

Praktikum IT-Sicherheit - Versuchshandbuch -

Aufgaben

VPN

In diesem Versuch lernen Sie eine sichere VPN Verbindung zu einem Server aufzubauen. Dabei werden zuerst ältere Verfahren eingesetzt und mittels eines Angriffs die Verwundbarkeit dieser Verfahren gezeigt. Anschließend wird anhand eines selbst erstellten Zertifikats eine L2TP-IPSec-VPN Verbindung eingerichtet.

B.Sc. AI, WI M.Sc. AI M.Sc. EB

Einleitung

In diesem Versuch lernen Sie, eine sichere VPN-Verbindung zu einem Server aufzubauen. In Aufgabe 1 wird zunächst eine VPN-Verbindung unter Verwendung von älteren Verfahren für die Verschlüsselung und Authentifizierung erstellt. In Aufgabe 2 wird die Verwundbarkeit dieser Verfahren mittels eines Wörterbuchangriffes gezeigt. Abschliessend wird mittels eines selbst erstellten Client-Zertifikats eine L2TP-IPSec-VPN Verbindung eingerichtet, die Schutz vor den zuvor kennengelernten Problemen bietet.

Netzwerkplan



Aufgabe 1: Einrichtung einer VPN-Verbindung mittels PPTP

- a) Melden Sie sich am VPN-Client an und errichten Sie über die Netzwerkumgebung (Desktop → Netzwerkverbindungen → Neue Verbindung) eine neue VPN-Verbindung mit dem VPN-Server. Als Firmennamen wählen Sie "Seclab VPN". Als Server geben Sie die IP-Adresse des VPN-Servers an.
- b) Testen Sie die VPN-Verbindung. Verwenden Sie den Benutzernamen "Administrator" und das Passwort "W2K3Boss" für die Anmeldung.
- c) Sehen Sie sich die Details der VPN-Verbindung an (Rechte Maustaste auf die Verbindung → Status). Welche Technologien werden zur Authentifizierung und Verschlüsselung eingesetzt?

d) Wo befinden sich die Schwachstellen dieser Techniken?

e) Trenne Sie nun die VPN-Verbindung.

Aufgabe 2: Angriff auf die PPTP-Verbindung

a) Offnen Sie auf dem Angreifer-PC die Konsole generieren Sie im Ordner "Desktop" die Hashwerte zu der dort befindlichen Passwortliste (german.txt). Verwenden Sie folgendes Kommando:

genkeys -r german.txt -f german.dat -n german.idx

Hinweis: Dies kann etwas dauern und verursacht zur Laufzeit mehrere Dateien auf dem Desktop, die anschliessend selbstständig gelöscht werden.

 b) Führe Sie nun unter Verwendung der Passworthashes einen passiven Angriff auf die VPN-Verbindung durch. Verwenden Sie dazu folgendes Kommando: asleap -i eth0 -f german.dat -n german.idx -v

Hinweis: Lassen Sie nach Eingabe des Kommandos die Konsole geöffnet und verändern Sie nun nichts mehr am VPN-Angreifer.

c) Starten Sie nun die VPN-Verbindung (wie in Aufgabe 1b) erneut und sehen Sie sich anschliessend die Konsole auf dem VPN-Angreifer an. Was fällt Ihnen auf?

d) Beschreiben Sie den durchgeführten Angriff mit einigen Worten. Welchen Zweck erfüllt die Hashwertliste?

e) Trenne Sie nun die VPN-Verbindung.

Aufgabe 3: Sichere Verbindung mittels L2TP und IPSec

a) Was ist L2TP?

b) Was ist IPSec?

- c) Ändern Sie die in Aufgabe 1 erstellte VPN-Verbindung so ab, dass die Technologien L2TP und IPSec verwendet werden. Gehen Sie wie folgt vor:
 - Öffnen Sie die Eigenschaften der VPN-Verbindung
 - Wechseln Sie zur Registerkarte Sicherheit und wählen dort die erweiterten Sicherheitsoptionen
 - Wählen Sie zur Authentifizierung ausschliesslich das MS-CHAP V2 Protokoll und bestätigen Sie mit OK.
 - Wechseln Sie nun in die Registerkarte Netzwerk und wählen Sie als VPN-Protokoll L2TP-IPSec-VPN aus und bestätigen Sie mit OK.
- d) Versuchen Sie die Verbindung zu aktivieren. Was fällt Ihnen auf? Welches Problem liegt vor?

