Ticket; Erlaubnisticket, um Service Tickets (ST) für Ressource-Zugriffe (Quasi: ST für die Verwendung des KDCs)

ST	Service Ticket; Muss für Ressource-Zugriffe erworben werden. Enthält die SID des Users und seiner Sicherheitsgruppen. ACL, Art der Berechtigung
RT	Referral Ticket – Empfehlungs- oder Überweisungsticket

Diese Komponenten werde also benötigt, wenn sich ein Windows 2k+ Rechner an einer Domäne anmelden will.

4.2.1 Key Distribution Center (KDC)

Das KDC versorgt User und Computer mit einem Ticket Granting Ticket und einem Service Ticket. Das KDC tauscht Informationen zwischen Benutzern und Server durch, wenn sich ein Benutzer und der Server gegenseitig authentifizieren.

Der Authentifizierungs-Service (AS) führt für die Benutzer die anfängliche Authentifizierung durch und rüstet den Benutzer mit deinem Ticket Granting Ticket (TGT) aus.

Fordert ein User eine Ressource an, muss er dem Ticket Granting Service (TGS) sein Ticket Granting Ticket (TGT) vorweisen!

Der Ticket Granting Service (TGS) gibt dem User ein Service Ticket für die Authentifizierung bei der gewünschten Ressource.

4.2.2 Ticket Granting Ticket

Bei der Anmeldung an einer Domäne bekommt der User ein Ticket Granting Ticket (TGT). Ein TGT ist auch ein Service Ticket für die Benutzung des KDCs.

Der User braucht ein TGT um STs vom KDC anzufnordern. Verlangt ein User ein ST, muss er dem KDC sein TGT vorweisen um die Authentifizierung an der Domäne zu bestätigen.

Bei jeder Ausstellung eines ST wird der Useraccount auf Gültigkeit geprüft. Ist der User deaktiviert oder gelöscht (oder sonst bei den Hasen) stellt der KDC keine STs mehr aus.

Erwerb eines TGT

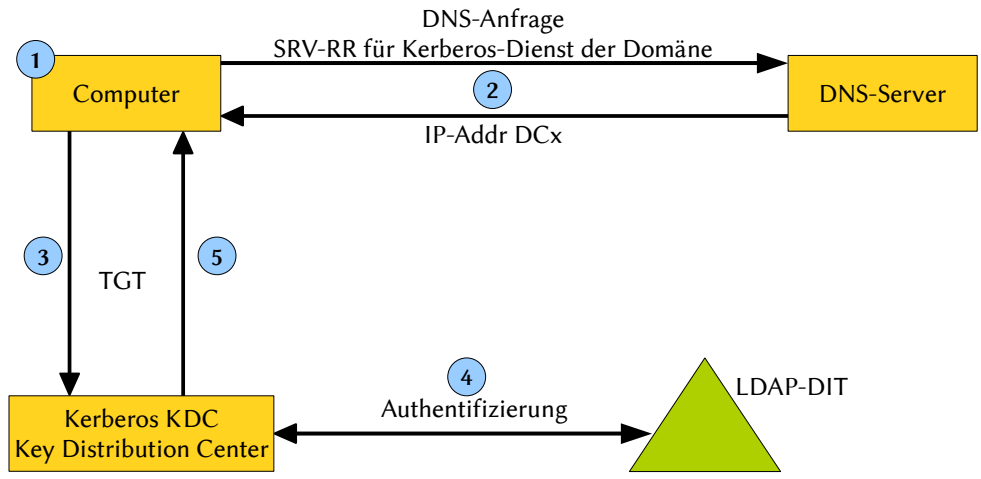


Abbildung 1: Erwerb eines TGT

1. User gibt seine Logindaten im Anmeldefenster ein
2. Computer fragt den DNS-Server nach dem „_kerberos“-RR (Forward-Lookup-Zonenfile)
3. Client macht einen „Authentification Service Request“ an den Kerberos-Server (Kontoinformationen & Systemzeit werden Verschlüsselt) (Wireskark sagt „KRB_AS_REQ-Message“)
4. Der Authentifizierungs-Service auf dem DC authentifiziert den Benutzer gegen Einträge im LDAP-DIT.
5. Der KDC generiert ein TGT, welches dem Benutzer mit einer „Authentification Service Response“ (KRB_AS_REP) mitgeteilt wird.

