



NETACAD NEWSLETTER

03/
07



Výročná konferencia programu NetAcad



Vážená NetAcad komunita,

dovoľujeme si Vás pozvať na 6. ročník výročnej konferencie vzdelávacích inštitúcií zapojených do programu NetAcad v Českej a Slovenskej republike.

Dátum: 12. - 14. apríl 2007
Miesto: Hotel Krystal, Praha 6

Výročná konferencia programu NetAcad spoločnosti Cisco je už tradične organizovaná spoločne pre zástupcov z Českej a Slovenskej republiky.

Konferencia je striedavo organizovaná v Českej a Slovenskej republike. V súčasnosti patrí k najvýznamnejším odborným podujatiam venovaným sieťovým technológiám a vzdelávaniu sieťových profesionálov.

PROGRAM

Program konferencie je rozdelený na niekoľko **tematických blokov**, ktoré vytvárajú priestor pre prezentáciu aktuálnych informácií o programe a jeho rozvoji.

Konferencia je miestom zaujímavej **výmeny skúseností z implementácie programu NetAcad** do študijných osnov stredných a vysokých škôl, a miestom pre diskusie o **význame vzdelávania profesionálov z oblasti sieťových technológií**.

Okrem prezentácií zástupcov NetAcad inštitúcií jednotlivých regiónov, výmeny skúseností z úspešných implementácií programu, podrobností o uzavretých partnerstvách a mnohých ďalších informáciách, Vás čaká **spoločenský večer** plný súťaží a prekvapení.

Súčasťou programu konferencie bude aj slávnostný ceremoniál **vyhodnotenia najlepších akademii, lektorov programu NetAcad a ocenenie významných aktivít roku 2006**.



V tomto čísle nájdete:

KONFERENCIA NETACAD

Registrácia na konferenciu je otvorená
na stránkach NetAcad (strana 1)

MICHAL BRUNCKO

Rozhovor s víťazom súťaže Cisco
OLYMP 2006 (strana 2)

CISCO OLYMP

Zmena termínov (strana 2)

ZO ŽIVOTA ŠTUDENTOV

„KNŠ sada“ na opravu
CISCO 2811 (strana 3)

SERIÁLY

Sieťová bezpečnosť (strana 4)
Cisco IOS (strana 5)

REGISTRÁCIA

Registrujte sa ešte dnes na stránkach:

www.netacad.sk
najneskôr do
26. marca 2007



Veríme, že sa Vám oplatí investovať svoj čas a zúčastníte sa výročnej konferencie programu NetAcad.

Tešíme sa na stretnutie s Vami

Organizačný tím
Výročnej konferencie programu NetAcad

Partneri programu NetAcad pre SR

Generálny partner

**SLOVENSKÁ
SPORTEĽŇA**

Mediálny partner

PC REVUE



Prihovor AAM

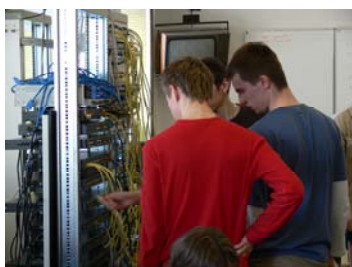
Vážení kolegovia, dovoľujem si Vám pripomenúť, že v nasledujúcom mesiaci nás čaká niekoľko dôležitých aktivít, ktoré sú organizované v rámci našej sieťovej komunity.

Jedná sa o školské kolá **súťaže Cisco Olymp**, ktoré by mali prebehnúť na školách do konca marca. Pevne veríme, že súťaž bude mať medzi študentmi minimálne taký úspech ako v minulom roku a hlavne, že sa do súťaže zapojí ešte väčší počet škôl. Tento rok boli upravené súťažné kategórie tak, aby bolo umožnené zúčastniť sa aj školám, ktoré z rôznych dôvodov nemajú implementované do svojich študijných programov všetky 4 semestre programu NetAcad a neboli tak znevýhodnené. Víťazov súťaže čakajú zaujímavé ceny: pre postupujúcich zo školských kôl to bude účasť na regionálnych kolách v Košiciach a Bratislave, následne pre víťazov účasť v národnom a medzinárodnom kole súťaže. Cisco Olymp už v svojom prvom ročníku vyvolala veľký záujem IT spoločností – budúcich potenciálnych zamestnávateľov úspešných študentov a bola podporená aj Ministerstvom školstva SR.

Druhou významnou udalosťou, na ktorú by som Vás rád upozornil je **výročná konferencia programu NetAcad**, ktorá sa tento rok bude konať v dňoch 12. a 13. apríla 2007 v Prahe (www.netacad.sk). Konferencia je o to významnejšia, že sa koná v roku, kedy program NetAcad oslavuje 10 výročie svojej existencie. Dovoľujem si Vás touto cestou osobne pozvať k účasti na konferencii, ktorá sa určite tak ako predchádzajúce ročníky stane významným miestom prezentácie aktuálneho stavu programu NetAcad v SR a ČR, perspektív jeho ďalšieho rozvoja a určite aj miestom, kde sa stretávajú ľudia, ktorí majú spoločné záujmy, a ktorí si majú čo povedať.

Prosím využite túto príležitosť. Tešíme sa na stretnutie s Vami.