Aufgabe 4: Erzeugen des benötigten Zertifikats

- a) Um die in Aufgabe 3 erstellten VPN-Verbindung verwenden zu können, wird ein Zertifikat benötigt. Dieses kann über den Webdienst des VPN-Servers beantragt werden. Gehen Sie wie folgt vor:
 - Öffnen Sie auf dem VPN-Client einen Webbrowser und laden Sie die Webseite unter http://seclab-vpn/certsrv/
 - Fordern sie über die "erweiterte Zertifikatsanforderung" ein neues Zertifikat (ohne Base24-Codierung) an. Verwenden Sie die folgenden Angaben:

Evented 2 edition content Martine Martine Martine Martine Martine Martine Martine Auton Bach Bach Bach Bach Bach Bach Bach Bach	Microsoft Zertifikatd	lienste Seclab VPN CA	Startseite
Wentifikationsinformationer: Name WPNN Testhemutzer Saclab E-Mail-Adresse Benutzer@asclab vpn local Firms beckab Statelang: Beckab Bundesland/Kanton: Hessen Land/Region: DE Profestention: Image: Schlüsselsatz erstellen Periodestind/Kanton: Hessen Schlüsseloptioner: Image: Schlüsselsatz erstellen Optionseller: Image: Schlüsselsatz erstellen Schlüsseloptioner: Image: Schlüsselsatz erstellen Optionseller: Image: Schlüsselsatz erstellen Schlüsseloptioner: Image: Schlüsselsatz erstellen Optionseller: Image: Schlüsselsatz erstellen Optionseller: Image: Schlüsselsatz erstellen Optionseller: Image: Schlüssel in Schlüssel in Schlüssels in Schlüssels in Schlüssel in Schlüss	Erweiterte Zertifi	ikatanforderung	
Identificationshifermations: Warr: Warr: Warr: Wint Testburgter Sectab Absteilung Statt: Hudnakanses DendeslandfAston BundeslandfAston DendeslandfAston BundeslandfAston DendeslandfAston Schlusselptionen: OPSecZentfikat: OPSecZentfikat: Marxie: Signatur OPsides Schlussel and "Expontenbar" markiterer OPSchlussel and "Expontenbar" markiterer OPSchlussel and "Expontenbar" markiterer OPSchlussel and "Expontenbar" markiterer OPSchlussel and "Expontenbar" Zentifikat: Nut Adomsiterbar contakaspositerer Beschlussendener Actionseer ansettizierengsoselleiterer </th <th></th> <th></th> <th></th>			
Name: VP-MI-Partibenduzzer Seclab E-Mai-Adresse: Immit: Mateilung: Seclab Stat: Inda Dateilung: Seclab Stat: Inda BundeslandKantor: Imsesse Der Ser Serfordstichen Zerriffstat: Immit: Police-Zerifikat: Immit: Schlusselgeride: Immit: Immit: Immit: Schlusselgeride: Immit: Schlusselgeride: Immit: Immit: Immit: <tr< th=""><th>Identifikationsinfor</th><th>mationen:</th><th></th></tr<>	Identifikationsinfor	mationen:	
E-Mail-Adress: Eincurtureggeeclab. yen local Firms: Nechchule Fulda Budesland Kanton: Hessen Land Regio: D: P Sec-Zentifikat: P Sec-Zentifikat: P Sec-Zentifikat: Schlusselegröß: Chyptografiedienstanbieter: Neuen Schlusselsatz erstellen O Bestehenden Schlusselsatz verwenden Kryptografiedienstanbieter: Neuen Schlusselsatz erstellen O Bestehenden Schlusselsatz verwenden Schlusselgrößt: 1024 was:::ssell (M Bestehenden Schlusselsatz verwenden Schlüsselgrößt: 1024 was::ssell (M Bestehenden Schlusselsatz) Schlüsselgrößt: 1024 was::ssell (M Bestehenden Schlusselsatz) Schlüsselgrößt: 1024 was::ssell (M Bestehenden Schlüsselsatz) Schlüsselgrößt: 1024 was::ssell (M Bestehenz) Schlüsselgrö	Name:	VPN-Testbenutzer Seclab	
