VŠB - TECHNICKÁ UNIVERZITA OSTRAVA
FAKULTA ELEKTROTECHNIKY A INFORMATIKY
KATEDRA TELEKOMUNIKAČNÍ TECHNIKY

Technické zajištění pro výuku kurzů bezpečnosti počítačových sítí

2008 Miroslav Solodujev

Zadání

Téma:	Technické zajištění pro výuku kurzů bezpečnosti počítačových sítí
Diplomant:	Miroslav Solodujev
Vedoucí:	Ing. Petr Grygárek, Ph.D.
Akad. rok:	2007/2008
Obor:	2612R025 Informatika a výpočetní technika

Zásady pro vypracování:

Cílem práce je navrhnout vybavení laboratoře a materiály pro výuku kurzů bezpečnosti počítačových sítí formou série ověřených laboratorních úloh včetně přípravy ukázkových konfiguračních souborů pomocných síťových serverů a služeb.

1. Roztřiďte úlohy z kurzu Network Security I programu Cisco Networking Academy podle platformy (IOS/PIX), prakticky ověřte a opravte případné chyby. Místo nevyhovujících úloh navrhněte vlastní se stejnou tématikou.
2. Ověřte úlohy pro Cisco PIX na zařízení ASA, zdokumentujte rozdíly.
3. Nainstalujte server RADIUS, připravte iniciální konfiguraci a ověřte na něm úlohy na autentizaci, účtování 802.1x.
4. Nainstalujte server TACACS+, připravte iniciální konfiguraci a ověřte na něm úlohy na autentizaci, autorizaci a účtování.
5. Nainstalujte Syslog server, připravte iniciální konfiguraci a ověřte na něm úlohy na logování.
6. Nalezněte vhodné utility pro praktické ověřování reakce na pokusy o narušení sítě u příslušných úloh.
7. Nainstalujte NTP server a připravte vhodnou konfiguraci.
8. Nainstalujte a vytvořte iniciální konfiguraci pro běžné služby, na kterých bude možné zabezpečení sítě testovat(WWW,FTP apod).
9. Nainstalujte server s vhodnou emulací instancí Linuxu (např. User-mode Linux) pro simulaci serverů služeb. Jednotlivé simulované stroje budou přístupné prostřednictvím VLAN a budou hostovat servery služeb zmíněných výše.

Čestné prohlášení

Podepsaný Miroslav Solodujev tímto čestně prohlašuje, že svou Bakalářskou práci vypracoval samostatně na základně odborných konzultací, s využitím uvedené literatury a poznatků získaných v průběhu bakalářského studia.

V Ostravě dne 20.8.2008

……..

Podpis

Poděkování

Rád bych poděkoval panu Petru Grygarkovi za pomoc, laskavý přístup a trpělivost při tvorbě mé práce. Dále bych poděkoval všem instruktorům RCNA na VŠB za jejich ochotu dělit se a rozšiřovat jejich hluboké znalosti.

Abstrakt

V této bakalářské práci se zabývám technickou přípravou vyučování kurzu Network Security 1 v rámci RCNA (Regionální Cisco síťová akademie).Popisuji nastavení a použití firewallu, autentikace,autorizace a účtování uživatelů, zabezpečení Cisco prvku, překlad IP adres, bezpečné přihlášení a logování. Prakticky ověřuji, rozšiřuji a nově vytvářím cvičení společnosti Cisco, pomocí kterých si studenti mohou ověřit své teoretické znalosti v praxi.

Klíčová slova

Security, Firewall, IOS, AAA, Cisco, Network Security 1, NS1

Abstract

This bachelor thesis focuses on the technical preparation of the Network Security 1 learning materials as part of RCNA (Regional Cisco Networking Academy) course. The following features are described: functioning and usage of the firewall, authentication, authorization, accouting users, Cisco elements protection, IP address translation, secure access and logging. The practical part of the thesis includes verification, extension and preparation of new practical tasks for Cisco Academy, which enable the students to check their theoretical knowledge.

Key words

Security, Firewall, IOS, AAA, Cisco, Network Security 1, NS1

Obsah

Obsah

1 Úvod

Tuto bakalářskou práci jsem si vybral protože se delší čas zabývám počítačovou bezpečností. Pracuji v týmu, který se počítačovou bezpečností zabývá a chtěl jsem si rozšířit znalosti co se týče Cisco prvků a náhledu na sítě.

Při studiu bakalářského oboru jsem se v předmětu Počítačové sítě seznámil s Petrem Grygárkem, který tento předmět učil. Jeho práce mě zaujala natolik, že jsem se přihlásil na kurz regionální Cisco Akademie CCNA, který trvá 2 roky a počítačové sítě jsou zde probrány hlouběji. Byl jsem mile překvapen kvalitou Cisco instruktorů a stylem učení, kde kapitoly mají jasnou strukturu, cvičení a na závěr pokaždé test, který donutí studenty průběžně studovat.

Další kurzy Network Security, byly pro mě jasná volba, ale narozdíl od aktuálních a propracovaných kurzů CCNA, byly NS kurzy zastaralé a mnohdy zmatené a na průměrně starých cisco prvcích nepoužitelné. Dále se zaměřovali na cisco Access Control Server, který je pro akademické použití naší školy neúměrně drahý. Také bych zmínil, že cvičení jsou psané pro PIX verzi 5.0/6.0, který se dnes používá velmi zřídka a byl převážně nahrazen ASA zařízením, které má odlišnou syntaxi.

Cílem mé práce je přepsat, rozšířit nebo popřípadě vytvořit nové cvičení na ASA zařízení a IOS. Nahradit Cisco Access Control Server opensource řešením v podobě TACACS+ a freeradius serverů. Dále vytvořit distribuci linuxu, kde bude možné ověřit a použít DNS, FTP, HTTP, HTTP, TFTP, TELENT, SSH, SYSLOG, NTP služby a dále by měla obsahovat penetrační nástroje pro ověření Cisco IDS/IPS vlastností a zabezpečení druhé OSI vrstvy. K tomuto účelu jsem mi vybral NESSUSS, NIKTO, NMAP, YERSINIA nástroje. A dále, zde také nainstalovat server s vhodnou emulací instancí Linuxu.

2 Bezpečnost počítačových sítí

V této kapitole se budu snažit objasnit hodnotu počítačové bezpečnosti v dnešní době a běžnou realitu.

2.1 Stále podceňované odvětví

Není pochyb o tom, že počítačová bezpečnost je stále podceňovaným oborem. Hlavním důvodem je, že pokud funguje tak o tom nikdo neví a hlavně nejdou vidět hmatatelné zisky. Dále je to kvůli neinformovanému vedení společností, kteří se této problematice nevěnují nebo ji prostě nerozumí a berou investici do bezpečnosti počítačové sítě jako nutné zlo.

2.2 Obecně o obraně

Problém obránce je ten, že potřebuje znát veškerá fakta a možnosti. Například ve středověku válečný inženýr musel znát jak má udělat hradby, kolik věží, jak rozmístit a střídat stráže a spoustu další věcí. Zatímco útočníkovi stačila jen jediná informace, že na 10km zdi je v jednom místě porušena cihla (vznikla díra) a že hlídky se mění v 22.00 večer a mohl proniknout velmi složitým systémem zabezpečení. Samozřejmě, že to platí i dnes v počítačové síti.

2.3 Běžná realita výchozích nastavení

Většina předních výrobců ještě dnes stále používá filozofii, že bezpečnost je zodpovědností uživatele, který si od nich produkt kupuje, tzn. že své výchozí nastavení produktů je úplně nezabezpečené a všechny služby puštěné. Je to logické, když výrobce neví, pro jaký druh použití si ho pořizují a mělo by být vše funkční. A jelikož je bezpečnost tak široký a složitý okruh jen málo uživatelů si systém kvalitně zabezpečí. A vzhledem k tomu, že je malé povědomí o možných rizicích je na internetu spousta totálně nezabezpečených počítačů, systému jak firemních tak koncových uživatelů (výchozí hesla, puštěné nepoužívané servisy atd.)