František Jakab
koordinátor programu NetAcad v SR



Rozhovor: Michal Bruncko, víťaz Cisco OLYMP 2006

Michal Bruncko bol prvým víťazom v súťaži Cisco OLYMP v kategórii vysokoškolských - jednotlivcov v roku 2006. Keďže sa blíži termín nového kola súťaže, požiadali sme ho o priblíženie minuloročnej súťaže.

Kedy si sa po prvý krát dozvedel o programe NetAcad? Ako dlho už v programe NetAcad študuješ?

Bolo to ešte na strednej škole, keď som bol tuším druhák. Prišiel k nám do triedy náš školský zástupca a oboznámil nás s týmto projektom. Vtedy som ešte o firme Cisco nepočul. Takže na strednej škole som absolvoval prvé dva semestre CCNA 1 a CCNA 2 a s ďalšími som pokračoval na vysokej škole v Žiline.

Vyzerá to, že je Ti problematika sietí blízka?

Už ako malého fagana ma bavilo "vítat" sa v systémoch. Neskôr prišlo do módy sieťovanie počítačov, tak sme si s kamarátmi takú koaxiálnu sieť postavili. Postupne sa to stalo ešte väčšou záľubou, keď sme sa siete začali učiť aj v škole. Neskôr som popri výške začal pomáhať na jednej strednej škole s počítačovými učebňami. Teraz tam robím správcu siete a tiež som donedávna spravoval WiFi sieť na internátoch v Žiline. Takže problematika sietí mi blízka určite.

Pamätáš sa ešte na minuloročnú súťaž Cisco OLYMP? Ako sa Ti podarilo postúpiť až do národného kola?

Tak na tú asi tak skoro nezabudnem. Jednoducho som si povedal, že súťaž skúsím a tak som sa jednoducho prihlásil. Keďže som mal CCNA už rok za sebou, tak som si dal narychlo „opakovačku“. A oplátilo sa. Školským kolom som prešiel. Pred národným kolom mi dost pomáhal s prípravou náš inštruktor Peter Palúch, ktorému sa chcem touto cestou poďakovať za čas, ktorý mi venoval. Veľmi mi jeho rady pomohli.

Takže sa hodí pomoc inštruktora v príprave na súťaž?

To určite áno. Má väčšie skúsenosti, odporučí na čo sa zamerať, občas hodí nejaký "hint". Vie zodpovedať kopec otázok, ktoré sa nahromadia počas prípravy. A určite sa aj on takto snaží aby cena ostala v akadémii.

Bola súťaž Cisco OLYMP náročná? Priblíž nám svoje pocity a skúsenosti, ktoré si účasťou v súťaži získal?

Praktické úlohy vo všetkých kolách boli predovšetkým náročné na čas, ktorého nebolo nikdy nazvyš. Na druhej strane zložitost' úloh nebola vysoká, ale skôr rozsahovo náročná. Bolo nutné si dobre zorganizovať čas a pokiaľ bol s nejakou pod-úlohou väčší problém, tak najlepšie bolo nechať si ju na koniec.

A čo sa týka pocitov, tak boli fakt príjemné. Stretla sa tam špička ľudí z celého Slovenska. Uspieť v takej konkurencii človeka naozaj poteší.

Ako by si nalákal študentov, ktorí uvažujú, či sa súťaže v tomto roku zúčastnia?

Je to jedna z mála príležitostí počas štúdia, ako si sám sebe dokázať, že ti štúdium sieťových technológií niečo dáva. Iné súťaže podobného zamerania sa snád' ani neorganizujú, takže všetkým študujúcim záujemcom o sieťové technológie odporúčam zúčastniť sa. Taktiež je to výborná možnosť ako si zjednotiť vedomosti získané štúdiom CCNA. Okrem toho si myslím, že aj takéto zviditeľnenie pomôže pri získaní nového, lukratívneho zamestnania. A v neposlednom rade sú aj ceny lákavé.

Keď už hovoríš o cenách. Čo si dostal ako odmenu a kedy Ti bola odovzdaná?

No s cenami organizátori počas súťaže dost' napínali. Hlavná cena pre víťaza bol notebook, celkom slušná „mašina“. Cenu som si prevzal spolu s víťazom stredoškolských na tlačovke



v hoteli Carlton v Bratislave, pri príležitosti piateho výročia plnenia Memoranda o spolupráci medzi Ministerstvom školstva SR, spoločnosťou Cisco a Slovenskou sporiteľňou. Samozrejme všetko za účasti dvoch členov vlády Slovenskej republiky).

Spomínaš si s príprav na niečo veselé?

No na mnoho veselých príhod si nespomínam. Len to, že v prípravách bola aj noc, kde sa mi o routroch dokonca snívalo (ale to ani neuverejňujte, nechcem vyzerat' ako IT „kockáč“, od toho mám ďaleko).

Ďakujem Ti veľmi pekne za rozhovor. Verím, že tvoj príklad motivuje ďalších študentov. Práve Ti veľa úspechov.