Firm: Motenbule Fulda Abteilung: Seciab Stat: Iuda UndRegio: E Top des enfordentichen Zertifikat: For des enfordentichen Zertifikat: Iversenden Schlüsselsatz erstellen Statise for des enfordentichen Zertifikat: Schlüsseler enfordentichen Zertifikat: Statise for des enfordentichen Zertifikat: Schlüsseler enfordentichen Zertifikatspielen: Schlüssel in Datei exportieren Orteritähte Schlüssel enfordentichen: Zertifikat Win Administatoren duftieren: Zertifikat: Schlüssel en des Epochere enfordentichen: Zertifikat: Marken des Zertifikatspielen: Zertifikat: Marken des Z	E-Mail-Adresse:	Benutzer@seclab.vpn.local	
Abtellung Sicili Sitili Fulda Bundeslandk/kanton Fessen LandRegion: E Spides enforteeticten Zentifikat:	Firma:	Hochschule Fulda	
Stati: Fulda BundestandKantor: Hesen Land/Regior: E Typ des ordordetichen Zertifikat: Image: Schlusselsatz erstellen Bestehenden Schlüsselsatz verwenden Kryptografiedienstanbieter: Microsoft Enhanced Cryptographic Provider v1.0 Schlüsselsgrößer: Exchange: Schlüsselsgrößer: Schlüsselsotortainername: Schlüsselsgrößer: Schlüsselsotortainername: Schlüssel in Datei exportieren Schlüssel in Datei exportieren Schlüssel in Datei exportieren Schlüssel in obtei exportieren Schlüssel in Datei exportieren Schlüssel in obtei exportieren Schlüssel in Datei exportieren Schlüssel in obtei exportieren Schlüssel in obtei exportieren Schlüssel in obtei exportieren Schlüssel in obtei exportieren Schlüssel in obtei exportieren Schlüssel in obtei exportieren Schlüssel in obtei exportieren Schlüssel vertifikat wid in Kinden zortifikatspeicher Schlüssel in obtei exportieren Schlüssel in obtei exportieren Schlüssel in obtei exportieren Autrident vertifikat wid in Kinden zortifikatspeicher Schlüssel in obtei exportieren Autrident vertifikat <	Abteilung:	Seclab	
Bundesland/Kantor: Messen Land/Regior: DE To des enforderlichen Zertifikat Piese-Zertifikat Schlusseloptionen: Microsoft Enhanced Cryptographic Pooider v1.0 Schlusselenstanbieter Microsoft Enhanced Cryptographic Pooider v1.0 Microsoft Enhanced Cryptographic Pooider v1.0 Schlusselen Intel Regioner Schlussel and Schlussel Containenname Schlussel and Schlussel Containenname Microsoft Enhanced Cryptographic Pooider v1.0 Microsoft Enhanced Schlussel Containenname Microsoft Enhanced Cryptographic Pooider v1.0 Microsoft Enhanced Cryp	Stadt:	Fulda	
<form> Landrægior: De Typ des enfonderlichen Zertifikat: Pøe-Zertifikat: Schlusselpatenen: Okuena Schlusselsatz erstelle: Okumatischer Schlusselsatz erstelle: Okuena Schlusselsatz erstelle: Okumatischer Schlusselsatz erstelle: Okumatischer Schlusselsatz erstelle: Okumatischer Schlusselsatz erstelle: Okumatischer Schlusselsatz erstelle: Okumatischer Schlusselsatz erstelle: Okuen Schlussel and Exponieren: Okuen Schlussel and Exponieren erstelle: Okuen Schlussel and Exponieren erstelle: Okuen Schlussel and Exponiere erstelle: Okuen Schlussel e</form>	Bundesland/Kanton:	Hessen	
Type des enforderlichen Zertifikati Schlusseloptionen:	Land/Region:	DE	
PSec-Zertifikat Schlusseloptionen: Kryptografiedienstanbieter, Microsoft Enhanced Cryptographic Provider v1.0. Schlüsselverwendung, Exchange Signatur Beide Schlüsselgrößer, 1024 Min.: 000000000000000000000000000000000000	Typ des erforderlic	hen Zertifikats:	
Schlusseloptionen:		IPSec-Zertifikat	
Schuisselopitielei:	C.1.10		
