IPK - Počítačové komunikace a sítě

Projekt č.2

Varianta termínu - Varianta 2: DHCP Starvation útok (Veselý)

Popis:

ZADÁNÍ:
Vašim úkolem je:
[1] Nastudovat problematiku DHCP útoků a relevantní informace uvést v projektové dokumentaci. (až 6 bodů)
[2] Naprogramovat aplikace realizující DHCP Starvation útok, který by vyčerpal adresní pool legitimního DHCP serveru; (až 12 bodů)
[3] Demonstrovat činnost aplikací v podmínkách Vaší vlastní testovací sítě. (až 2 body)

KONVENCE ODEVZDÁVANÉHO ZIP ARCHIVU xlogin00.zip

- dokumentace.pdf - výstupy zadání [1] a [3]
- readme - základní informace, případná omezení projektu
- Makefile
- *.c, *.cpp, *.cc, *.h - zdrojové a hlavičkové soubory výstupů zadání [2]

DOPORUČENÍ/OMEZENÍ:

- !!! Vzhledem k nátuře projektu se NEDOPORUČUJE projekt testovat na živé fakultní či kolejní síti. Provoz generovaný vašimi aplikacemi může být vyhodnocen jako bezpečnostní incident !!!
- K ad hoc testování použijte vaši domácí síť či si neváhejte vytvořit pomocí virtualizačních prostředí jako VirtualBox či VMWare Workstation jednoduchou laboratoř (např. 3×VM pro dvě oběti a jednoho útočníka) s uzavřeným síťovým segmentem (interní virtuální síťový adaptér). Pokud jste ještě nikdy nevirtualizovali, třeba vám pomůže následující článek http://www.brianlinkletter.com/how-to-use-virtualbox-to-emulate-a-network/.
- S blížícím se deadlinem projektu vám bude nabídnuta možnost otestovat si projekt v podmínkách laboratoře C304, kde pro vás bude připravena typizovaná síť s IPv4 konektivitou a několika oběťmi. Tuto nabídku berte jako vsřícné gesto, kdy máte možnost probrat s opravujícím Vaše případné dotazy; vaše (ne)účast na tomto hromadném sedánku není nijak vázána na Vaše výsledné hodnocení, protože nedílnou součástí zadání je, že byste si sami měli být schopni postavit testovací síť k tomuto projektu (ať už virtuální, a nebo reálnou).
- Implementované konzolové aplikace budou povinně v jazyce C/C++, využít můžete libovolné v systému dostupné standardní knihovny.
- Všechny implementované programy by měly být použitelné a řádně komentované. Pokud už přejímáte zdrojové kódy z různých tutoriálů či příkladů z Internetu (ne mezi sebou pod hrozbou ortelu disciplinární komise), tak je POVINNÉ správně vyznačit tyto sekce a jejich autory dle licenčních podmínek, kterými se distribuce daných zdrojových kódů řídí. V případě nedodržení bude na projekt nahlíženo jako na plagiát!
- Pro snadné parsování vstupních argumentů se doporučuje použít funkci getopt().
- Aplikace reagují korektním ukončením na SIGINT signál (tedy Ctrl+C).
- Počítejte s tím, že při opravování bude projekt testován na PC s Ethernetovým rozhraním vůči topologii s fyzickými zařízeními v laboratoři C304.
- Výsledky vaší implementace by měly být co možná nejvíce multiplatformní mezi OS založenými na unixu, ovšem samotné přeložení projektu a funkčnost vaší aplikace budou testovány na referenčním http://nes.fit.vutbr.cz/isa/ISA2015.ova pro předmět ISA, kterýžto bude sloužit jako virtuální mašinka s pravděpodobně jedním síťovým rozhraním.
- Projekt bude opravován ručně. Počítejte tedy s nejzazším možným termínem oprav a reklamací určených garantem předmětu.

- Do doprovodného souboru readme.txt uveďte případná omezení funkcionality vašeho projektu - na dokumentovanou chybu se rozhodně nahlíží v lepším světle než na nedokumentovanou!

UPŘESNĚNÍ ZADÁNÍ:

Ad [1]

V dobré dokumentaci se očekává následující: titulní strana, obsah, logické strukturování textu, výcuc relevantních informací z nastudované literatury, popis zajímavějších pasáží implementace, demonstrace činnosti implementovaných aplikací, normovaná bibliografie.

Přepisovat Wikipedii do teoretické části dokumentace není ideální. Pokuste se především vlastními slovy vysokoškoláka doplněnými vhodnými obrázky vysvětlit, o čem útoky spojené s DHCP jsou. Než na kvantitu bude se přihlížet hlavně ke kvalitě textu.

Ad [2]

Cílem aplikace je pomocí DHCP Discover zpráv vyčerpat adresní pool legitimního DHCP serveru tak, aby po spuštění aplikace už žádný nový klient nedostal DHCP výpůjčku.

Konvence jména aplikace a jejích povinných vstupních parametrů:

./ipk-dhcpstarve -i *interface*

- *interface* (řetězec) jméno rozhraní dle OS, na které útočník vygeneruje patřičný provoz s kompromitačními účinky na DHCP server;

Ad [3]

Demonstraci činnosti uveďte jako samostatnou kapitolu v dokumentaci. Nezapomeňte uvést specifika testované sítě (obrázek topologie, adresace) a vybrané výstupy při činnosti vašich aplikací validující a verifikující funkčnost.

Při testování vašich aplikací se chovejte zodpovědně! Některé sítě mohou na vámi implementované aplikace reagovat obranným způsobem. Ohledně tohoto si přečtěte informace související s pojmem DHCP Snooping.

LITERATURA:

- R. Droms, RFC 2131:*Dynamic Host Configuration Protocol*, https://tools.ietf.org/html/rfc2131
- Let's Explain, *DHCP Starvation (DOS Attack - Penetration Testing) - Example Demonstration with Kali*, http://letusexplain.blogspot.cz/2015/10/dhcp-starvation-denial-of-service.html
- P. Straatsma, *Network Takedown Part 2: Rogue DHCP Server with DHCP Starvation and Rogue Routing*, http://www.hackandtinker.net/2013/11/27/going-rogue/
- P. Bouška, *Cisco IOS 13 - DHCP služby na switchi*, https://www.samuraj-cz.com/clanek/cisco-ios-13-dhcp-sluzby-na-switchi/
- E. Banks, *Five Things To Know About DHCP Snooping*, http://packetpushers.net/five-things-to-know-about-dhcp-snooping/
- M. Harris, *DHCP Snooping: Basic Concepts and Configuration*, http://www.pearsonitcertification.com/articles/article.aspx?p=2474170