2.4 Bezpečnostní vrstvy

Existuje široká škála technologií a vrstev a každá by se měla zabezpečit. Je spousta front na kterých se musí bojovat od sociálního inženýrství, kde vám lidé jednoduše lžou tak, že jim uvěříte a neproškolený zaměstnanec řekne své heslo (průkopník Kevin Mitnick,, nebo v Evropě Raoul Chiesa – vznikl z toho vědní obor), fyzické zabezpečení, zálohy až po aplikační vrstvu.

Dnes se začíná prosazovat systém zvaný defence-in-depth, což jednoduše znamená propojit a nastavit všechny vrstvy tak, aby po selhání jedné vrstvy nepřevzal útočník kontrolu nad systémem, ale aby byl zachycen vrstvou další.

2.5 Vyhodnocení rizik a kompromis mezi svobodou a bezpečností

Každá společnost by měla mít zhotoven tzn. Risk Assesment, kde určí obecně kritické systémy (ne pouze počítačové) a vyhodnotit jaké ztráty a kolik prostředků by museli vynaložit na obnovení původního stavu. Na tomto základě vytvořit bezpečností politiky a aplikovat je na všech zmíněných vrstvách. Což v praxi znamená jestli má uživatele „otravovat“ autentikaci při vstupu do budovy, kolikrát měsíčně si musí měnit heslo, jestli se může připojit do systému z domu atd.

2.6 Běžné povědomí lidí a firem a internetová realita

Běžné povědomí je – „proč bych měl systém zabezpečovat? Já (náš systém) není pro útočníka zajímavý“ – Taková bláhovost! V dnešní době informací, je právě nejcennější informace. Většina seriózních průzkumů například zjistila, že si to myslí většina středních firem v EU (1000-2000 zaměstnanců), ale přesto více jak 2/3 byli napadeny 2x za rok. Stejně tak je zveřejněno pouze cca. 1/10*[1]* všech průniků (banky ještě méně – kdo by se pyšnil děravým e-bankovnictvím a dělal si velice špatnou reklamu?).

Můžeme si představit, že jsme zloději a pouze chodíme po bytech a zkoušíme jestli má uživatel zamknuté dveře, je docela možné, že když budeme šikovní tak se nám podaří obejít 100 bytů za den. Ale představte si, že pomocí internetu máte na dosah vaší ruky 1,450000000 uživatelů*[2]* a během sekundy umíte zkontrolovat 100 možná 1000 dveří. Když znáte nejznámější používané systémy a jejich výchozí nastavení.,tak můžete mít během dne 100 počítačů pod vaší kontrolou. Dále existují známé bezpečnostní díry a zveřejnění exploity (programy které tyto díry zneužívají). Tzn., že můžete ověřit množství systému a když mají díru, tak pouze spustit automatický skript.

Také když budete chodit po bytech tak si Vás brzy někdo všimne a zavolá policii, ale na internetu je velice složité právo a když získáte počítač v Brazílii nebo v Číně tak můžete legálně skenovat a myslím, že taky útočit (lámat zámky) a nikdo se vaším pc zabývat nebude.

Z napadených počítačů se dělají botnety, používají se na DDoS (distribuované odepření služby), vykrádají se soukromé informace jako funkční emailové účty (všech lidí z adresáře), čísla funkčních kreditních karet, certifikáty atd., pak se s těmito informacemi obchoduje na černých burzách. Dokonce se prodává systém jménem Mpack, který vyvíjí Ruští „informatici" a vy si pouze určíte jaký webový server chcete napadnout a jaké informace o uživatelech chcete a oni vám to nastaví, provedou a dokonce si můžete zaplatit roční servis, což znamená, že když nějaký antivir příjde na to, že z onoho napadeného serveru stahujete viry tak ho upraví tak, že je opět nedetekovatelný

Dneska není cílem být vidět, udělat nějaký vir, který většinu počítačů restartuje, ale napadnout systém, udělat zadní vrátka o odesílat citlivé informace a hlavě být nenápadný, proto mnoho lidí ani netuší, že jsou napadení, nebo, že jejich počítač byl použitý k útoku, možná si jenom říkají „dneska je ten internet nějaký pomalý"

Za rok 2007 v USA překročila počítačová kriminalita zisky z prodeje drog!

2.7 Příklad útoku

Kdybych chtěl získat informace o cílové skupině studentů FEI VŠB, tak bych se zaměřil na webový server, který používá většina zaměstnanců a studentů. Velice rychle bych zjistil, ze používá mysql admin a zneužil bych jeho zranitelnost nebo běžným SQL injection bych přidal to zdrojové stránky vlákno, které by uživatele skrytě přesměrovalo na určený webový server. Tento server bych opatřil pár zero-dey exploity (zatím neopravené chyby), které by se na jakémkoliv webovém prohlížeči s podporou javascript spustily (dnes je javascript nutnost na 99,9% uživatelů ho má spuštěn), existuje pár zemí kde si můžete zřídit anonymní web s podporou php třeba na měsíc. Pak z napadených počítačů shromažďoval hesla, čísla karet, na jaké internetové stránky chodí atd.

60 ze 100 nejpopulárnějších webů byly za rok 2008 napadeny *[3]*

3 Systémové služby

Část zadání byla připravit vhodnou distribuci Linuxu, na které poběží služby požadované ve cvičeních cisco network security. V budoucnu se počítá se zařazením této image do virtlabu (6.1.2) a proto by měla obsahovat také běžné služby, které se běžně s Cisco prvky používají.V této kapitole se stručně o nich zmíním.

3.1 Telnet

Telnet je již mnoho let používaný, relativně jednoduchý internetový protokol pro terminálové připojení na bázi příkazové řádky. Umožňuje uživateli přihlásit se ke vzdálenému počítači podobným způsobem, jakoby seděl u jeho terminálu. Po připojení Telnet klientem k serveru s běžícím Telnet démonem (zpravidla naslouchá na TCP portu 23) je uživatel dotázán na své přihlašovací jméno a heslo. Jakmile je uživateli povolen přístup, je mu zpřístupněna příkazová řádka (konzole) hostitelského systému, se kterou může dále běžným způsobem interaktivně pracovat – zadávat příkazy, spouštět programy atd.

Chování mnoha dalších protokolů (např. HTTP) je založeno na chování protokolu Telnet..

3.1.1 Bezpečnost protokolu Telnet

Protokol Telnet není považován za bezpečný protokol především pro jeho dva hlavní nedostatky.
Největším problémem je přenos dat v nešifrované podobě, včetně jména a hesla přihlašovaného uživatele. To dovoluje komukoliv, kdo má přístup k zařízením přes něž data procházejí, zachytávat přenášená data, zjistit uživatelovo jméno a heslo a použít tyto získané informace k nežádoucím účelům.

Druhým nedostatkem je nemožnost zajistit, že spolu opravdu komunikují dvě míněné strany. Komunikaci může napadnout útočník uprostřed, měnit přenášená data, nebo se vydávat za některou ze stran.

Problémem je také množství bezpečnostních děr v některých Telnet démonech. Většina chyb je již opravených, mohou však ještě existovat další.

Díky těmto bezpečnostním nedostatkům se protokol Telnet již pro vzdálené přihlášení uživatele k serveru příliš nepoužívá. Nahrazuje jej protokol SSH, který nabízí přinejmenším stejné možnosti jako Telnet, navíc poskytuje mnohem vyšší úroveň zabezpečení.