Veríme, že Vás príklad Michala Bruncka zaujal, a že využijete príležitosť zapojiť sa do súťaže Cisco OLYMP v tomto školskom roku. Všetky informácie o podmienkach súťaže nájdete na stránkach www.netacad.sk

Odpovedal: Michal Bruncko
Študent RCNA
pri Žilinskej Univerzite

Za Newsletter spovedala:
Zuzana Szabóová, Redakčná rada

Zmena termínov v súťaži CISCO OLYMP 2007

Ukončenie školského kola

do 31.03.2007

Regionálne kolá

19.04.2007 Slovenská technická univerzita Bratislava

20.04.2007 Technická univerzita v Košiciach

Národné a medzinárodné kolo

29.-30.06.2007

Technická univerzita v Košiciach

Viac informácií na: www.netacad.sk



„KNŠ sada“ na opravu CISCO 281 I

Traja švární šuhaji sa jedného krásneho dňa, vybrali sa na kurz CCNA3. Veľmi bážili za vedomosťami, ktoré tam získajú. Preto, keď za jedným z nich prišla deva, veľmi šumná a stepilá s pozvaním na malinovku, odpovedal jej švárný šuhaj, že nemôže, bo večer ide router konfigurovať a štruktúrovanú kabeláž inštalovať.

Teda všetci traja vybrali sa do laboratória, aby čo najlepšie inštalovať a konfigurovať vedeli. Sadli si oni za počítače, čerstvo vybalené a len

kým sa minúťová ručička dvakrát pretočí. Nuž zaháľat' by bolo nezodpovedné, priam pochabé. Inštruktor začal vysvetľovať spôsoby zaobchádzania s routermi, nakoľko boli úplne nové i nevidané, z dôvodu nesmierne dobrého zásobovania laboratória do najnovším všetkým vybavením. Vysvetlil (presnejšie vysvetlila, nakoľko prístup vhodný k študentom môže mať iba osoba, ktorá sa sama starala o svoje detúrence, teda matka) ako zaobchádzať s pamäťou typu „fleš“, nakoľko zariadenia, na ktorých študenti vykonávajú svoje pokusy sú hodné mnohociťnej sumy (a to ešte v líbrách) aby sa tak predišlo ich poškodeniu. Nakoľko jeden zo šuhajov, veľmi zaniatený pozorovaním najnovších rackov a tienových káblov, nevnímal veľmi inštrukcie inštruktorky, vykonal on niečo strašné!



s nutným legálnym softwarom vybavené. Ba veru rozhodli sa oni využiť krátke chvíle testovaním funkčnosti siete LAN, v ktorej sú prepojené počítače, a rozvíjať svoje inteligenčné schopnosti využitím edukačného softwaru Quake 3. Lenže času bolo neveľa, ba priam poskromne, a to z dôvodu pochopiteľného, že inštruktor nikdy nezahľal i priniesol im vytlačené zadania laboratórných cvičení č.5.4.400 a č.5.5.306, že ich treba vykonať po-

Najprv vyzeralo šuhajom všetko v poriadku. Lenže pri podrobnejšom štúdiu a kontrole novších zariadení, všimol si brat Orlie oko postupnosť, a nie hocijakú, zloženú len z prúžkov všakovakej šírky len dvoch farieb a to farby snehu a farby noci (tod'ho čiarový kód). Táto postupnosť bola odlišná od ostatných, čítaná zľava doprava. Logickou dedukciou (nakoľko študenti LCNA na Gymnázium P. Horova majú logické myslenie a schopnosti, ktoré sa



dajú využiť aj v rôznych súťažiach a akciách zameralých na rozvoj logiky) prišli na to, že „fleš“ pamäť bola vložená naopak. Ejho, trebalo ju vybrať a vložiť opätovne správnou stranou.

No nešlo to vybrať! Psychika jedného zo študentov utrpela riadny šok, keď sa dozvedel cenu ohrozených zariadení. No späť do sveta zdravých ho vrátilo to, že ono sú to zariadenia pre študentov a ráta sa s tým, že sa zničia J. Problém sa najprv pokúsili riešiť sami šuhaji manipuláciou ostrým hrotom narýchlo uchopeného predmetu. No márne!

Šuhaj najšvárnejší zo všetkých, oplývajúci odvahou a láskou k vlasti, priznal sa po návrate inštruktorky k svojmu činu. Očakávajúc túto situáciu, inštruktorka riekla: „Zas?!“. Uchopila kladivo, nožnice a šrubovák (KNŠ sada – CISCO router recovery kit) a riadnym silovým pôsobením s pomocou pána Iľvana vybrali externú pamäť z jemnej mechaniky.

Router i pamäť fungovali (dúfajúc na večné veky) a šuhaji v šťastí získali certifikáty.

Autori: Marcel Ďuriš,
Jakub Tomaga, Tomáš Benedikti
LCNA pri Gymnázium
P. Horova Michalovce

Informácie zo sveta

31 DAYS BEFORE YOUR CCNA EXAM

Prepare for your CCNA exam with this day-by-day quick reference study guide. Each day breaks down an exam topic into a manageable bit of information to review using short summaries from relevant parts of the four Networking Academy CCNA courses. You'll also find a visual calendar summarizing each day's study topic and a checklist with advice for preparation activities.

Visit the product page to download a sample chapter and access supplementary content from the author, including reading quizzes.

Visit: www.ciscopress.com

CCNA VERSION 3.1 MATERIALS

As you may have heard, Cisco announced a new CCNA curricula will launch in late 2007. However, the current version of CCNA 3.1 will continue to be offered to all academies. The current Cisco Press version 3.1 Companion Guides and Labs and Study Guides are still in full alignment with the available 3.1 curriculum from Cisco.

Predstavujeme

Gymnázium T. Vansovej

Ul. 6. novembra 6
064 01 Stará Ľubovňa
www.gymsl.sk



LCNA pri Gymnázium Terézie Vansovej v Starej Ľubovni

Lokálna akadémia pri Gymnázium Terézie Vansovej v Starej Ľubovni sa zriadila na jeseň roku 2003. Na začiatku nás zaujala ponuka zo strany pána Jakaba na založenie LCNA v regióne Severného Spiša. Rozhodli sme sa, že ideme do toho! Naše rozhodnutie bolo spojené s ďalšími krokmi:

1. **nástup dvoch inštruktorov do I. semestra CCNA** na RCNA v Košiciach v jeseni roku 2002, kde postupne absolvovali všetky 4 semestre programu,
2. **nadchnutie Školskej rady, Rady rodičovského združenia** pre túto ideu. Museli sme im vysvetliť zmysel a význam zriadenia akadémie na našej škole, načrtnúť perspektívu jej využitia študentmi, ako aj vysvetliť spôsob financovania nákupu základného vybavenia akadémie.

Dnes môžeme povedať, že vďaka pochopeniu rodičov ako aj sponzorov, ktorí zobrali na seba hlavné bremeno finančného zabezpečenia, akadémia beží už štvrtý školský rok. Prvú triedu

sme otvorili na jeseň v roku 2003. Vďaka programu NetAcad študenti prišli prakticky prvýkrát do styku s on-line študijnými materiálmi a on-line preskúšaním, ako aj k získaniu poznatkov v cudzom jazyku. Obsah programu NetAcad sme zaradili do ponuky voliteľných a nepovinných predmetov s názvom Sieťové technológie I a II. Každý maturant z Informatiky na našej škole absolvuje voliteľný predmet Sieťové technológie.

Program NetAcad máme aj v ponuke nepovinných predmetov a realizujeme ho aj cez záujmové krúžky. Tie orientujeme na prvákov, aby získali prvé kontakty s programom. Program tiež organizujeme aj pre záujemcov mimo našej školy - ako sú učitelia - správcovia počítačových sietí, študenti VŠ a študenti z okolitých stredných škôl.

Za uplynulé obdobie sme celkovo otvorili 21 tried. Do programu sa zapojilo cca 216 študentov. Úspešne ukončilo niektorý zo semestrov 112 študentov. V súčasnosti sú otvorené 3 triedy a v nich študuje 37 študentov.

Od marca plánujeme otvorenie ďalších 2 skupín.

Vlani sa zriadila nová učebňa Informatiky, ktorá slúži aj pre potreby LCNA. Štedrým sponzorom bola Taipejská kancelária v Bratislave, ktorá prefinancovala materiálne vybavenie v hodnote takmer 1 000 000 Sk. Štruktúrovanú kabeláž sme si vybudovali svojpomocne s príspevom študentov LCNA, ktorí si tak mohli prakticky po prvý krát naozaj „zasieťariť“ a overiť nadobudnuté poznatky:

a. Regionálne kolo:

- 2. miesto v súťaži družstiev: **Fedák, Svrček, Galajda**
- 1. miesto v súťaži jednotlivcov: **Matúš Fedák**

a. Celostátné kolo: **Súťaž jednotlivcov—stredoškôľakov za 1. miesto: Matúš Fedák.**

Peter Petřík
Hlavný kontakt
LCNA pri Gymnázium
T. Vansovej v Starej Ľubovni

SERIÁL

Sieťová bezpečnosť

Systémy na detekciu a prevenciu proti prienikom – pohľad dovnútra.

V minulých mesiacoch sme opísali technológie používané v oblasti IDS/IPS systémov a aj zariadenia, ktoré na tieto účely poskytuje Cisco. Dnes by som rád nahliadol pod kryt týchto zariadení a trochu bližšie sa pozrel na IDS funkcie detekčného systému IDS/IPS senzora.

Momentálne je detekčný systém na rozhraní verzií 5.x (aktuálne 5.1.5) a 6.x (6.0.1). Signatúrové aktualizácie sa vydávajú paralelne pre obidve major verzie.

Senzor pri vyhľadávaní vzoriek podozrivého správania sa na sieť používa tzv. signature engines. Každý z nich je špecializovaný na inšpekciu určitého protokolu na L2 (ARP) až L7 (napr. HTTP) vrstve, štatistickú analýzu paketov (sweep, flood engines), špeciálne spracovanie udalostí (META), normalizovanie prevádzky (normalizer) atď.

Prvý z enginov je **Application Inspection and Control (AIC)**, ktorý umožňuje hĺbkovú aplikačnú inšpekciu konkrétnych aplikačných protokolov. K dispozícii sú inšpekcie pre FTP (**AIC FTP**) a pre HTTP (**AIC HTTP**). Tento engine kontroluje prevádzku na známych anomálií v danom aplikačnom protokole. AIC FTP napríklad kontroluje FTP prevádzku na konkrétne, prípadne neznáme FTP príkazy, AIC HTTP môže kontrolovať HTTP prevádzku podľa Content Type, Request Method, rôznych kódovaní, vyhľadávať reťazce v tele správy a pod.

Enginy typu **Atomic** sú určené pre signatúry, ktoré sa odpália na základe informácií z jediného paketu. Patria tu **Atomic ARP** a **Atomic IP** enginy. Atomic ARP kontroluje ARP pakety, a deteguje napr. počet zmien MAC adresy pre jednu IP adresu, operačný mód ARP (request/reply), nevyváženosť medzi ARP požiadavkami (request) a odpoveďami (reply). Ďalej vie detegovať cieľový (destination) broadcast (cieľová MAC adresa je broadcast), rovnakú zdrojovú aj cieľovú MAC adresu, zdrojový broadcast alebo multicast (zdrojová adresa je broadcast alebo multicast). Atomic IP engine ovláda TCP, UDP aj ICMP protokoly, vie kontrolovať fragmentáciu paketov, dĺžku IP hlavičky, dĺžku oblasti aj celkovú dĺžku paketu, typ služby (ToS), dĺžku života paketu (TTL), verziu IP, IP identifikátor. Môže hľadať konkrétny, alebo iba abnormálne IP nastavenia (IP options), vie detegovať aj rôzne varianty IP adresy (podľa RFC 1918, rovnaká zdrojová aj cieľová

IP, adresa localhost – 127.0.0.1 a pod.). Samozrejmosťou je aj vyhľadávanie reťazca v dátovej časti pomocou regulárnych výrazov.

V ICMP paketoch skontroluje ICMP kód, identifikátor, sekvenčné čísla, typ aj celkovú dĺžku.

V hlavičke TCP protokolu vie skontrolovať v podstate všetky parametre, ktoré sa tam vyskytujú. TCP príznaky (flagy) sa kontrolujú pomocou masky (maskou sa vyhradia príznaky, ktoré sa majú kontrolovať a následne sa určí, ako majú byť nastavené, aby sa signatúra odpálila).

Pre UDP protokol je k dispozícii kontrola zdrojových a cieľových adries, dĺžka paketu, prípadne nezhoda medzi deklarovanou a skutočnou veľkosťou paketu.

Flood engines poskytujú signatúram informácie o záplave paketov. **Flood Host engine** kontroluje záplavu paketov proti jednotlivým hostom. Jednotlivé ciele majú pridelené počítadlo (packet per second – PPS), ktoré je aktualizované na sekundovom základe. **Flood Net engine** kontroluje celú agregovanú prevádzku v segmente siete a každú sekundu generuje PPS počítadlo pre celý virtuálny senzor. Dajú sa definovať parametre, ktoré určujú, čo je považované za záplavu (flood). Je možné definovať hraničnú hodnotu (rate), nastaviť čas, po ktorý musí konkrétna prevádzka ostať nad hraničnou hodnotou, aby bola považovaná za záplavu (peak, špička), aj čas, na ktorý musí prevádzka klesnúť pod



hraničnú hodnotu počas špičky, aby bol časovač špičky vynulovaný (gap, medzera).

Meta engine je zvláštny engine, ktorý je určený na generovanie „zložených“ alarmov, t.j. alarmov, ktoré sa skladajú z viacerých signatúr, odpálených v danom časovom slede a intervale.

Na identifikovanie útokov typu manipulácia TTL, URG smerníka alebo veľkosti okna, RST alebo FIN príznaky mimo poradie alebo pakety mimo poradie a podobne, je určený **Normalizer engine**, ktorý si udržiava stavovú tabuľku TCP spojení. Existujú preddefinované signatúry, ktoré využívajú tento engine, ale nie je možné si tvoriť



používateľské signatúry. S výhodou sa tento engine používa pri inline (IPS) režime senzora, kde je možné anomálie spojení alebo paketov opraviť – normalizovať.

Service engine analyzuje prevádzku služieb na vyšších vrstvách (>L4) tak, že dekoduje aplikačný protokol (napr. umožňuje detegovať špecifikované parametre protokolu: DNS transfer request, MSSQL login name,...) a identifikuje potenciálne útoky. Podporuje tieto služby: DNS, FTP, H225, HTTP, ident, MSRPC, MSSQL, NTP, RPC, SMB, SNMP, SSH.

State engine používa na svoju činnosť stavový automat, ktorý definuje počiatočný stav a legálne prechody medzi jednotlivými stavmi. Momentálne podporuje tri stavové automaty pre Cisco Login, LPR formátovací reťazec a SMTP.

String engines kontrolujú TCP, UDP a ICMP prevádzku na výskyt reťazcov pomocou regulárnych výrazov (regexp). Rozlišujú pri tom smer (from service, to service), offset (presný, minimálny alebo maximálny), cieľové porty atď.

Sweep engines identifikujú situácie, kde jeden systém nadväzuje spojenia na viacero cieľov alebo na viacero cieľových portov. Kontrola prevádzky je možná na úrovni TCP, UDP aj ICMP protokolov. Umožňuje definovať rozsah portov a počet unikátnych spojení pre všetky protokoly, navyše typ pre ICMP, fragmentáciu a príznaky pre TCP.

Do **Miscellaneous engines** patrí **Trojan Horse Signature engine**, ktorý kontroluje prevádzku na známej činnosti trójskych koní typu Back Orifice 2k na TCP alebo UDP a DDos nástroja Tribe FloodNet 2K (TFN2K). Pomocou tohto enginu sa nedajú robiť používateľské signatúry.

Takmer každá signatúra sa dá individuálne ladit' (t.j. meniť jej parametre, vyvolávanie rozšírených alarmov a pod.). Pomocou **event filtrov** sa dá pre konkrétne signatúry odfiltrovať prevádzka, ktorá spôsobuje FP (false positives).

Definovaním aktív v sieti (asset) sa určia obzvlášť citlivé ciele na sieť (servery obsahujúce citlivé ekonomické, personálne alebo iné údaje a pod.), kde aj pri menšom útoku s nižšou štandardnou závažnosťou (severity) sa môže generovať alarm s vyššou závažnosťou.

Verzie IPS OS 6.x majú oproti starším 5.x niekoľko veľkých výhod. Podporujú virtuálne IPS politiky. Je teda možné na jednom fyzickom zariadení zároveň nakonfigurovať niekoľko paralelných „virtuálnych senzorov“, ktoré majú

Informácie z NetAcad

PROPAGAČNÉ MATERIÁLY PRE AKADÉMIE

Pri príležitosti 10-teho výročia programu NetAcad, je možné si na stránke academypacket.ciscolearning.org zažiadať o propagačné materiály pre Vašu akadémiu.

Cisco Learning Institute daruje pri príležitosti osláv 10-teho výročia programu NetAcad zostavu, ktorá obsahuje:

- **zástavu**, na identifikovanie Vašej akadémie ako kľúčového člena NetAcad komunity,
- **plagáty**: 4 postery zamerané na príležitosti, ktoré program NetAcad ponúka,
- **nálepky**: ktorými si môžete ozdobiť Vaše knihy a materiály a identifikovať tak NetAcad program na Vašej škole.

Ak ste inštruktorom, alebo hlavným



kontaktom a Vaša akadémia aktívne vyučuje program NetAcad, môžete si o materiály požiadať. V prípade záujmu, neváhajte a kliknite na stránku academypacket.ciscolearning.org.

Dúfame, že Vám materiály pomôžu v šírení dobrého mena programu NetAcad.

Frantisek Jakab
koordinátor programu NetAcad
pre Slovensko

rozdielne globálne nastavenia, nastavenia signatúr, rôzne zdroje prevádzky, ktorú sledujú a pod. Nová verzia umožňuje presnejšie určenie závažnosti pomocou systému ohodnotenia (ratingu) riziku/hrozby, obsahuje aj nové enginy **Database protecion engine (TNS)** a **SMBProtection engines** určené na ochranu databázových systémov a serverov zdieľajúcich súbory pomocou SMB. Funkcionalita IPS bola rozšírená aj o detekciu anomálií (behavioral-based IPS) a pasívny fingerprinting operačných systémov zariadení na sieť. Tieto funkcie sú však použité len na spresnenie hodnotenia odpálených alarmov.

Ján Valo
Lynx s.r.o. (jan.valo@lynx.sk)

SERIÁL

Zaujímavé vlastnosti Cisco IOS - ako si urýchliť svoju prácu

V tejto rubrike sa budeme spoločne zoznamovať so zaujímavými vlastnosťami Cisco IOS, ktoré nie je možné nájsť v žiadnom ucelenom kurze. Naučíme sa ako si zjednodušiť prácu a dozvieme sa ako použiť smerovač aj na funkcie, na ktoré primárne nebol určený.

Ako si urýchliť prácu v prostredí Cisco IOS CLI (časť V.)

Už dlhšiu dobu na seba zisťujem, že som možno až príliš na prácu v konzole Cisco IOS. Už ma nebaví ani len čakať na kompletný výpis smerovacej tabuľky, alebo na kompletný výpis príkazu `show ip protocols`. Našťastie aj

výpisy príkazov `show` sa dajú skrátiť a zobraziť tak len tie informácie, ktoré v danej chvíli potrebujem najviac.

Zoberme si príkaz `show ip route`. Každý z nás ho používa, ale možno menej známe sú jeho ďalšie parametre. Napríklad, ak si chcete zobraziť len cesty, ktoré sa smerovač naučil cez EIGRP, zadajte `show ip route eigrp`. Ak chcete zistiť, či daná sieť sa v smerovacej tabuľke nachádza, zadajte príkaz `show ip route` spolu s adresou podsiete, ktorú hľadáte (napr. `show ip route 10.0.0.0`). Ak sa sieť v smerovacej tabuľke nachádza, vypíše vám príkaz veľmi podrobné informácie o danej sieti. A ak chcete tento výpis zúžiť len na príslušný riadok smerovacej tabuľky, zadajte `show ip route | in 10.0.0.0`. Znak `|` je tzv. rúra a za ňou je možné zadať viacero parametrov, za ktorý sa dávajú tzv. regulárne výrazy:

- `in` (include) – zobrazí všetky riadky príkazu `show`, kde sa daný výraz nachádza
- `ex` (exclude) – zobrazí všetky riadky príkazu `show`, kde sa daný výraz **N**echádza
- `be` (begin) – zobrazí všetky riadky príkazu `show` od riadka, kde sa daný výraz nachádza

Teraz uvediem príklady na jednotlivé parametre. Najskôr uvediem typické použitie príkazu, potom použitie spolu s rúrou:

```
Switch#show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1		connected	12	a-full	a-100	10/100BaseTX
Fa0/2		connected	12	a-full	a-100	10/100BaseTX
Fa0/3		notconnect	1	auto	auto	10/100BaseTX
Fa0/4		notconnect	1	auto	auto	10/100BaseTX

... (výstup orezaný kvôli krátkosti, ináč by ukázal všetky porty)

```
Switch#show interfaces status | ex not
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1		connected	12	a-full	a-100	10/100BaseTX
Fa0/2		connected	12	a-full	a-100	10/100BaseTX

```
Router#sh ip ro 1.0.0.0
```

Routing entry for 1.0.0.0/8

Known via "connected", distance 0, metric 0 (connected, via interface)

Routing Descriptor Blocks:

* directly connected, via Serial0/0

Route metric is 0, traffic share count is 1

```
Router#sh ip ro | in 1.0.0.0
```

C 1.0.0.0/8 is directly connected, Serial0/0

Ako môžete vidieť, v prvom prípade som si za pomoci rúry vypísal len tie porty, ktoré má prepínač zapojené. V druhom prípade som sa na jedinom riadku výpisu príkazu `show ip route` presvedčil, či daná sieť sa nachádza v smerovacej tabuľke.

Peter Mesjar, CCIE #17428
Inštruktor RCNA, FIIT STU Bratislava
(pmesjar@centrum.sk)



Pohodlná práca v Cisco IOS CLI

Ako si zabezpečiť pohodlnú prácu v prostredí Cisco IOS CLI

V tomto vydaní Newsletter-a, by som Vás chcel zoznámiť so zaujímavými vlastnosťami príkazu `reload`. Mnohý z nás ho pozná len ako príkaz na „reštartovanie“ routera, no tento príkaz toho zvládne oveľa viac.

Stalo sa Vám niekedy, že ste pracovali s routerom na diaľku a po zadaní nepremysleného príkazu ste si „podpíli pod sebou konár“, čo malo za následok, že v okamihu ste stratili konektivitu na router, konkrétne na obsluhu porty ako `telnet`, `ssh` a `http`? Jediné východisko z tejto situácie, je osobne prísť k routeru opraviť konfiguráciu pomocou konzolového pripojenia.

V takomto prípade Vás vie príkaz `reload` ochrániť. Príkaz `reload` má aj ďalšie parametre, pomocou ktorých dokážeme napríklad reštartovať router až za určený časový interval, alebo dokonca na konkrétny dátum. Je to jednoduché! Stačí pred každým „nepredvídateľným“ príkazom zadať napríklad reštart o 2 minúty.

Príklad: Router# reload in 2

Syntax: reload in [hh:]mm

Následne sa Vás IOS opýta, či uložiť aktuálnu konfiguráciu, čo samozrejme potvrdíme. A teraz môžeme zadať náš

príkaz. V prípade, že by príkaz spôsobil niečo, čo by sme nechceli, tak router sa sám reštartuje po zvolenom časovom intervale do uloženej konfigurácie, ktorá nie je modifikovaná príkazom, ktorý sme zadali, čiže stačí počkať 2 minúty + dobu bootovania IOSu samého a môžeme pracovať ďalej.

V prípade ak príkaz nevykoná nič, čo by sme nechceli, stačí už len zrušiť automatický reload.

Príklad: Router# reload cancel

Ak by ste náhodou zabudli zrušiť automatický reload, tak IOS v určitých časových intervaloch oznamuje na všetky telnet a konzolové spojenia, že má dôjsť k reload-u.

Ak chceme naplánovať automatický reload na konkrétny deň, mesiac a hodinu, môžeme použiť príkaz `router at`.

Príklad: reload at 17:30 Feb 14

Syntax: reload at hh:mm [month day]

Všetky aktuálne nastavenia časovných reload-ov, môžeme skontrolovať príkazom `show reload`.

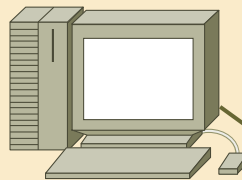
Prajem Vám pekný, reštartom nerušený deň.

Ahmed Al Hafoudh
študent na LCNA
SPŠE K. Adlera 5, Bratislava

Nápady pre NetAcad

Stačí len maličký krok a ... úspech je tu!

Problematika „sietí“ je niekedy naozaj náročná. Poznám študenta, ktorý úspešne absolvoval prvý semester CCNA. Snažil sa pred kamarátmi demonštrovať svoje vedomosti, no zlyhal na maličkom detaile – praktickým aplikovaní poznatkov na domácej sieti.

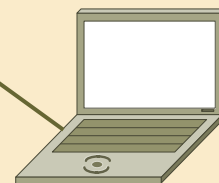


Chcel prepojiť dva počítače s operačným systémom Windows XP SP2. Počítače prepojil káblom, pridelil správnu IP adresu, spravil ping, ktorý fungoval a ... skončil! Nevedel totiž využiť aplikačnú vrstvu na prenos súborov medzi počítačmi.

Aby sa tomu predišlo, zaradil som na záver I. semestra cvičenie so zamieraním na zdieľanie súborov, kde ukážem nastavenie:

- zdieľania k súboru/zložke,
- prístupových práv pre sieťových používateľov,
- nastavenie vlastností Windows Firewall.

Pre počítače s Linuxom poviem o ftp a iných možnostiach zdieľania. Ak patríte tiež do skupiny neistých, pozrite si napríklad stránky www.theelderageek.com a www.microsoft.com, alebo do vášho obľúbeného vyhľadávča napíšte dopyt „how to share files windows XP SP2“. Veď sa učíme riešiť praktické úlohy!



Využite sieť vo svoj prospech a staňte sa úspešní s projektom NetAcad!

Július Baráth
Hlavný kontakt
RCNA pri akadémii ozbrojených síl
gen. M.R. Štefánika, Liptovský Mikuláš



CISCO UNIVERSITY NETWORKING TECHNOLOGY ROADSHOW & STUDENT FAIR

Druhý a tretí z pripravovanej série workshopov "Moderné sieťové technológie a technologické platformy Cisco" na vybraných univerzitách v SR sa uskutočnili dňa 21. a 28. februára 2007 na významných technických univerzitách v SR (RCNA na Žilinskej univerzite a RCNA na STU Bratislava).



Cieľom organizácie workshopov bola prezentácia možností budovania kariéry sieťových špecialistov na báze NetAcad a prezentácia najnovších sieťových technológií, technologických platforiem a riešení spoločnosti Cisco.

O celodenné workshopy bol medzi študentmi veľký záujem. Celkovo sa na Roadshow v Košiciach (7.12.2006), v Žiline (21.2.2007) a v Bratislave (28.2.2007) zúčastnilo viac ako 250 účastníkov – prevažne študentov vyšších ročníkov univerzít. Program všetkých troch Roadshow bol tvorený zaujímavými prednáškami, v rámci

ktorých boli prezentované možnosti budovania kariéry sieťového profesionála.

Peter Mesjar, ktorý ako prvý študent v SR získal už počas štúdia certifikát CCIE, prezentoval svoje skúsenosti a opísal svoju doterajšiu životnú kariéru (ako sa práve prostredníctvom programu NetAcad dostal k tejto významnej sieťovej certifikácii). V rámci programu vystúpila aj **Sedef M. Buyukataman**, ktorá prezentovala program Cisco ASR. Veľký ohlas malo aj vystúpenie dvoch súčasných účastníkov programu ASR, ktorí boli do programu vybraní v roku 2006 a v súčasnosti končia ročný pobyt v Amsterdame (**T. Kelemen, P. Skakala**).

Pozornosť vzbudili aj prezentácie M. Rempera: Progresívne riešenie bezdrôtových sietí pre akademickú sféru a K. Bakšovej: Konceptia budovania bezpečných sieťových riešení. Študentov zaujali aj príbehy uvedených prezentujúcich o tom, ako sa vlastne dostali k sieťam a k práci v Cisco vôbec. **Michal Remper** (CCIE) sa začal zaoberať sieťami až po ukončení štúdia v úplne inom odbore. **Klaudia Bakšová** je absolventkou filozofickej fakulty



so zameraním na výučbu angličtiny. Ako angličtinárka sa zamestnala u jedného z partnerov Cisco a po niekoľkých rokoch vyučovania angličtiny zmenila svoju profesiu a úspešne začala študovať sieťovú problematiku. V súčasnosti obaja pracujú v spoločnosti Cisco v Bratislave ako špecialisti.

Prednášky bolo možné tradične sledovať aj prostredníctvom videokonferenčného prenosu, pričom z jednotlivých prezentácií boli pripravené záznamy, ktoré sú pre záujemcov voľne dostupné na: <http://videosever.cnl.tuke.sk>. Úroveň Roadshow bola vysoko hodnotená všetkými univerzitami, pričom prejavili veľký záujem o podobné aktivity v budúcnosti.

Pavol Segeč

Hlavný kontakt
RCNA pri Žilinskej univerzite

VTIPY ©

Koľko **PC-čkárov** potrebujete k výmene žiarovky? 100. Jeden vymení žiarovku a 99 sa bude podieľať na výrobe príručiek: „Začínáme s výmenou žiarovky“, „Výmena žiarovky pre pokročilých“, „Technické parametre žiaroviek“, „Registračný formulár“, „Lokalizácia pre strednú v východnú Európu“, ...

Koľko **programátorov** potrebujete k výmene žiarovky? Žiadneho. Je to problém hardwaru.

Koľko **hardwarových odborníkov** potrebujete k výmene žiarovky? Žiadneho. Prehlásia, že diagnostické testy sú v poriadku, takže je to chyba softwaru.

Koľko **inžinierov z veľkej IT spoločnosti** potrebujete k výmene žiarovky? Žiadneho. Marketingové oddelenie prehlási, že prasknutá žiarovka je nový trend, a týmto smerom sa bude vývoj uberať. Alebo spoločnosť vyhlási tmu ako štandard.



<http://www.funehumor.com>
"You should check your e-mails more often. I fired you over three weeks ago."



CISCO OLYMP 2007

Medzinárodná súťaž študentov programu NetAcad.

➤ Si dobrý/á v počítačových sieťach?

➤ Si študentom programu NetAcad?

➤ Chceš vyhrať skvelé ceny
a získať nové možnosti
pre svoju kariéru?

Zisti viac na
www.netacad.sk