Ports

Folgende Ports werden dabei verwendet:

- 53 (DNS), 88 (Kommunikation mit KDC)
- 123 (Zeitsynchronisierung)
- 464 (Kerberos-Kennwortänderungen)

4.2.3 Service Ticket

Der User muss sein Service Ticket (ST) (welches er vom KDC bekommen hat) vorweisen, wenn er auf eine Ressource zugreift.

Das Service Ticket beinhaltet Infos über die Ressource / Service und über den User, der die Ressource nutzen will. Vom User ist die SID und die SIDs von seinen Gruppen gespeichert. So kann anhand der DACL überprüft werden, ob und wie der User auf die Ressource zugreifen darf oder nicht.

Das ST ist mit einem gemeinsamen Session-Key verschlüsselt. Nur der zugehörige PC kann das Ticket entschlüsseln.

4.2.4 Referal Ticket (Empfehlungs- oder Überweisungsticket)

Das Referal Ticket wird ebenfalls vom KDC ausgestellt. Damit kann ein User bei einer anderen Domäne empfohlen werden. Das Referal Ticket dient in der anderen Domäne als Ticket Granting Ticket (TGT).

Verschlüsselt wird das Ticket mit dem Interdomänenschlüssel welcher bei der Vertrauensstellung der Domänen der Gesamtstruktur erzeugt wird.

4.3 Gruppenrichtlinien in Active Directory

- Rechte an Systemen
- Konfigurationen
- Skripte (Anmeldung, Abmeldung, Booten)
- Kann gebunden werden zu folgenden Active Direcotry Container (wirken für User und Computer die sich in den betreffenden Containern befinden)
    - Standort: Lokaler Proxyserver angeben

- Domäne: default Domain Policy
- Organisationseinheit: Domain Controllers (default Domain Controller Policy)

4.3.1 Merkmale für Standorte

- Physikalischer Standort entspricht einem IP-Teilnetz!
- Die Inter-Standort-Replikation muss konfiguriert werden.
- Die Inter-Standort-Konnektivität der RFC 1918 Teilnetze über das Internet muss durch eine IP-in-IP-Technologie abgewickelt werden!!!
  - IPinIP, IPSec (ISAKMP, ESP)

4.3.2 GPO als Element des Security Management

Zuordnung von Policies am bestimmte Servertypen:

- Domain
  - OU Domain Controllers
  - OU Infrastrukturserver
    (Unterstützt durch Microsoft Server Security Dokumentationund Konfigurationsskripte)
    - OU Fileserver
    - OU Printserver

5 Kryptographie

Heuristik	Mit wenig Aufwand zu einer guten Lösung kommen (Bei Antivirenprogrammen: was macht ein Programm und ist es deshalb böshaft?)
Kerberos	Authentifizierungsdienst; in ActiveDirectory
Symmetrisch	Beide verwenden den selben Schlüssel (DES (nur 56 Bit lang), AES (löste DES ab), Blowfish)
Asymmetrisch	Beide verwenden verschiedene Schlüssel (RSA, Rabin, Elgamal)
Deterministisch	Berechenbar
Stochastisch	Zufällig
SSH	Secure Socket Shell; Remotezugriff auf Server, Filetransfer, Tunneln; AES-128, 3DES, Blowfish,
Knacktechniken	Bruteforce: Durchprobieren von Kombinationen bei Passwörtern Dictionary probiert ein Wörterbuch durch Rainbowtable: vorberechnete Hashes
Hash	Prüfsumme, immer gleich lang, nicht zurück rechenbar; zur verifizierung von Dateien
Einsatz	
Zyklische Redundanzprüfung	CRC
VPN	NPPE, EPP, ... /etc... komisch...
WLAN	WEP, WPA (802.11i)

5.1 Verschlüsselungsverfahren

5.1.1 Symmetrisches Verschlüsselungsverfahren

- Absender und Empfänger besitzen den gleichen Schlüssel.
- Dieses Verfahren ist sehr schnell.
- Bietet eine gute Sicherheit.
- Das Problem ist der Austausch der Schlüssel.
- Wenn ein dritter diesen Schlüssel kennt, kann er die Daten manipulieren.
- **Substitution**: Einzelne Zeichen eines Textes durch andere tauschen
- **Transposition**: Reihenfolge der Zeichen ändern.