3.2 SSH

Z toho důvodu nízké úrovně bezpečnosti protokolů Telnet, rsh, rlogin a rcp byl v roce 1995 navržen protokol SSH (Secure Shell), určený jako jejich náhrada. Hlavní důraz při vývoji SSH byl kladen na bezpečnost. V roce 1997 byla sdružením IETF navržena verze 2, která řešila některé bezpečnostní problémy a rozšiřovala možnosti protokolu SSH

3.2.1 SSH verze 1

Protokol SSH verze 1 je dnes již poměrně zastaralý a nedoporučuje se jej používat, i když jsou s ním SSH servery zpravidla zpětně kompatibilní. Trpí několika bezpečnostními problémy, které umožňují útočníkovi například převzít spojení.
Šifrovací klíč se přenáší bezpečnou asymetrickou šifrou (RSA), samotná data jsou pak šifrována rychlým symetrickým algoritmem (např. IDEA nebo DES). Klíč sezení se každou hodinu obměňuje. Autorizace uživatele může být provedena podle uživatelova hesla nebo veřejného klíče.

3.2.2 SSH verze 2

SSH verze 2 přináší významné změny, protokol SSH již není tvořen jedinou vrstvou, ale je rozdělen na tři hlavní vrstvy, z nichž každá je ve specifikacích IETF popsána zvlášť. Vylepšena byla zejména bezpečnost protokolu. SSH2 také povoluje další možnosti autorizace uživatele, například pomocí systému Kerberos, certifikátů X.509 nebo elektronických kreditních karet. V rámci jednoho SSH spojení umožňuje SSH2 současný běh několika konzolových sezení.

3.3 HTTP

Protokol HTTP (HyperText Transfer Protocol) je základní metodou zveřejňování webových stránek na internetu. Byl vyvinut ve spolupráci WWW konsorcia a pracovních skupin IETF za účelem poskytnout cestu k publikaci HTML stránek.

Základní princip jeho funkce je, že se webový prohlížeč na straně klienta připojí na webový server, vznese požadavek na určitý dokument (HTML soubor, obrázek atd.) a pokud je dokument nalezen, je klientovi předán jako součást odpovědi serveru. Pokud je požadovaným dokumentem proveditelný skript, je na serveru spuštěn metodou definovanou v konfiguračních souborech HTTP serveru a klientovi je předán výstup skriptu.

Využitím protokolu HTTP lze nejen prohlížet domovské webové stránky uživatelů, ale je možno je i spravovat. Na webovém serveru bude pro tento účel umístěna webová aplikace, nejčastěji napsaná v některém skriptovacím jazyce jako PHP, ASP nebo Perl. Výstupem webové aplikace je text v jazyce HTML, zobrazitelný webovým prohlížečem na straně klienta. Pomocí interaktivních prvků umístěných v hypertextovém dokumentu, jako jsou odkazy a formuláře, může uživatel webovou aplikaci ovládat. Podporované funkce pro správu souborů domovských stránek závisí na implementaci webové aplikace a způsobu, jakým k souborům přistupuje. Soubory je možno přenášet přes HTTP oběma směry, většinou se ale nepřenáší více souborů najednou v jednom požadavku. Pro upload mnoha souborů je vhodnější použít protokol určený pro práci se soubory, například FTP nebo SFTP..

3.4 HTTPS

Data přenášená protokolem HTTP nejsou šifrována a podobně jako protokol Telnet nenabízí HTTP žádné bezpečnostní mechanismy. Útočník schopný zachytit přenos tedy může odposlouchat přihlašovací jména i hesla, čísla účtů, nebo jiné důvěrné informace. Proto byl společností Netscape navrhnut protokol HTTPS jako zabezpečená obdoba protokolu HTTP, poskytující především autentifikaci a šifrování přenosu dat. Přenos už neprobíhá ve formě čistého textu, ale je šifrován pomocí protokolu SSL nebo TLS. Implicitním portem protokolu HTTPS je TCP/IP port 443. Pokud chce uživatel, používající webový prohlížeč, přistoupit k webové stránce pomocí protokolu HTTPS, znamená to pro něj, že zadá URL adresu začínající písmeny „https://“místo „http://“.

Protokol HTTPS by měl být použit všude, kde se přenáší citlivé údaje. Bohužel dnes ještě velké množství webových serverů HTTPS nepodporuje a uživatel musí často riskovat únik informací při použití nechráněného protokolu HTTP.

3.5 Freeradius

Jedná se o open source RADIUS (Remote Authentication Dial In User Service) server. RADIUS protokol je AAA (authentication, authorization, accounting) protokol, který umožňuje ověřování uživatele, který se připojuje k síti, síťovým prvkům apod.

Jedná se o protokol klient/server. RADIUS server autentizuje a autorizuje vzdálené uživatele pro přístup do systému. RADIUS server také rozhoduje o zpřístupnění služby (například připojení do sítě). RADIUS klient je zodpovědný za odesílání uživatelských informací

určenému RADIUS serveru a zpracování odpovědí, které RADIUS server vrátí. Oficiálně přidělené číslo portu pro RADIUS je 1812.
Mezi nejdůležitější rysy patří jeho vysoká síťová bezpečnost. Transakce mezi klientem a RADIUS serverem je autentizována pomocí sdíleného tajemství, které není nikdy posíláno přes síť. Navíc všechna uživatelská jména jsou přes sít zasílána šifrovaně (šifrování se sdíleným heslem symetrickým algoritmem), a tím je eliminována možnost vysledování nechráněného hesla na síti.

Jako tlumočník mezi uživatelem "toužícím" po přístupu do sítě a RADIUS serverem slouží RADIUS klient (přístupový server, fyzicky Access Point nebo switch). RADIUS server zpracovává požadavek ve 2 krocích - ověření a autorizace. Ověřením zkontroluje identitu uživatele, tedy porovná údaje ve své databázi se zaslanými údaji. Po úspěšném ověření dojde k autorizaci, která rozhoduje, jaké služby budou uživateli zpřístupněny. RADIUS server může také působit jako prostředník (proxy klient) pro jiné RADIUS servery nebo i ostatní typy autentizačních serverů.*[6]*

3.5.1 Nastavení

Pro konfiguraci nás budou zajímat dva soubory

clients.conf – kde přidáme síť, na které budeme naslouchat a určíme klíč pro autentikaci se klientem

```
client 192.168.100.0/24 {
  secret    = cisco
  shortname = cisco
  nastype = cisco
}
```

users – kde nastavíme typ a vlastnosti připojení uživatele

raduisuser Auth-Type:=Local, - použití lokální databáze uživatelů

raduisuser Auth-Type:=Systeml, použití databáze uživatelů v systému (linux účty)

raduisuser Auth-Type:=EAP, -typ pro 802.1x autentizaci při použití lokální databáze

"$enab15$" Auth-Type:=Local – dále určení hesla pro enable mód

Ladící mód – kde můžeme sledovat podrobnou komunikaci s klientem na obrazovce:

freeradius –X

3.6 TACACS+

Tato zkratka znamená (Terminal Access Controller Access-Control System) je vzdálený autentikační protokol používaný ke komunikaci s autentikačním serverem často používaný v UNIX sítích. TACACS umožňuje vzdálenému přístupovému serveru komunikovat s autentikačním serverem, aby se rozhodlo, zda má uživatel přístup k síti.

TACACS umožňuje klientu přijmout uživatelské jméno a heslo a poslat požadavek na TACACS autentikační server, někdy zvaný TACACS démon nebo jen TACACSD. Tento server rozhodne zda přijmout nebo zamítnout požadavek a pošle zpět odpověď. Takto je rozhodovací proces otevřený a algoritmy a informace k němu použité jsou zcela na tom, kdo provozuje TACACS démona.