Neuen Schusselsatz erstellen O Bestehenden Schusselsatz verwenden Kryptografiedienstanbieter: Microsoft Enhanced Cryptographic Provider v1.0 Schlüsselgroße: 1124 Min: 304 (Altgemeine Schlüsselgröße: 512 1024 2048 4008 8192 15084) O Automatischer Schlüsselcontainername Schlüssel als "Exponierbar" markieren Schlüssel in Datei exponieren Vom Benutzer angegebener Containername Schlüssel in Datei exponieren Schlüssel in Idael Tertifikatspeicher gespeicher des Benutzers. Installiert nicht iden Speicher des Benutzers. Installiert nicht iden Speicher des Benutzers. Installiert nicht iden Speicher des Benutzers. Installiert nicht des Stammzentfizinungsstellen- zentlikat. Nur Administratoren dürfen Schlüssel im kolaeln Zentlikatspeicher Wird nur zum Signieren der Anforderung verwendet. Anforderungsformat: OCMC OPKCS10 Hashalgorithmus Maci m Datei speicher Antroide: Antroide: Antroide: Antroide: Antroide: Antroide: Antroide: Antroide: Antroide: Desten: Antroide: Desten: D	Schlusseloptionen:		
Krybiogramedianstanburgter. Mitching Charlander Cryptographic Provider VI.0 Schlüsselverwendum; Exchange Osignatur Beide Schlüsselgröße: 1024 Mittil 304 Mittil gemeine Schlüsselgrößen: 152 1924 2040 4080 1932 153043 Schlüsselgröße: 1024 Mittil 304 Mittil gemeine Schlüsselgrößen: 152 1924 2040 4080 1932 153043 Schlüssel in Carl Max: 1934 Maximose Ovon Benutzer angegebener Containername Schlüssel in Datei exportieren Schlüssel als "Exportierbar" markierer] Schlüssel in Datei exportieren Schlüssel, in Datei exportieren Schlüssel als "Exportierbar" beruffikatspeicher Schlüsselerbar Zentifikat wir in dem Speicher des Benutzers. Installiert nicht das Stammerthizierungsselelenzerthizerungsselelenzerthizerungsselelenzerthizerthizers belüssel im bikalen Speicher erstellen oder verwenden. Zesatzliche Optionen: Mittil vur Zum Signieren der Anforderung verwendet. Anforderung in Datei speichern Anforderung in Datei speichern Anforderung in Datei speichern Signieren der Anforderung verwendet.	1/	Neuen Schlüsselsatz erstellen OBestehenden Schlüsselsatz verwenden	
Schlüsselerewendung: Orzkranden Organization Oreade Schlüsselgröße: 1024 Min: 1939 (Allgemeine Schlüsselgrößen: 512 1024 2040 4000 8192 150304) O Automatischer Schlüsselcontainername Orom Benutzer angegebener Containername Orom Benutzer angegebener Antor Mint nur zum Signieren der Anforderung verwendet. Antributer Orom Benutzer angegebener Anzeigename: Deinenden Deinenden	Cohlisson	dieter. Microsoft Enhanced Cryptographic Provider VI.0	
Schlusselgrote: [1024] Max: 18984 (Wigemeine Schlusselgroten: 127 (2024 2028) (2006 [1027 States)	Schlusselverwen	Idung: O'Exchange Signatur O'Beide	
Automatischer Schlüsselcontainername Ovom Benutzer angegebener Containername Schlüssel als "Exportierbar" markieren Schlüssel in Datei exportieren Schlüssel in Datei exportieren Zertifikat in lokalem Zertifikatspeicher aufbewahren Zertifikat in lokalem Zertifikatspeicher des Benutzers. Installiert nicht das Stammzettifizierungsstellen- zertifikat. Nur Administratoren dürfen Schlüssel im lokalen Speicher erstellen oder verwenden. Zestatzliche Optionen: Anforderungsformat: OCMC OPKCS10 Hashalgorithmus: SH4.1 Wird nur zum Signieren der Anforderung verwendet. Anforderung in Datei speichern Attribute: Anzeigename: Einsenden	Schlusselg	rolse: 1024 Max::16384 (Aligemeine Schlusseigroben: <u>512 1024 2040 4080 0192 16304</u>)	
