Cvicenie12

OBSAH

Úloha 0: Nahlásenie opravných testov a konštruktívna kritika [editovať]

Ak vaše skóre z niektorého minulého testu (testy 1-11, alebo bonusové body za účasť na prednáškach, alebo body za DÚ) nie je ešte doriešené (napríklad mali ste zle formulovanú otázku, alebo chybnú otázku, alebo systém vám nesprávne spočítal body a pod.), konštruktívnu kritiku prijímame najneskôr do začiatku 12. týždňa. Neskôr už reklamácie neprijímame.

Po tomto cvičení, najneskôr však do nedele 23:55 je potrebné nahlásiť, ktoré testy si budete opravovať v 13. týždni v čase vášho cvičenia. Každý študent si môže opraviť max. 3 testy, započítava sa posledný pokus v teste, nie vyššie skóre.

- Opravou nazývame aj písanie takého testu, ktorý študent v riadnom termíne na cvičení vôbec nepísal.
- Ak študent napríklad vôbec nepísal testy č. 5 a 7, potom si zrejme vyberie na "opravu" tieto dva testy č. 5 a 7, a okrem nich si ešte môže opraviť max. jeden, v ktorom získal nízke skóre - - - tak aby opravoval spolu max. tri testy
- Pre zjednodušenie manažovania opravných testov Vám prvé pokusy na testoch nemažeme, ale zvýšili sme počet možných pokusov na každý test na dva. Systém Vám pre daný test zaráta posledný pokus (t.j. nie vyššie skóre z oboch pokusov). Ak si študent týmto spôsobom opraví viac ako 3 testy (t.j. nedodrží dohodnuté pravidlo), nebude pripustený ku skúške (pri distančnom vyučovaní - nebude mu zapísaná známka z predmetu, aj keď bude mať dostatočný počet bodov, pre porušenie pravidiel) - - - vieme si pozrieť dátumy vašich pokusov na testoch, preto Vás žiadame, aby ste sa takýmto špekuláciám vyhýbali.

Nahlásiť si testy, ktoré chcete opravovať, sa dá na hlavnej stránke Moodle, v 12. týždni: Tu si vyberiete max. 3 testy, ktoré chcete opravovať v 13. týždni (pridáme čoskoro, najneskôr 10.5.2022, pošleme echo do Teamsu)

DU_12 (Upozornenie k nasledujúcim úlohám 1-3)
Nasledujúce úlohy 1-3, ktorých stručný popis nájdete nižšie sme integrovali do jednej **.pka** topológie, ktorá je **hodnotená**, bodovaná 3 bodmi, a odovzdáva sa do nedele pol noci v týždni keď bola zadaná. Konkrétne inštrukcie nájdete po otvorení pka súboru, v okne, ktoré sa Vám otvorí spolu s topológiou (Inštrukcie / Instructions). V každej topológii sa generujú náhodné premenné, a tým, je každá topológia jedinečná. Erasmus študenti majú inštrukcie v extra Word dokumente, s anglickým prekladom, ale upozorňujeme, že konkrétne hodnoty treba pozrieť priamo v pka v časti Instructions, pretože sa generujú náhodne (do budúcna toto upravíme, a dáme anglickú mutáciu priamo do pka do Instructions).

Odovzdáva sa **pka** súbor, v ktorom **názov súboru**, ktorý si stiahnete z odkazu nižšie nijako nebudete meniť, iba na jeho koniec pridáte: **_Priezvisko_Meno** (t.j. za pôvodný názov súboru, a príponu pka samozrejme ponecháte, nepoužívajte v Priezvisko_Meno diakritiku, ak máte viac mien, použite to prvé, ak máte viac priezvisko, zadajte z nich to posledné).

Po otvorení pka súboru zadajte do **User profile:**

-
  - Name zadajte svoje: **Priezvisko_Meno** (bez diakritiky, pričom študenti s viac menami uvedú prvé meno, a tí s viacerými priezviskami, uvedú posledné priezvisko)
  - E-mail: ***login*@stud.uniza.sk** (namiesto *login* zadajte to čo máte vo vašom študentskom e-maile)
  - Additional info: **2023** (zadajte aktuálny rok)

inak vám riešenie nebude uznané.
Topológia: PIKS_LAB_12_CDP_SSH_Backup_TFTP_2023_04_25.pka
Inštrukcie:

- v slovenčine: priamo v PT aktivite, po otvorení súboru, v extra okne
- v angličtine: PIKS_LAB_12_CDP_SSH_Backup_TFTP_EN_2023_04_25_instructions.docx

Úloha 1: Využitie protokolu CDP na odhalenie sieťovej topológie
[editovať]

Cisco Discovery Protocol (CDP) je proprietárny protokol, ktorý pracuje na druhej vrstve sieťového modelu OSI. Tento linkový protokol slúži na získavanie informácií o priamo pripojených susedných sieťových zariadeniach k smerovaču alebo prepínaču. Dopomáha získať prehľad o komplexnej topológií celej siete.

Protokol však vysiela po sieti CDP rámce. Pre zvýšenie bezpečnosti je vhodné v prípadoch, kedy nie je protokol CDP nevyhnutný, v záujme zníženia bezpečnostného rizika deaktivovať protokol globálne alebo aspoň na portoch kde existuje akékoľvek riziko zneužitia protokolu. Prvým z možných útokov je zachytenie CDP rámcov útočníkom. Z informácií nesených týmto rámcom môže útočník odhaliť topológiu siete. Druhým možným útokom je vysielanie podvrhnutých rámcov. Útočník sa na sieti môže vydávať za smerovač alebo prepínač. Posledným z útokov je realizácia DoS útoku s využitím CDP rámcov. Cieľom je zahltiť sieťové zariadenie a spôsobiť jeho nedostupnosť, poprípade vyvolať výpadok konzolového pripojenia či pripojenia vzdialeného prístupu.

Preskúmajte fyzickú topológiu siete pomocou príkazov:

- **ipconfig /all** - zistíme IP, masku siete, GW
- **telnet** - na GW, heslo: cisco
- **show version** - Cisco 1841
- **show ip interface brief** - mená lokálnych interfejsov a ich IP adresy
- **show protocols** - aj masky sietí (192.168.0.25/30)
- **show cdp neighbors** - mená susedov a lokálne a vzdialení porty
- **show cdp neighbors detail** - IP adresy susedov (ta tie sa dá pripojiť cez telnet)
- **ping 255.255.255.255** - z R - odpovedia všetci susedia aj PC (skutočné W7 má vo FW defoltne zakázané odopvedať na ping)

Vašou úlohou je:

1. **Nakresliť** ako vyzerá celková topológia (vo Worde).
2. Zistiť počet zariadení v skrytej časti topológie.
3. Vyplniť tabuľku s informáciami, ktoré zistíte o zariadeniach (tabuľku si skopírujte do Wordu):

Hostname	Model zariadenia	IP adresa	Maska	Rozhranie

Úloha 2: Konfigurácia SSH [editovať]

Riešiť ju začínate na cvičení, kto nestihne celú, dorieši doma.

Úloha 3: Záloha konfiguračných súborov a show príkazy [editovať]

Po tejto úlohe,

je možné ako opakovanie a prípravu na skúšku, overiť si na smerovači v danej topológii výpisy týchto show príkazov:
show arp
show flash:
show ip route
show interfaces
show ip interface brief
show protocols
show users
show version

1. Which commands would provide the IP address, network prefix, and interface?

_____

_____

2. Which commands provide the IP address and interface assignment, but not the network prefix?

_____

_____

3. Which commands provide the status of the interfaces?

_____

_____

4. Which commands provide information about the IOS loaded on the router?

_____

_____

5. Which commands provide information about the addresses of the router interfaces?

_____

_____

6. Which commands provide information about the amount of and Flash memory available?

_____

_____

7. Which commands provide information about the lines being used for configuration or device monitoring?

_____

_____

8. Which commands provide traffic statistics of router interfaces?

_____

_____

9. Which commands provide information about paths available for network traffic?

_____

_____

10. Which interfaces are currently active on the router?

_____

_____

Ďalšie úlohy k téme, pre rýchlejšie skupiny študentov (skupina A):

Úloha 4: Preskúmanie sieťových bezpečnostných hrozieb [editovať]

Administrátor siete sa vždy musí zaoberať aj otázkou bezpečnosti danej siete, a mal by byť informovaný o externých hrozbách, ktoré môžu byť pre jeho sieť a používateľov v nej nebezpečné. Na identifikáciu najnovších hrozieb môže využiť web stránky, ktoré sa intenzívne zaoberajú otázkou bezpečnosti a poskytujú aj možnosti pre ochranu proti takýmto hrozbám.

Jednou z takýchto stránok je SANS, SysAdmin, Audit, Network, Security, populárna a dôveryhodná stránka o tom, ako sa chrániť pred počítačovými a sieťovými bezpečnostnými hrozbami. Poskytuje rôzne zdroje:

- Zoznam: „20 Critical Security Controls for Effective Cyber Defense" (tento zoznam pripravuje CIS – Center for Internet Security)
- Týždenník o nových sieťových útokoch a hrozbách: @Risk: The Consensus Security Alert newsletter.

1. Preskúmajte web stránku **SANS**: https://www.SANS.org > hlavné horné menu: **Resources**
   - Čo všetko je v tejto ponuke? (prezrite si všetkých 13 odkazov v Resources)
2. Prejdite potom na podmenu: **The Critical Security Controls** (Top 20)
   - Top 20 Critical Security Controls sú odporúčanou sadou akcií pre počítačovú ochranu, ktorá poskytuje špecifické a proaktívne spôsoby, ako zastaviť dnešné najrozšírenejšie a nebezpečné útoky. Pracujú na tom rôzne štátne aj súkromné organizácie prevažne z US (Department of Defense (DoD), National Security Association, Center for Internet Security (CIS), SANS Institute):
   - Hlavným kľučom k atuálnosti je to, že táto sada je aktualizovaná na základe nových útokov, ktoré sú identifikované a analyzované viacerými skupinami, napr. Symantec, ESET (pre nás známy), a mnohé iné.

- Zistite, aké produkty ponúka firma Cisco pre oblasti kontroly CS1, CS8, CS12, CS15 a CS19.
  - SANS hlavné horné menu > Resources > The Critical Security Controls > CS1 .... CS20.
  - Vypíšte produkty, ktoré ste tam našli a pokúste sa o nich zistiť niečo viac na stránke Cisco tu (http://www.cisco.com/c/en/us/products/security/product-listing.html).

3. Zistite, kedy a kde (ako ďaleko od nás) je najbližší **tréning „Cyber Security"**.
   - SANS hlavné horné menu > Live Training > Upcoming Events
4. Preskúmajte 3 dostupné **Newsletters** na stránke SANS.
   - SANS hlavné horné menu > Resources >Newsletters.
     - SANS NewsBites - A high level summary of the most important news articles that deal with computer security. The newsletter is published twice a week and includes links for more information.
     - @RISK: The Consensus Security Alert - A weekly summary of new network attacks and vulnerabilities. The newsletters is also provides insights on how recent attacks worked.
     - Ouch! – A security awareness document that provides end users with information about how they can help ensure the safety of their network.
5. Preskúmajte stránku **CIS**
   - CIS je skratka pre Center for Internet Security, ktorého náplňou je:
     - Identifikovať, vyvíjať, overovať, poskytovať a udržiavať "best practices" pre bezpečnosť v Internete
     - Poskytovať bezpečnostné riešenia celosvetovo a robiť tak prevenciu, resp. rýchle reakcie na bezpečnostné útoky
     - Budovať a viesť komunity pre vytvorenie dôveryhodného priestoru v Internete.
   - Poskytuje zoznam: **20 Critical Security Controls** [www.cisecurity.org > CIS Critical Security Controls > Overview > dole PDF alebo Excel]
     - na stiahnutie v PDF alebo v Exceli - je potrebné sa registrovať na ich stránke mailom - aby ste toto nemuseli robiť, tu sme pre vás stiahli tento zoznam s aktuálnosťou k dátumu 15.5.2016: stiahnite si tu.
     - Preskúmajte podrobnejšie oblasti kontroly CS1, CS11 a CS15.
       - Vyučujúci Vám pridelí jednu podoblasť a budete ju mať naštudovať a vlastnými slovami v niekoľkých vetách (1-5) vysvetliť ostatným.
       - Najprv 2-5 min príprava
       - Potom každý odprezentuje svoju podoblasť, v poradí ako nasledujú za sebou (jednotlivo alebo v menších skupinkách).

6. Identifikujte **aktuálne sieťové bezpečnostné hrozby**
    - Skúmať ich možno z rôznych zdrojov, napríklad:
        2.
        - Z Newslettra na stránke SANS:
            - @Risk: Consensus Security Alert Newsletter
            - Z archívu si vyberte najaktuálnejšie číslo a preskúmajte časti:
                - RECENT VULNERABILITIES FOR WHICH EXPLOITS ARE AVAILABLE
                - MOST PREVALENT MALWARE FILES
            - Prezrite si ako funguje útok Enterprise Survival Guide for Ransomware Attacks
        - Doma preskúmajte aj ďalšie externé stránky a zistite aké podrobné info poskytujú o aktuálnych bezpečnostných hrozbách:
            - www.symantec.com
            - http://www.eset.com/sk/
            - www.mcafee.com/us/mcafee-labs.aspx
            - http://www.cnet.com/topics/security/
            - www.sophos.com/en-us/threat-center/
            - us.norton.com/security_response/
7. Otázky na záver:

- Akými krokmi (akciami) si viete zabezpečiť svoj osobný počítač proti bezpečnostným útokom?
- Akými krokmi vie organizácia (firma, škola, ..) zabezpečiť jej zdroje proti bezpečnostným útokom?

Domáca úloha 2: Cvičné komplexné zadanie na skúšku. [editovať]

Vysoko odporúčame študnetom pri príprave na praktickú časť skúšky vyriešiť si toto nami vytvorené zadanie v programe PT --- počkajte na aktualizáciu pre tento školský rok - uverejníme najneskôr 10.5.2022.

Veľmi vhodné sú aj "Skill Integration" zadania z portálu Netacad, výber najvhodnejších zadaní uvádzame tu.