Novější verze TACACS od roku 1990 byly nazývány XTACACS nebo extended (rozšířený) TACACS. Obě verze již byly většinou nahrazeny novějšími protokoly TACACS+, RADIUS nebo DIAMETER. TACACS+ je zcela nový protokol, který není zpětně kompatibilní s protokoly TACACS nebo XTACACS.

TACACS je definován v RFC 1492 a používá buď TCP nebo UDP a standardně port 49.[7]

3.6.1 Nastavení

Konfiguruje se souborem **tac_plus.conf**

Kde můžeme nastavit klíč pro šifrování, účtovací soubor a hlavně vlastnostmi uživatelských účtu a skupin.

key = cisco - nastavení klíče pro šifrování

accounting file = /var/log/tac_plus/tacacs – soubor pro logování – je třeba ho první vytvořit a přiřadit mu příslušná práva

user = admin { -vytváříme uživatele admin s heslem admin a povolením všech služeb

default service = permit

login = cleartext "admin"

}

3.7 DHCP

DHCP je obecně uznávaný standard; celý název, který zní Dynamic Host Configuration Protocol, což se běžně překládá jako "protokol pro konfiguraci síťových hostitelů", napovídá, že 'umí' konfigurovat parametry TCP/IP jednotlivých klientů serveru. Je tedy nezávislý na použitém OS (pokud ho ten samozřejmě podporuje) a celý je definován a upřesňován několika dokumenty RFC (seznam je třeba na adrese http://www.ietf.org/iesg/1rfc_index.txt). Vychází z protokolu BootP, se kterým je zpětně kompatibilní a vylepšuje ho o mnoho nových a užitečných vlastností. Server DHCP můžeme tedy klidně nasadit i pro klienty protokolu BootP, ovšem připravujeme se tím o mnoho výhod, namátkou třeba o proklamovanou dynamičnost.

Dynamičnost v tomto případě znamená, že adresy a vůbec informace distribuované serverem DHCP klientům nejsou přidělovány staticky, napořád, ale jen na určitou stanovenou dobu. Po této době klient adresu vrátí, nebo obnoví (typicky po půli pronajaté doby). Umožňuje to ekonomicky hospodařit s adresním prostorem a usnadňuje to konfiguraci hlavně u větších sítí a mobilních zařízení.

Kromě IP adresy může DHCP server přidělovat například i masku sítě, implicitní bránu, DNS servery, jméno hostitele a domény, může hostitelům vnutit chování podle určitých norem, 'změnit' jeho MAC adresu, informovat ho o SMTP, POP, time a dalších serverech, zapnout, nebo vypnout IP forwarding, bezdiskovým stanicím určí cestu k bootovacímu obrazu, apod.

V případě potřeby samozřejmě můžeme pomocí DHCP nastavit určité stroje staticky, typické je to například pro počítače poskytující určité služby: web server, SMTP server, router apod. Usnadňuje se tak nejen přístup k samotným službám, ale i vzdálená konfiguraci jednotlivých serverů.

Jak vidno, zprovozněním serveru DHCP získáme silný nastroj pro centrální správu, a notně si tak ušetříme práci.*[8]*

3.7.1 Nastavení

Pro naše použití bude stačit základní nastavení

Nasvavíme /etc/dhcpd3/**dhcp.conf;**

option domain-name "cisco.com";nastávíme doménové jméno
option domain-name-servers 172.16.0.1;;zvolíme name-server
option routers 172.16.0.1;;určíme výchozí bránu
default-lease-time 3600;;set lease time in secound
subnet 172.16.0.0 netmask 255.255.255.0 {;požadovaná síť
arrange 172.16.0.2 172.16.0.30;;určení přidělovaného rozsahu IP adres

}

3.8 NTP

Network Time Protocol (port 123 udp a pro trasování také tcp) používající mj. 64bitové časové značky ve formátu čísla s pevnou řádovou čárkou je již mnohem sofistikovanější a složitější než Time, ale také přesnější. Je přímo určen pro trvalou synchronizaci hodin více počítačů po síti. Filozofie protokolu NTP spočívá v tom, že se nesnaží synchronizovat hodiny počítačů navzájem (tedy nesnaží se čas jaksi "zprůměrovat"), ale synchronizuje je oproti času UTC ("Universal Time Coordinated").

Synchronizované servery jsou to postaveny do hierarchické několika úrovňové stromové struktury, díky které lze rozložit zátěž a distribuovat službu NTP podle potřeb uživatelů. V nejvyšší vrstvě jsou vlastní časová zařízení (atomové hodiny, GPS, hodiny řízené časovým signálem, atp.) Každý server je v určité vrstvě (stratum), přičemž ve vrstvě číslo jedna (stratum-1) je server, který je připojen na nějaké externí časové zařízení (stratum-0). Jeho "potomci" (např. ve druhé, třetí nebo čtvrté vrstvě) se považují za méně přesné.

Primárních serverů (stratum-1) bylo na světě v roce 1999 cca 230, sekundárních (stratum-2) pak něco přes 100.000 a jejich počet neustále roste. Vlastníci primárních serverů obvykle omezují, kdo se k nim smí připojovat. Poskytovatelé internetových služeb mají zpravidla vlastní servery stratum-2, odchylka těchto sekundárních serverů od primárních je zanedbatelná a servery této úrovně se nejvíce používají pro synchronizaci času. Menší firma si jistě založí jeden nebo více serverů na úrovni stratum-3 a klientské stanice, které se s nimi budou synchronizovat, pak budou na úrovni stratum-4. Obecně platí, že čím vyšší úroveň (nižší číslo), tím je zaručena vyšší přesnost a menší tolerance, ale vzhledem k tomu, že velmi záleží také na parametrech síťového připojení, je nejrozumnější synchronizovat se podle topologicky blízkého stroje, i kdyby byl nižší úrovně. Přestože NTP stanoví maximální možný počet vrstev

na 15, již pátá vrstva se vyskytuje pouze výjimečně a nejvíce počítačů se nachází ve třetí vrstvě (tj. synchronizují se podle serveru úrovně stratum-2).

Principiálně rozlišujeme několik základních vztahů mezi jednotlivými "účastníky" synchronizačního procesu:

- **Server a klient** - Server poskytuje klientům na požádání přesný čas s doplňujícími informacemi (svoji vrstvu, přesnost času atd.). Naopak klient získává přesný čas od jednoho či více serverů, a to k synchronizaci svých vlastních hodin.
- **Peer** - Jde minimálně o dvojici strojů, které si navzájem vyměňují informace o přesném čase, a vždy ten z nich, který má nejpřesnější čas, je server a ostatní klienti - nemusí být tedy stanoven jeden fixní server.
- **Broadcast / multicast server a klient** - Server vysílá v pravidelných intervalech informaci o čase na broadcastovou či multicastovou adresu. Při vysokém počtu klientů tak může dojít ke značnému ušetření síťových i výpočetních prostředků. Naopak klient přijímá informace o přesném čase a navíc může využít pravidelné vysílací periody k lepší synchronizaci.