Schlüssel als "Exponterbar" markteren Chlüssel als "Exponterbar" markteren Chlüssel als "Exponterbar" markteren Control Contr		Automatischer Schlüsselcontainername OVom Benutzer angegebener Containername	
Controlseen in Date exponention Controlseen in Date exponentin Controlseen in Date exponention		Schlüssel als "Exportierbar" markieren	
Zertifikat in lokalen Zertifikatspeicher aufbewahren Zertifikat wird im lokalen Zertifikatspeicher gespeichert, nicht in dem Speicher des Benutzers. Instellier nicht das Stammzertifizierungsstellen- zertifikat. Nur Administratoren dürfen Schlüssel im kokalen Speicher erstellen oder verwenden. Zusätzliche Optionen: Anforderungsformat: CMC OPKCS10 Hashalgorithmus: SHA-1 Wird nur zum Signieren der Anforderung verwendet. Anforderung in Datei speicher Attribute: Anzeigename:		Verstärkte Sicherheit für den nrivaten Schlüssel aktivieren	
Zertifikat wird im lokalen Zertifikatspeicher gespeichert, nicht in dem Speicher des Benutzers. Instellier nicht das Stammzertifikennossetellen- zertifikat. Nur Administratoren dürfen Schlüssel im lokalen Speicher erstellen oder verwenden. Zusätzliche Optionen: Anforderungsformat: OCMC OPKCS10 Hashalgorithmus: SHA-1 V Wird nur zum Signieren der Anforderung verwendet. Anforderung in Datei speichern Attribute:		Zertifikat in lokalem Zertifikatspeicher aufbewahren	
Bespeichert, nicht die Speicher des Behutzers. Instellier nicht das Speicher des Behutzers. zertifikat. Nur Administratoren dürfen Schlüssel im lokalen Speicher erstellen oder verwenden. Zusätzliche Optionen: Anforderungsformat: OCMC OPKCS10 Hashalgorithmus: SHA-1 W Wird nur zum Signieren der Anforderung verwendet. Anforderung in Datei speichern Attribute: Anzeigename: Einsenden		Zentilikat wird im lokalen Zentilikatspeicher	
zertifikat. Nur Administratoren dürfen Schlüssel im kokalen Speicher erstellen oder verwenden. Zusätzliche Optionen: Anforderungsformat: OCMC OPKCS10 Hashalgorithmus: SHA-1 Wird nur zum Signieren der Anforderung verwendet. Anforderung in Datei speichern Attribute: Anzeigename: Einsenden		gespeichert, nicht in dem Speicher des Benutzers. Installiert nicht das Stammzertifizierungsstellen-	
Zusätzliche Optionen: Anforderungsformat: OCMC OPKCS10 Hashalgorithmus: SHA-1 Wird nur zum Signieren der Anforderung verwendet. Anforderung in Datei speichern Attribute: Anzeigename:		zertifikat. Nur Administratoren dürfen Schlüssel im	
Zusatzliche Optionen: Anforderungsformat: OCMC OPKCS10 Hashalgorithmus: SHA1 V Wird nur zum Signieren der Anforderung verwendet. Anforderung in Datei speichern Attribute: Anzeigename: Einsenden		lokalen Speicher erstellen oder verwenden.	
Anforderungsformat: © CMC © PKCS10 Hashalgorithmus: SHA1 ♥ Wird nur zum Signieren der Anforderung verwendet. CAnforderung in Datei speichem Attribute: Anzeigename: Einsenden	Zusätzliche Optione	en:	
Hashalgorithmus: SHA-1 V Wird nur zum Signieren der Anforderung verwendet. Anforderung in Datei speichem Attribute: Anzeigename:	Anforderungsfo	ormat: @CMC OPKCS10	
Wird nur zum Signieren der Anforderung verwendet. Anforderung in Datei speichern Attribute: Anzeigename: Einsenden	Hashalgorith	hmus: SHA-1 💌	
Anforderung in Datei speichem Attribute: Anzeigename: Einsenden		Wird nur zum Signieren der Anforderung verwendet.	
Attribute:		Anforderung in Datei speichern	
Anzeigename:			
Anzeigename:	Attr	idote.	
Einsenden	Anzeiger	name:	
Einsenden		·	
		Einsenden	

- Klicken Sie auf Einsenden und Installieren Sie das Zertifikat anschliessend. Bestätigen Sie dabei alle Sicherheitsoptionen mit "Ja". Das Zertifikat befindet sich nun im Zertifikatspeicher des Webbrowsers.
- b) Installieren Sie das Zertifikat nun in den lokalen Zertifikatspeicher des Betriebssystems. Gehen Sie wie folgt vor:

 Navigieren Sie dazu zum Zertifikatstamm des Browsers (Internetexplorer → Extras → Internetoptionen → Inhalte → Zertifikate) und exportieren Sie das zuvor erstellte Zertifikat. Wählen Sie im Export-Assistenten die folgenden Einstellungen:

BSc. AI, WI MSc. AI

MSc. EB

VPN

Zertifikatsexport-Assistent					
Privat en Schlüssel exportieren Sie können den privaten Schlüssel mit dem Zertifikat exportieren.					
Private Schlüssel sind kennwortgeschützt. Wenn Sie den privaten Schlüssel mit dem ausgewählten Zertifikat exportieren möchten, müssen Sie auf einer der folgenden Seiten ein Kennwort eingeben. Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren? ③ Ja, privaten Schlüssel exportieren ④ Nein, privaten Schlüssel nicht exportieren					
< Zurück Weiter > Abbrechen					
Export dateiformat Zertifikate können in verschiedenen Dateiformaten exportiert werden.					
Wählen Sie das gewünschte Format:					
DER-codiert-binar X.509 (.CER)					
Base-64-codiert X.509 (.CER)					
 Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B) Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen 					
Privater Informations austausch - PKCS #12 (.PFX)					
Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen					
Verstärkte Sicherheit aktivieren (IE 5.0, NT 4.0 SP4 oder höher erforderlich)					
Privaten Schlüssel nach erfolgreichem Export löschen					
< Zurück Weiter > Abbrechen					

• Vergeben Sie ein beliebiges Passwort, um die unbefugte Verwendung des Zertifikates zu verhindern und speichern Sie das Zertifikat auf dem Desktop ab.



• Starten Sie die Zertifikatskonsole vom Desktop aus und importieren Sie das Zertifikat.

🚡 Konsolenstamm\Zertifikate (Lokaler Computer)\Eigene Zertifikate								
C Korsolenstamm Ob		Oby	#ityp					
🖻 🞒 Zertffkate (Lokaler Computer)			In deser Angrit worden kaine Elemente angeheint					
E Constra	Zertifikate suchen		The design which is we don not be contained on group.					
E 🖸 Organ	Allo Tasks	F	Zertifikate suchen					
E - Vertra	Ansicht	•	Neues Zertifikat anfordern					
🗄 🧰 Mate s	Neues Fenster		Importieren					
B-Condition B-Condition B-Condition SPC	Neue Taskpadansicht							
	Aktualisieren Liste exportieren							
	Hife							
< 0	3	<	11	>				
Fügt einem Speicher ein Zertifikat hinzu.								

- Kopieren Sie zum Schluss das Root Zertifikat (Verwendungszweck: <Alle>) von "Eigene Zertifikate/Zertifikate" nach "Vertrauenswürdige Stammzertifikate/Zertifikate"
- c) Die Zertifikate müssen nun auch auf dem Server nach "Eigene Zertifikate" importiert werden, damit sich der VPN-Client mit diesem authentifizieren kann. Das Zertifikat müsste bei einem produktiven Einsatz natürlich im Firmennetz verteilt werden, wo Zugriff zu dem Server besteht, um es dann für die VPN Verbindung von extern nutzen zu können.

Kopieren Sie das Zertifikat auf den Server und importieren Sie es dort (Verwenden Sie den Freigabe-Ordner auf dem Desktop des VPN-Client)

d) Starten Sie die VPN-Verbindung (wie in Aufgabe 1b) und sehen Sie sich die Verbindungseigenschaften auf dem Client erneut an. Was hat sich verändert? Ist die Verbindung nun sicher (Begründung)?