5.1.2 Asymmetrisches Verschlüsselungsverfahren

- Es gibt private und öffentliche Schlüssel.

- Dieses Verfahren nennt man PKI (Public Key Infrastructure)
- Es wird mit dem öffentlichen Schlüssel verschlüsselt.
- Der dazugehörige private Schlüssel kann die Nachricht wieder entschlüsseln.
- Dieser Vorgang ist 1000 mal langsamer als die symmetrische Verschlüsselung.

5.1.3 Hybridverfahren

- Die Schlüssel für die symmetrische Verschlüsselung werden mit der asymmetrischen Verschlüsselung übertragen.

5.1.4 Authentifikation

- Mit dem privaten Schlüssel wird eine Nachricht verschlüsselt.
- Mit dem dazugehörigen öffentlichen Schlüssel wird die Nachricht entschlüsselt.
- Der öffentliche Schlüssel kann jeder einsehen.
- Die Nachricht kann gelesen, jedoch nicht manipuliert werden, weil man zum erneuten Verschlüsseln wieder den privaten Schlüssel braucht.

5.1.5 Elektronische Unterschrift

1. Hash-Wert einer Nachricht wird mit dem privaten Schlüssel verschlüsselt.
2. Empfänger entschlüsselt den Hash-Wert mit dem dazugehörigen öffentlichem Schlüsel.
3. Empfänger bildet auch den Hash-Wert.
4. Ist der Hash-Wert der selbe, dann wurde die Nachricht nicht verändert.

5.1.6 Zertifikate

- Damit man sichergehen kann, dass der öffentliche Schlüssel wirklich von der anzunehmenden Person stammt, wurden Zertifizierungsstellen eingerichtet.
- Diese Zertifizierungsstellen veröffentlichen den eigenen öffentlichen Schlüssel in einem Zertifikat, das von der Zertifizierungsstelle elektronisch unterschrieben ist.

5.2 Verschlüsselung

Funktioniert nicht wirklich

- Bob: PrivKeyBob(PubKeyAlice(DocAlice))
  - Geht, aber führt zu nichts.
- Alice: PrivKeyBob(PubKeyBob(DocBob)):
  - Geht nicht, da Alice PrivKeyBob nicht hat.

- Bob: PrivKeyAlice(PrivKeyAlice(DocAlice)):
  - =DocAlice (alle können das tun)
- Bob: PrivKeyBob(PubKeyBob(DocBob))
  - =DocBob (kann nur Bob machen)

Funktioniert

- Alice will ein Dokument verschlüsseln, das nur von Bob gelesen werden kann.
  - PublicKeyBob(DocAlice)
- Bob will das verschlüsselte Dokument entschlüsseln (das kann nur Bob ausführen)
  - PrivKeyBob(PubKeyBob(DocAlice))

5.3 Digitale Signaturen

Ziele

- Nichtabstreitbarkeit der Urheberschaft
- Schutz der Integrität der Daten

6 WLAN-Security

6.1 IEEE 802.1X (WPA-Enterprise)

- Kann auch mit Layer 2 Switchen genutzt werden!!!
- PEAP mit Kennwörter
- Zertifikatdiente zur Verwendung von PEAP anstelle von EAP-TLS

6.1.1 Vorteile

- Zentraler Authentifizierungssserver
- Der entscheidende Vorteil: nur nach erfolgreicher persönlicher Authentifizierung ist der Zugang offen. Bei PSK ist kein Benutzer sichtbar.

6.1.2 Diagramm für die Authentifizierung

Nach der Authentifizierung läuft der Connect vollständig „normal“.

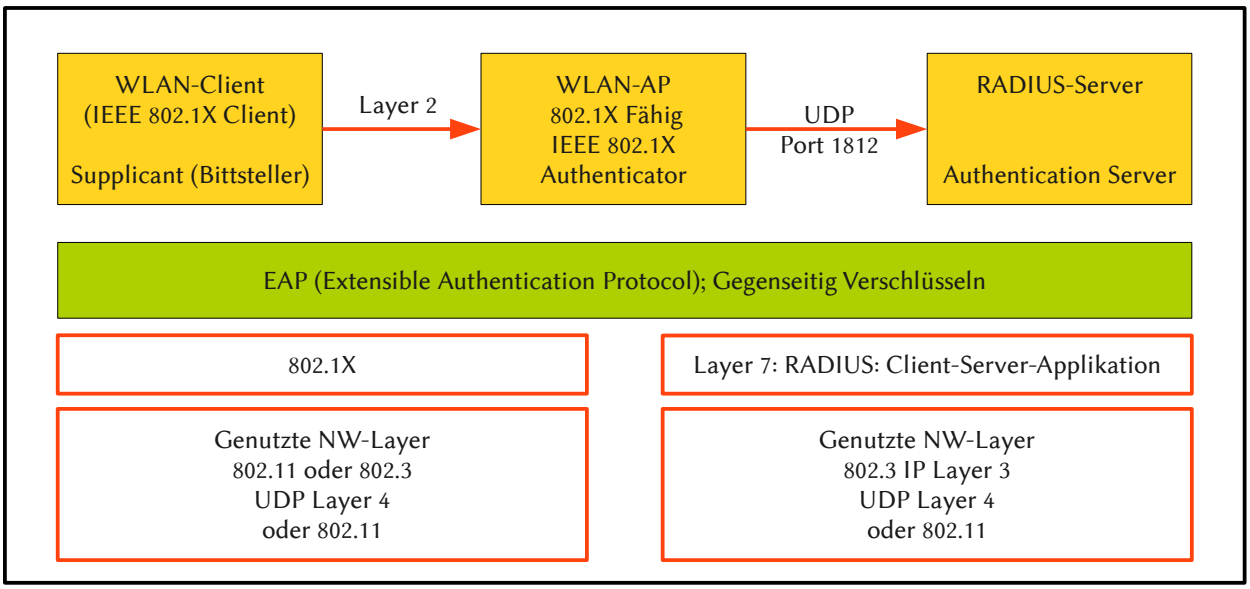


Abbildung 2: Authentifizierungsdiagramm

Radius: Remote Authentication Dial-In User Service

Supplicant

Authenticator

6.1.3 Ablauf der Authentifizierung

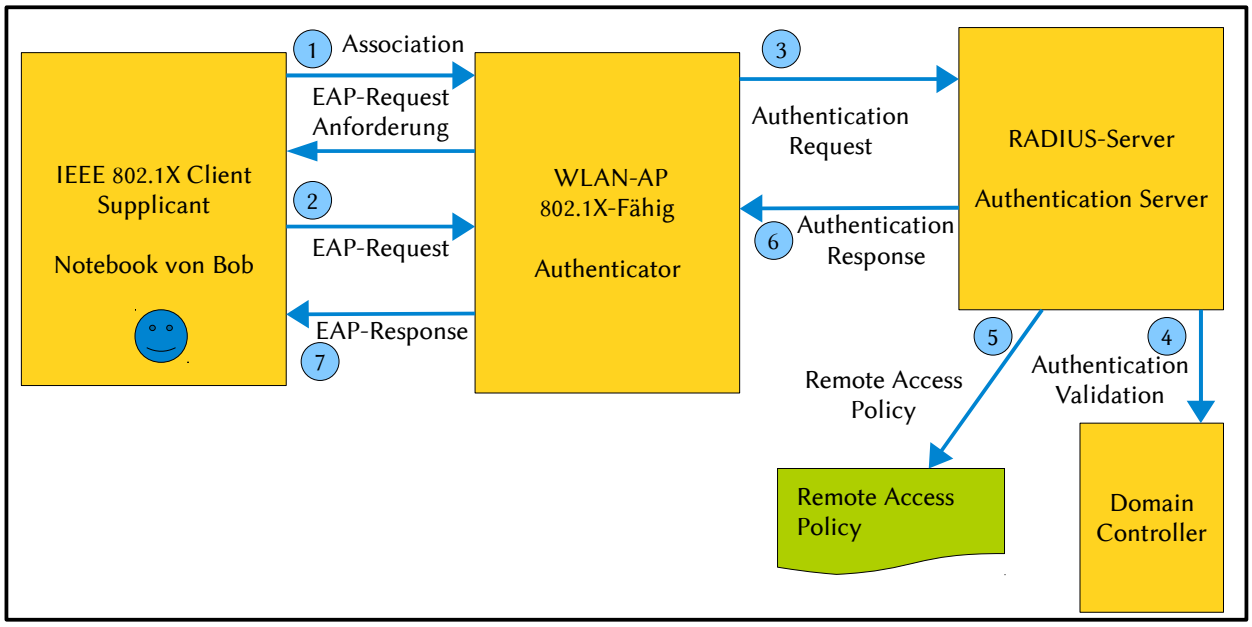


Abbildung 3: Ablauf der Authentifzierung

1. Client will Verbindung mitAuthenticator herstellen; Authenticator reatiert entsprechend
2. Client gibt Anmeldeinformation an den Authenticator weiter
3. Authenticator übersetzt die EAP-Authentifizierungsnachricht und leitet diese an den RADIUS-Server weiter
4. Der RADIUS-Server überprüft am DC die Signatur des Zertifikats, welcher der Client gesendet hat.
5. Der IAS-Server überprüft die RAS-Richtlinien, ob der im LDAP identifizierte Computer über den Authenticator Zugang erhalten soll.
6. Der RADIUS-Server sendet eine Erfolgs- bzw. Fehlermeldung an den Authenticator
7. Der Authenticator sendet eine EAP-Erfolgs bzw. Fehlermnachricht an den Client

Dach der Authentifizierung erfolgt die IP-Konfiguration.

6.2 Managed Port

Managed Port: IEEE 802.1x gemanagter Port: Port-Konnektivität ist erst nach erfolgter Authentifizierung nutzbar.

7 Intrusion Detection Systems (IDS)

Zweck: Erkennen von Angriffen gegen Computer oder Netzwerken.

7.1 Typen

Es gibt Host Intrusion Detection Systems (HIDS) und Network Intrusion Detection System (NIDS).

7.1.1 Host Intrusion Detection Systems (HIDS)

- HIDS werden auf Hosts installiert.
- Sie ergänzen das Betriebssystem in der Erkennung von Angriffen.
- Dazu werden Log-Dateien des Betriebssystem ausgewertet.
- Ein HIDS schlägt Alarm, wenn ein vermeintlicher Angriff erkannt wird.
- Vorteil: Umfassende Sysgemüberwachung
- Nachteil: Performanceeinbusse, Anfälligkeit gegen DoS-Angriffe
- Verwendung: Serversysteme, die häufig Angriffen ausgesetzt sind: http, https, smtp, pop3, imap, ftp, dns

7.1.2 Network Intrusion Detection System (NIDS)

- Der Netzwerkverkehr wird analysiert und anhand von Angriffsmuster Angriffe erkennt.
- Vorteil: Ein einzelnes NIDS kann ein ganzes Netzwerk (typischerweise die DMZ!) überwachen
- Nachteil: NIDS sind häufig den Bandbreite-Anforderungen leistungsfähiger LAN (z.B. GBits/s) nicht gewachsen. Dann müssen Pakete weggeworfen werden, was keine Lückenlose Überwachung ergibt.
- Verwendung: Perimeter-Netzwerke (Übergangsnetzwerke, DMZ): Hier sind Angriffe aus dem Internet besonders häufig zu registrieren.

7.2 Falschmeldungen

IDS sind sehr komplex und oft weichen die angegebenen Leistungen von den realen Leistungen ab.

- False positive: Falscher Alarm: Es wurde ein Angriffsmuster erkannt, obwohl es keinen Angriff gab.
- False negative: Kein Alarm, obwohl ein Angriff stattgefunden hat.

7.3 Funktionsweise

Die meisten IDS arbeiten mit Filtern und Signaturen (spezifische Angriffsmuster). Der Nachteil ist, dass nur bekannte Angriffe erkannt werden.

1. Warnehmung (HIDS: Logdaten; NIDS: Netzwerkverkehr)
2. Erkennung:
    1. Die Meisten IDS machen eine Mustererkennung: Vergleich mit Signaturen aus der Musterdatenbank
    2. Einige IDS verwenden heuristische Methoden, die nicht nur bekannte, sondern auch ähnliche Angriffe oder ein Abweichen von einem Normalzustand erkennen
3. Reaktion:Trifft Muster zu: Alarm (E-Mail, SMS, Twitter-Nachricht ^^)
    1. Ein IPS (Intrusion Prevention System) kann die Verbindung unterbrechen oder die übertragenen Daten ändern. Hierfür ist ein Firewallsystem notwendig.

Neue IDS/IPS erkennen mit einer Kombination aus Stateful inspection, Pattern Matching und Anomalieerkennung auch Abweichungen vom RFC-Standard in Protokollen.

7.4 Software

Sehr bekannt ist die OpenSource-Software Snort.

7.5 Honeypot

Mit Honeypots simuliert man Netzwerkdienste eines Computers, eines ganzen Netzwerks oder das Verhalten eines Anwenders.

Honeypots werden eingesetzt, um Informationen über Angriffsmuster und Angreiferverhalten zu erhalten. Erfolgt ein Zugriff auf ein Honeypot-Host, werden alle damit verbundenen Aktionen protokolliert und evtl. Sogar ein Alarm ausgelöst.

Es werden also gezielt Angreifer auf ein System angelockt, das sonst nicht verwendet wird. Da das System bei einem Angriff dann plötzlich verwendet wird, kann man von einem Angriff ausgehen.

Durch die Angriffsmuster können die Firewalls und IDS verbessert werden.

Administratoren sollen über die Angriffe informiert werden.

7.6 WLAN-Roaming

ESSID

Alle APs bekommen die selbe SSID. Hierfür müssen sie die erweiterte Version ESSID (Extended Service Set Identifier) unterstützen. Man muss jedoch unterschiedliche Kanäle verwenden!

IEEE 802.11f (IAAP)

Man kann auch Inter Access Point Protocol (IAAP) verwenden. Dabei teilen sich die APs Infos über die Clients mit. So kann die Verbindung unterbrechungsfrei sein.

[Quelle: http://www.elektronik-kompendium.de/sites/net/1407081.htm]

8 Netzwerksicherheits-Tools

Tools für Penetrationstests und Audits zum Aufdecken von Schwachstellen wie

- Offene Ports
- schwache Authentifizierungssysteme
- Vulnerabulities von eingesetzten OS (z.B. Anfälligkeit gegen [D]DOS) und Serversoftware (z.B. Buffer overflow)
- Datenübertragung (Vertraulichkeit, Integrität)
- Datenzugriff (Berechtigungskonzept)

8.1 Buffer Overflow

Buffer Overflow überschreibt die Return-Adresse um einen privilegierten SW-Einsprung zu machen.

8.2 Tools

Portscanner	Nmap (inkl. versteckte Scan, OS-Fingerprinting), portbunny, wolpertinger
Paketsniffer	Tcpdump, Wireshark, MS Netzwerk Monitor
Security und Vulnerability Scanner	Nessus (Funktioniert als Client-Server-Prinzip) BOss 2.0 vom BSI (basiert auf Nessus)
Passwort-Cracker	John (John the Ripper), Cain & Abel, CmosPWD, VNCrack, PWDUMP2, LCP, OphCrack
Keylogger	Refog, Sub7
Password Review	SAMinside, HTTP BruteForcer
Remote Access Tools	dfrost, Optix-Pro
Wireless Hacking	kismet, aircrack-ng, Network Stumbler (netstumbler)
Paketgeneratoren	netcat (nc), hping, arpspoof (aus dem dsniff-Paket)
Sonstige Tools	netcat (nc), Metasploit Framework (MSF), USBDUMPER, Net Tools, Satans Trick, WMF Maker

Tabelle 9: Tools

Weitere Informationen

- http://emanuelduss.ch
  Weitere Zusammenfassungen, Dokumentationen und Dokumente von mir

Glossar

Begriff	Definition

Stichwortverzeichnis