Protokol NTP používá sofistikované algoritmy zohledňující vlastnosti protokolů z rodiny UDP/IP, topologickou vzdálenost serverů (čas, který uplyne od vyslání údaje k jeho přijetí), eliminují síťový jitter a další statistické chyby. Přitom platí pravidla, jak měnit místní čas: Je-li odchylka příliš vysoká, považuje se za nepravděpodobnou chybu a čas se synchronizovat nebude. Je-li naopak přijatelná, budou se systémové hodiny mírně zrychlovat nebo přibrzďovat o malou hodnotu. Proto také úvodní synchronizace nějakou dobu trvá, řádově několik minut. Přesnost synchronizace tímto protokolem je v řádu desetin milisekundy.Základním přenosovým protokolem je UDP. Popis protokolu NTP pak lze nalézt v dokumentu RFC-1305.*[9]*

3.9 Syslog

Většina systémových služeb, programů a utilit provádí tzv. logování, tedy zapisuje informace o své činnosti do textových souborů s tím, že zpravidla přidává nové řádky na jeho konec. Takže program zaznamená své spuštění, příkazy, problémy a příčiny, proč nemohl udělat to či ono. Logování v Linuxu je velmi propracované a dotažené téměř k dokonalosti. Soubory s logy můžete najít především v adresáři **/var/log**, ale některé programy mají své vlastní logovací soubory. Jejich umístění najdete v manuálu k programu.
Logování lze nastavit přesně podle potřeb. Můžete veškerá data okamžitě zahazovat, periodicky mazat, logy můžete rotovat a po určitou dobu je skladovat, nebo třeba komprimovat, archivovat na zálohovací médium či přeposílat na jiná místa své sítě.

4 Penetrační nástroje

Součástí práce bylo najít vhodné testovací nástroje, aby mohli studenti otestovat slabiny operačních systému, systémových a Cisco služeb. Tyto nástroje by měli být součástí připravované Linuxové distribuce. V této kapitole je stručně představím a vysvětlím použití.

4.1 Nessus

Použitý nessus verze 2 je GPL a funguje na bázi klient – server. Je to nejznámější vulnerability skener zdarma. Obsahuje okolo 2700 různých pluginů*[4]* které testují tyto kategorie:

AIX Local Security
Backdoors (trojské koně)
CGI zranitelnosti
CGI zranitelnosti XSS
CISCO
Databáze
Debian Lokální Security Audit
Default Unix Acounts
Denial od Service
FTP server
Zranitelnosti služby Finger
Firewaly
GPL Feed
Vzdálené získání shell
Vzdálené získání root
Gentoo Lokální Security Audit
MacOS Lokální Bezpečnostní Audit
Netware
Peer-To-Peer sdílení souborů
RPC
Red Hat Lokální Security Audit
Remote File Aceess (vzdálený přístup k souborům)
SMTP problémy
SNMP
Useless Servers (Nepotřebné služby)
Webové servery
Windows.

4.2 Nmap

Je nejznámější a nejpropracovanější skener portů, který zvládá desítky různých technik a má databázi 1500 služeb. Umí také docela slušně hádat operační systém a umí různé druhy skenování od pomalého nedekovatelného až po agresivní prohledávání rozsáhlých sítí.

4.3 Nikto

Jedná se o open source GPL webový skener, který umožňuje důkladný test webového prostředí, obsahuje databázi, kde je okolo 3500 záznamu o nebezpečných souborech, 900 verzí serveru, 250 konkrétních problémech na webovém serveru.

4.4 Yersinia

Tento cisco penetrační nástroj vyšel ve známost na konferenci BlackHat v Americe kde ho uvedl Michael Lynn, který v té době pracoval pro společnost, kterou si najalo Cisco na testování svých zařízení. Jelikož byl Michael rozhořčen postojem Cisco společnosti, které své bezpečnostní díry tutlalo a více než rok nespravovalo, tak vše zveřejnil a Cisco prvky na konferenci úplně znemožnil. Na to samozřejmě dostal ihned výpověď, ale tuším, že přešel do Juniperu.

Tento nástroj se zaměřuje na zranitelnosti Cisco služeb a obsahuje tyto možnosti:

Spanning Tree Protocol

1. Sending RAW Configuration BPDU
2. Sending RAW TCN BPDU
3. DoS sending RAW Configuration BPDU
4. DoS sending RAW TCN BPDU
5. Claiming Root Role
6. Claiming Other Role
7. Claiming Root Role dual home (MITM)

Cisco Discovery Protocol

1. Sending RAW CDP packet
2. DoS flooding CDP neighbors table
3. Setting up a virtual device

Dynamic Host Configuration Protocol

1. Sending RAW DHCP packet
2. DoS sending DISCOVER packet (exhausting ip pool)
3. Setting up rogue DHCP server
4. DoS sending RELEASE packet (releasing assigned ip)

Hot Standby Router Protocol

1. Sending RAW HSRP packet
2. Becoming active router
3. Becoming active router (MITM)

Dynamic Trunking Protocol

1. Sending RAW DTP packet
2. Enabling trunking

802.1Q

1. Sending RAW 802.1Q packet
2. Sending double encapsulated 802.1Q packet
3. Sending 802.1Q ARP Poisoning

802.1X

1. Sending RAW 802.1X packet
2. Mitm 802.1X with 2 interfaces

VLAN Trunking Protocol

1. Sending RAW VTP packet
2. Deleting ALL VLANs
3. Deleting selected VLAN
4. Adding one VLAN
5. Catalyst crash

5 Vytvoření distribuce Linuxu a instalace služeb

Součástí této práce bylo vytvoření Linuxové distribuce, která bude součástí Cisco cvičení a počítá se s jejím zařazením do Virtlabu(6.1.2). Studenti by měli mít možnost snadného přístupu k běžně používaným síťovým službám a službám využívaných Cisco prvky. Zde popíšu stručně, které služby jsem instaloval a nastavoval.

Rozhodl jsem se pro stabilní síťovou distribuci Debianu Etch.

Po instalaci základního systému a vyladění, vypnutí nepoužívaných služeb jsem postupně instaloval a nastavoval ftp, sftp, http, https, ssh, telnet, dhcp a dns servery.

Poté jsem zkonfiguroval a přeložil další programy potřebné pro Cisco cvičení : mc, yersinie 7.0.1, nmap 4.68-1, tac-plus 4.0.4, freeradiusu 2.0.4, elinks, nikto, nessusu 2.2.10.3

Dále jsem musel ručně nastavil služby https a nessus.

6 Praktické řešení bakalářské práce

Hlavním cílem bakalářské práce bylo vytvořit soubor cvičení, které budou demonstrovat použití látky z jednotlivých kapitol kurzu NS1. Hlavní problém byl v zastaralosti některých cvičení, s konfigurací a přizpůsobení opensource produktů na cisco prvky jako freeradius a takacs+ a cvičení na PIX, které používá poněkud jinou syntaxi než nové ASA.

6.1 Laboratorní vybavení

K řešení bakalářské práce jsem využíval dvou laboratoří. Učebny J257, nacházející se v budově VŠB Ostrava a také virtuální laboratoře

6.1.1 Fyzická laboratoř

Učebna J257 patří ke stěžejním učebnám Regionální Síťové Akademie Cisco. Je osazena síťovými prvky, na kterých jsem konfiguroval a zkoušel cvičení. V této učebně se i vyučují kurzy síťové bezpečnosti, pro které je tato bakalářská Práce určená.

6.1.2 Virtuální laboratoř – Virtlab

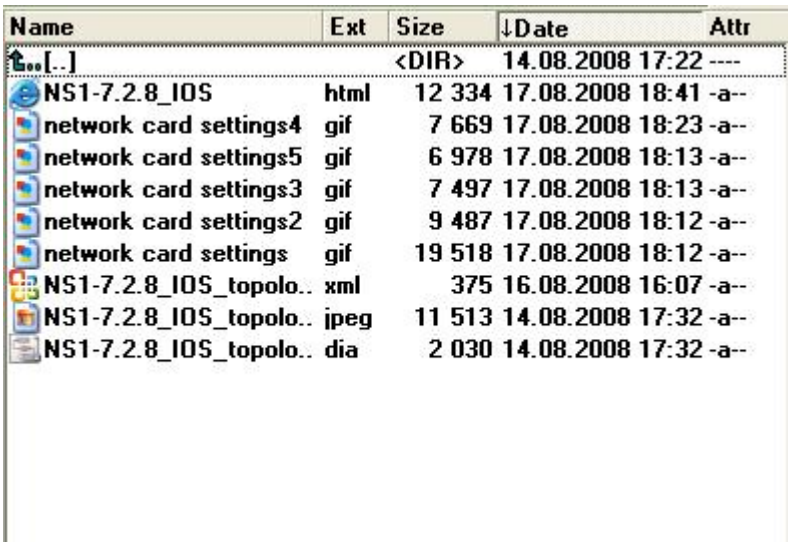
Je projekt Fakulty Elektrotechniky a Informatiky. Fyzické prvky jsou ovládány a spojovány do logických topologií přes webové rozhraní. Cvičení jsou připravena pro výuku dálkových studentů přes Virtlab. Tato laboratoř je přístupná z internetu na adrese *[4]* pro registrované uživatele. Ti zde mohou používat předdefinované topologie, přidávat vlastní cvičení, nebo měnit stávající. Bližší popis Virtlabu lze nalézt na internetové adrese *[5]*.
Vybavení se principielně příliš neliší od vybavení fyzické laboratoře na J257 a je dostačující pro tvorbu této práce.

6.1.2 Seznam vybavení

Ve většině případu jsem používal směrovače Cisco 2801, firewall ASA 5510 a přepínače Cisco 3550. Seznam vybavení je obsažen v příloze 1.

6.2 Struktura cvičení

Jako přílohu každého cvičení dodávám i konfigurační soubory s předpřipravenou konfigurací.



Name	Ext	Size	↓Date	Attr
[..]		<DIR>	14.08.2008 17:22	----
NS1-7.2.8_IOS	html	12 334	17.08.2008 18:41	-a--
network card settings4	gif	7 669	17.08.2008 18:23	-a--
network card settings5	gif	6 978	17.08.2008 18:13	-a--
network card settings3	gif	7 497	17.08.2008 18:13	-a--
network card settings2	gif	9 487	17.08.2008 18:12	-a--
network card settings	gif	19 518	17.08.2008 18:12	-a--
NS1-7.2.8_IOS_topolo..	xml	375	16.08.2008 16:07	-a--
NS1-7.2.8_IOS_topolo..	jpeg	11 513	14.08.2008 17:32	-a--
NS1-7.2.8_IOS_topolo..	dia	2 030	14.08.2008 17:32	-a--

Obr. 1: Adresářová struktura odevzdávaných cvičení.

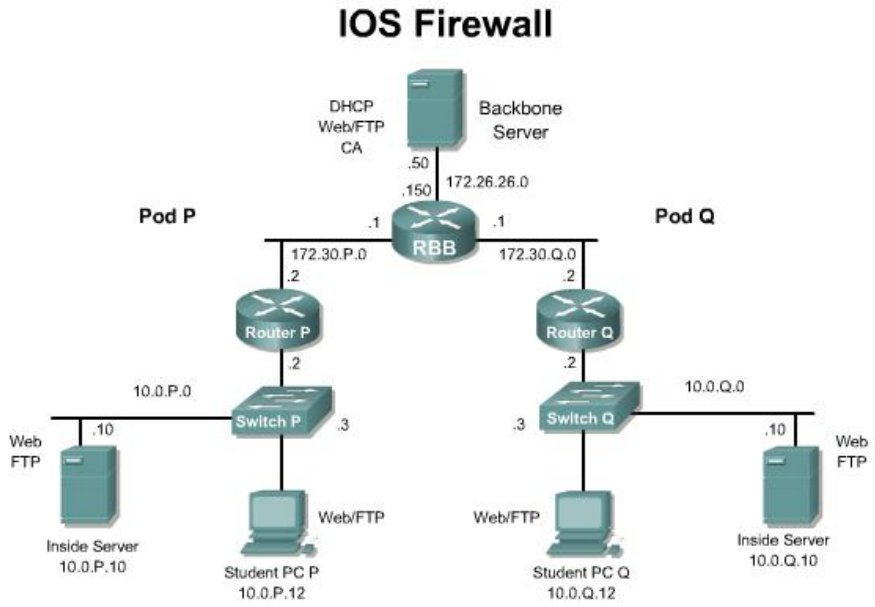
V jednotlivých řešeních používám tyto soubory:

- .html – je hlavním dokumentem cvičení, využívá formátování pomocí stylů – css soubor v *[x]*
- .jpg – obrázky ke cvičením
- .xml – je soubor s logickou topologií zadání pro Virtlab
- .dia – obrázek topologie

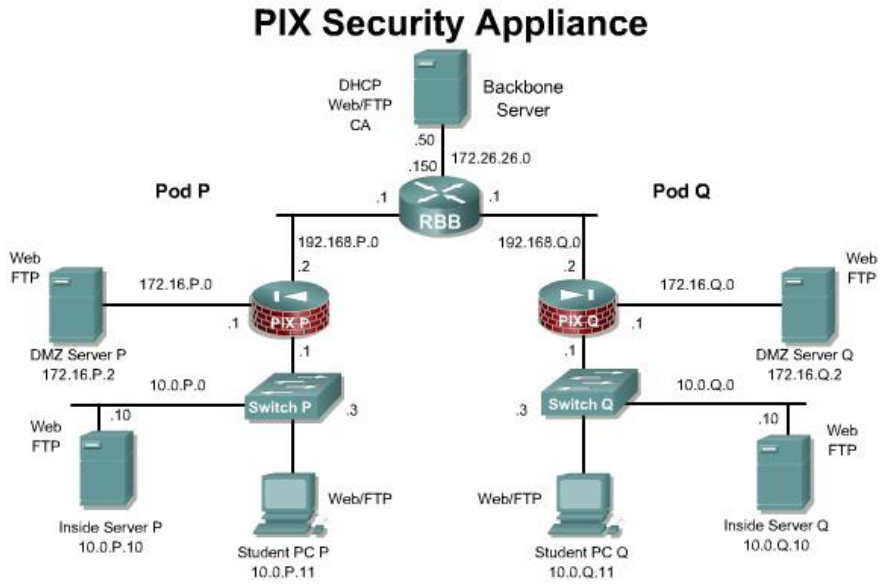
Pro tvorbu a formátování úloh jsem použil software, který je uveden v příloze 6.

6.3 Původní topologie sítě

Původní topologie sítě byla zřejmě zamýšlená zřejmě jako trvalá a laboratoř se měla používat výhradně k Network security účelům. Je to důvod proč je docela obsáhlá a perzistentní pro všechny úlohy na IOS a PIX



Obr. 2: Původní Cisco Topologie IOS



Obr. 3: Původní Cisco Topologie PIX

Samozřejmě je tato topologie pro účely a možnosti RCNA akademie těžko použitelná, když se každý den vyučují různé druhy cisco kurzů a školních předmětů. A další důvod předělání topologie je možnost snadno přenést tyto cvičení do Virtlabu.

Z těchto důvodu jsem vytvořil pro jednotlivá cvičení svou vlastní topologii, která by měla splňovat všechny požadavky na funkčnost a neměla by studentům zabírat spoustu času zapojením

Proto například při cvičením na zabezpečení přístupu na router se obejdeme se zapojením jednoho routeru a jednoho počítače.

6.4 Vypracovaná cvičení

Cvičení 2.5.2a

Cíl

Cílem cvičení je nakonfigurovat SSH na směrovači Cisco a otestovat jeho funkci.

Postup řešení

Po fyzickém zapojení příslušné topologie a úspěšným testem spojení si studenti na směrovači vygenerují RSA klíč, pro který je nezbytné nastavit hostname a domain name. Potom si zkusí nastavení vlastností SSH serveru jako čas otevřeného ssh spojení nebo počet neplatných pokusu o přihlášení a verzi ssh. Poté ošetří vstup tak, že povolí pouze ssh protokol a vytvoří uživatele v lokální databázi, který se bude moci připojit.

Problémy a připomínky

Při generování RSA klíče je třeba brát v potaz, že defaultní nastavení velikosti na 512 bits je v dnešní době mnoha systémy zamítáno, proto doporučuji změnit velikost RSA klíče na 1024 bits. Studenti si můžou vyzkoušet toto zamítnutí na Linuxu. Dále jsem přidal konfiguraci SCP serveru pro šifrovaný přenos souboru po síti

Cvičení 2.5.2b

Cíl

Toto cvičení je zvláště důležité, mělo by studenty naučit jak správně zabezpečit směrovač.

Postup řešení

Po připojení na příslušný směrovač se studenti přesvědčí jaká je výchozí konfigurace a postupně provedou zabezpečení. Postupně procházet jednotlivé servisy, vysvětlovat k čemu slouží a jak by je mohl útočník zneužít a pak je vypínat. Studenti by si mohli v budoucnu vyzkoušet penetrační nástroj yersinia a přesvědčit se jakou neplechu může způsobit na nezabezpečeném směrovači.

Problémy a připomínky

Zde cisco v původním cvičení nabízí 12 příkazů které vypínají nepoužívané služby. Mě se podařilo najít přes 30 takových příkazů. Tuto kapitolu jsem rozdělil na vypínaní služeb v globálním režimu a na vypínání služeb v na konkrétním síťovém rozhraní. Dále jsem přidal kapitolu a zabezpečení webového rozhraní směrovače a vstupu.

Zmínil jsem ještě jednu novou vlastnost jménem auto secure, což je průvodce zabezpečením, který interaktivně zabezpečuje směrovač podle uživatelova přání.

Cvičení 2.5.7

Cíl

Seznámit studenta se zabezpečení směrových protokolů a důvodech proč zabezpečení používat.

Postup řešení

Po zapojení a otestovaní konfigurace se studenti postupně seznámí se zabezpečením směrového protokolu RIPv2, kde nastaví základní směrování, potom vygenerují klíče a nastaví pro daný protokol šifrování. Dále přiřadí access-list na kterých sítích můžou směrovací protokoly směrovat a nakonec vypnou směrování na síťovém rozhraní, pro které si nepřejí odesílat RIPv2 pakety. Více méně podobné postupy použijí a otestují dále pro protokoly OSTF a EIGRP.

Problémy a připomínky

Původní cisco cvičení se zajímá pouze o verzi RIP, proto jsem toto cvičení dále postupně rozšířil o protokoly OSPF a EIGRP

Cvičení 3.4.6b

Cíl

Seznámit studenta se odlišnostmi ASA zařízení a otestovat základní funkce

Postup řešení

Studenti se seznámí se základními příkazy ASA a odlišnostmi oproti IOS. Dále zjistí odlišné výchozí nastavení.Vyzkouší si nastavit 3 síťové rozhraní s odlišnými vlastnostmi jako vnitřní, vnější a dmz (demilitarizovaná zóna) rozhraní a nastaví o otestují překlad adres.

Problémy a připomínky

Toto cvičení je poměrně jednoduché, ale je nezbytné, aby si studenti uvědomili zásadní rozdíly mezi směrovači a prvky ASA. Taky by si měli projít výchozí nastavení ip inspectu ve kterém chybí icmp.

Cvičení 6.1.3

Cíl

Seznámit studenta jak nakonfigurovat autentikaci na lokální databázi směšovače.

Postup řešení

Po nastavení ssh spojení viz. cvičení 2.5.2b si studenti vytvoří různé uživatelské účty a nastaví různá hesla pro ssh a konzolová připojení. Poté zapnou autentikaci a vytvoří autentikační skupiny, poté přidělí tyto skupiny do autentikace vstupů a otestují spojení a zjistí jaké účty a hesla jsou platné.

Problémy a připomínky

Je to základní cvičení na AAA a je to dobrá průprava na pochopení složitějších cvičení.

Cvičení 6.1.4

Cíl

Seznámit studenta jak nakonfigurovat autentikační proxy server na směrovači.

Postup řešení

Po zapojení a otestování topologie si studenti vyzkouší konfiguraci RADIUSu aTACACS+ serverů, kde vytvoří různé uživatele. Poté vytvoří a nastaví TACACS+ RADIUS skupiny na směrovači. Dále nastaví web rozhraní na směrovači a vytvoří a přiřadí access-listy a autentikační proxy na příslušná síťová rozhraní.

Problémy a připomínky

Na vnitřní komunikaci mezi NAS servery se používá klíč, který jsem zvolil pro jednoduchost cisco, mělo by být při každém použití hesla cisco vysvětleno studentům, ať to nikdy nepoužívají ve své praxi. Při nastavení AAA skupin na směrovači se musí pokaždé nastavovat příslušné porty serverů, např. RADIUS autentikační port udp/1812 a účtovací port udp/1813.

Cvičení 6.3.9

Cíl

Seznámit studenta jak nakonfigurovat autentikaci na lokální databázi ASA.

Postup řešení

Po nastavení ssh spojení si studenti vytvoří různé uživatelské účty. Poté nastaví na příchozí spojení autentikaci pro různé služby a taktéž nastaví i odchozí spojení. Vyzkouší si nastavit autentikační hlášení pro přijmutí, odmítnutí a úvodní řádek autentikace. Dále nastaví různé časové úseky pro reautentikaci nebo nečinnost uživatele.

Problémy a připomínky

Důležité je při určení lokálních AAA serveru používat velké písmena LOCAL.

Cvičení 6.3.10

Cíl

Seznámit studenta jak nakonfigurovat autentikaci, autorizaci a účtování na zařízení ASA s použitím freeRADIUS a TACACS+ serverů.

Postup řešení

Po zapojení a otestovaní topologie si studenti vyzkouší konfiguraci RADIUSu a TACACS+ serverů, kde vytvoří různé uživatele. Poté vytvoří a nastaví TACACS+ a RADIUS skupiny na ASA.
Vyzkouší si vytvoření autentikace příchozího spojení různými způsoby, a to include, exclude a s použitím access-listu. Dále nastaví autorizaci a účtování na ssh spojení a otestují. Dále nastaví různé časové úseky pro reautentikaci, nebo nečinnost uživatele.

Problémy a připomínky

Na vnitřní komunikaci mezi NAS servery se používá klíč, který jsem zvolil pro jednoduchost cisco, mělo by být při každém použití hesla cisco vysvětleno studentům ať to nikdy nepoužívají ve své praxi. Při nastavení AAA skupin na směrovači se musí pokaždé nastavovat příslušné porty serverů, např. RADIUS autentikační port udp/1812 a účtovací port udp/1813.

Cvičení 7.2.8

Cíl

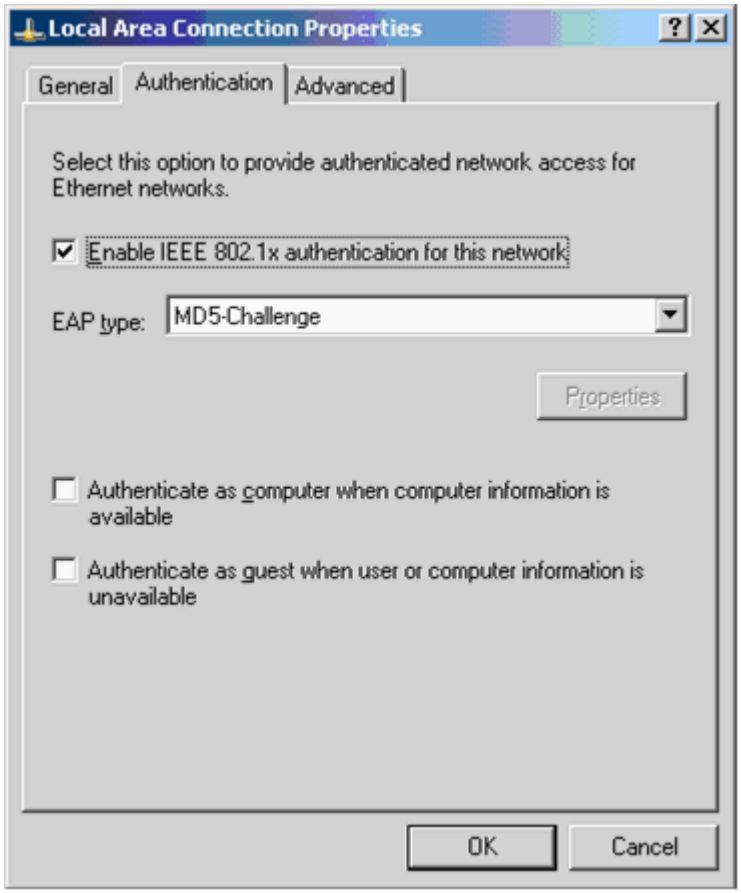
Seznámit studenta jak nakonfigurovat 802.1x na přepínači, autentikaci na 2 vrstvě OSI

Postup řešení

Po zapojení a otestovaní topologie si studenti vyzkouší konfiguraci RADIUS servru na autentikaci EAP.Toté nastaví 802.1x autentakaci a RADIUS server na přepínači. A nakonec se naučí nastavit DHCP server. Poté nastaví na 802.1x příslušného klienta a vše otestují.

Problémy a připomínky

Je důležité nastavit na přepínači na příslušných portech STP fast port, tak se vyhnou studenti 2 minutovému čekání autentikaze a třeba mylnému přesvědčení, že je konfigurace nefunkční. V operačním systému Windows XP je třeba v nastavení síťové karty nastavit IEEE 802.1x autentikaci na EAP typ MD-Challenge



Obr. 4: nastavení EAP ve Windows XP

Cvičení 8.3.13

Cíl

Seznámit studenta jak nastavit stavový firewall s inspekcí tzv. Content base access control CBAC na směrovači.

Postup řešení

Po zapojení a otestování topologie si studenti nastaví ssh server a syslog server. Poté nastaví access-listy a CBAC a logování na směrovači. Na dalším PC budou simulovat webové a další služby, které si otestují.

Problémy a připomínky

Pro tuto příležitost jsem vytvořil topoligii, která simuluje prostředí sítě, kde je povolený pouze příchozí port 22 a síťové spojení, které bylo iniciováno z vnitřní sítě, zbytek zakázán. Myslím si, že CBAC představuje ohromný kus dopředu v kontrole síťové aktivity a nastavování s porovnáním s Reflexivními access listy RACL.

Cvičení 9.1.9

Cíl

Seznámit studenta jak nastavit access listy na zařízení ASA a filtrování škodlivého aktivního kódu.

Postup řešení

Po nastavení a otestovaní topologie, si studenti nastaví překlad adres a vytvoří a připojí access listy na příchozí a odchozí spojení. Dále nastaví activex a java filtrování. Vše potom otestují.

Cvičení 9.2.5

Cíl

Seznámit studenta jak nastavit skupiny objektu a ukázat jak jsou efektivní

Postup řešení

Po zapojení a otestovaní topologie si studenti nastaví skupiny objektu a servisu a poté aplikují vytvořené access-listy.

Problémy a připomínky

Pro tuto příležitost jsem vytvořil topologii, která simuluje prostředí dmz, kde jsou povolené pouze určité služby a síťové spojení, které bylo iniciováno z vnitřních sití, zbytek zakázán. Studenti zjistí, že použití skupiny objektů může zjednodušit access list z 20 záznamů na jeden přehledný a použitelnější pro případné změny.

Cvičení 10.2.4

Cíl

Seznámit studenta jak zabezpečit používané služby na přepínači.

Postup řešení

Po zapojení a otestovaní topologie si studenti postupně projdou zabezpečení portu, dhcp serverů, arp inspekci a strážce zdrojové(adresy).

Problémy a připomínky

Původní cvičení jsem rozšířil o ARP inspekci a ip source guard

Cvičení NS1-syslog-IOS

Cíl

Seznámit studenta nakonfigurovat logování na směrovači a nakonfigurovat vzdálený syslog server.

Postup řešení

Po zapojení a otestovaní topologie se studenti naučí nastavit vzdálený syslog server na Linuxu a poté si vyzkouší různé úrovně logování. Dále se naučí jak logování správně nastavit. Nakonec zkontrolují výsledný log soubor.

Problémy a připomínky

Toto cvičení jsem vytvořil zcela nové.

Cvičení NS1-NTP-IOS

Cíl

Naučit studenta nakonfigurovat ntp službu na směrovači.

Postup řešení

Studenti se naučí nastavovat časové servery , formát data, určovat primární ntp server a mnohé další vlastnosti ntp jako autentikaci a logování.

Problémy a připomínky

Toto cvičení jsem vytvořil zcela nové.

Cvičení NS1-AAA-SSH

Cíl

Seznámit studenta nakonfigurovat AAA službu pro přístup ssh

Postup řešení

Po nastavení a ověření topologie studenti nastaví RADIUS server a vytvoří ssh připojení na směrovači. Poté nastaví RADIUS server na a aaa skupinu na směrovači, dále nastaví autentikaci autorizaci a účtování pro ssh spojení. Vše nakonec otestují a prověří účtovací soubor.

Problémy a připomínky

Toto cvičení jsem vytvořil zcela nové. A myslím, že je jednoduché a pěkně demonstruje sílu aaa služby.

7 Závěr

Hlavní cílem této bakalářské práce bylo vytvořit aktuální, funkční a otestované úlohy z kurzů network Security a přizpůsobit na vybavení RNCA akademie a tím pomoci instruktorům vyhnout se ztrátě času řešením nekontability a neaktuálnosti.

Přínosem bylo pro mě hlubší pochopení cisco náhledu na sítě a zdokonalení se v síťové problematice. Velmi si přeji , aby tato práce měla přínos pro RNCA akademii.

Výsledkem je celkem 16 úloh a cca. 10 dalších předpřipravených pro výuku a vytvoření Linux distribuce obsahující běžně používané služby s penetračními nástroji a AAA servery.

Seznam obrázků

Použitá literatura

[1] URL:< http://www.net-security.org/secworld.php?id=6380

[2] URL:< http://www.internetworldstats.com/stats.htm

[3] URL:< http://www.theregister.co.uk/2008/07/30/websense_high_profile_website_malware_survey/

[4] URL:< http://virtlab.cs.vsb.cz

[5] URL:< http://cs.vsb.cz/vl-wiki

[6] URL:< http://www.cs.vsb.cz/grygarek/TPS/projekty/0405Z/RADIUS/index.html

[7] URL:< http://encyklopedie.seznam.cz/heslo/488519-tacacs

[8] URL:< http://www.abclinuxu.cz/clanky/site/dhcp-1-instalace-a-konfigurace-serveru

[9] URL:<http://hw.cz/Teorie-a-praxe/Dokumentace/ART1027-Presny-cas-na-PC-prostrednictvim-Internetu.html

Přílohy

Veškeré přílohy se nacházejí na CD s textem bakalářské práce. Jejich seznam s popisem obsahu jsem uvedl v následujícím textu:

Priloha_1.pdf – Seznam použitého vybavení s verzemi operačních systémů.

Priloha_2 – Adresář s kompletními úlohami.

Priloha_3.pdf – Seznam použitého software.

Priloha_4 – obraz připravené ditribuce Linuxu

Místo pro vaše poznámky: