elektrorevue
ISSN 1213 - 1539

Rok / Year:	Svazek / Volume:	Číslo / Number:	Jazyk / Language
2020	22	1	CZ

Přehled kybernetických útoků na linkové a transportní vrstvě

Overview of cyber attacks on the link and transport layer

David Hirš, Zdeněk Martinásek

{xhirsd00, martinasek}@feec.vutbr.cz

Fakulta elektrotechniky a komunikačních technologií VUT v Brně

DOI: -

Abstract: Currently, there are many cyber-attacks within computer networks. In local networks, attacks aimed at eavesdropping/modifying data communications (man in the middle), spoofing basic network parameters, unauthorized manipulation of network segmentation protocols, or denial of service threat users. These attacks and their combinations typically escalate to more dangerous attacks that are already targeted to application protocols of end user (such as HTTPS (Hypertext Transfer Protocol Secure)). This article focuses on current state analyses of cyber-attacks, that are realized on the link, network or transport layers (L2 to L4). The main goal of the article is present attacks within the basic detection mechanisms that can be signature based or anomaly detection based. The last contribution of the article is the evaluation of the possible impact of the attacks and the description of basic mitigation mechanism.

elektrorevue
ISSN 1213 - 1539

Přehled kybernetických útoků na linkové a transportní vrstvě

David Hirš, Zdeněk Martinásek

Fakulta elektrotechniky a komunikačních technologií VUT v Brně
Email: xhirsd00@feec.vutbr.cz, martinasek@feec.vutbr.cz

Abstrakt *– V současnosti existuje mnoho kybernetických útoků v rámci počítačových sítích. V lokálních sítích hrozí uživatelům zejména útoky cílené na odposlech/modifikaci datové komunikace (mužem uprostřed), podvržení základních síťových parametrů, neoprávněnou manipulaci s protokoly pro segmentaci sítě nebo odepření služeb. Tyto útoky a jejich kombinace typicky eskalují na nebezpečnější útoky, které jsou již cílené na aplikační protokoly HTTPS (Hypertext Transfer Protocol Secure) koncových uživatelů. Jako nejznámější útoky, které vzniknou kombinací útoku na nižší a aplikační vrstvě lze zmínit SSLstrip nebo SSLsplit. Tento článek přehledně analyzuje současný stav kybernetických útoků, které jsou realizovány na spojové, síťové a transportní verstě (L2 až L4) a umožňují tak různé kombinace útoků. Cílem článku je přehledně uvést jednotlivé útoky včetně detekčních mechanizmů, které využívají vytvořené vzory, popřípadě model pro detekci anomálií. Posledním přínosem článku je hodnocení možného dopadu jednotlivých útoků a popis protiopatření eliminující kybernetický útok.*

1 Úvod

Rizika kybernetických útoků na informační a komunikační systémy státní správy, komerčních firem i běžných koncových uživatelů představují v dnešní době reálnou hrozbu. Dopadem útoků jsou finanční ztráty způsobené ztrátou citlivých informací. V současnosti existuje mnoho kybernetických hrozeb a útoků v rámci počítačových sítích, které mohou mít externí a interní charakter. Interní útoky snažící se o manipulaci a spoofing parametrů vedené z kompromitovaných vnitřních síťových entit a z koncových stanic mohou být velmi nebezpečné a těžko detekovatelné na vyšších vrstvách modelu OSI/ISO [1]. Model OSI/ISO sestává ze sedmi vrstev označovaných L1 až L7. Popis modelu není předmětem tohoto článku, ale útoky jsou z důvodu přehlednosti zařazeny do vrstev modelu.

V lokálních sítích (LAN - Local Area Network) hrozí uživatelům nespočet kybernetických útoků, ale zejména útoky cílené na odposlech/modifikaci datové komunikace (mužem uprostřed), podvržení základních síťových parametrů, neoprávněnou manipulaci s protokoly pro segmentaci sítě nebo odepření služeb. Tyto útoky a jejich kombinace typicky eskalují na nebezpečnější útoky, které jsou již cílené na aplikační protokoly HTTPS (Hypertext Transfer Protocol Secure) koncových uživatelů. Jako nejznámější útoky které vzniknou kombinací útoku na nižší a aplikační vrstvě lze zmínit SSLstrip. Při tomto útoku se útočník dostane podvržením síťových parametrů mezi oběť útoku a webový server (útok mužem uprostřed), následně přeposílá veškerou datovou komunikaci s webovým serverem v otevřené podobě, tedy s použitím nezabezpečeného protokolu HTTP (Hypertext Transfer Protocol). Realizace tohoto útoku je jednoduchá, ale může mít fatální následky. Realizace útoku spočívá v nezabezpečení protokolů nižších vrstev L2 až L4, například které zaručují doručení rámce koncové stanici.

Tento článek přehledně analyzuje současný stav kybernetických útoků, které jsou realizovány na spojové, síťové a transportní verstě (tedy L2 až L4 modelu OSI/ISO) a umožňují tak kombinaci útoků v nebezpečnější varianty s vyšším dopadem na aktiva. Cílem článku je přehledně uvést jednotlivé útoky včetně možných detekčních mechanizmů, které využívají vytvořené vzory (signatury) popřípadě model pro detekci anomálií. Signatury si lze představit jako vzor typického chování pro daný útok (jak útočník postupuje). Dojde-li k zjištění shody aktuálních událostí se známou signaturou útoku, zařízení pro detekci a prevenci útoků provede definované kroky k zamezení probíhajícího útoku. V případě realizace útoku, jehož signatura není známa, se používají modely normálního chování uživatelů a detekce odchylek od tohoto chování (detekce anomálií). Dále článek analyzuje bezpečnostní mechanizmy, které je možné použít k eliminaci těchto útoků například na hraničních síťových prvcích. Posledním přínosem článku je hodnocení složitosti útoku a možného dopadu. Hlavním přínosem článku je tak vytvořená tabulka (tabulka A) představující souhrn útoků, ohodnocenou složitost realizace spolu s hodnocením vážnosti dopadu jejich uskutečnění, způsob možné detekce a mitigace.

2 Analýza kybernetických útoků L2 až L4

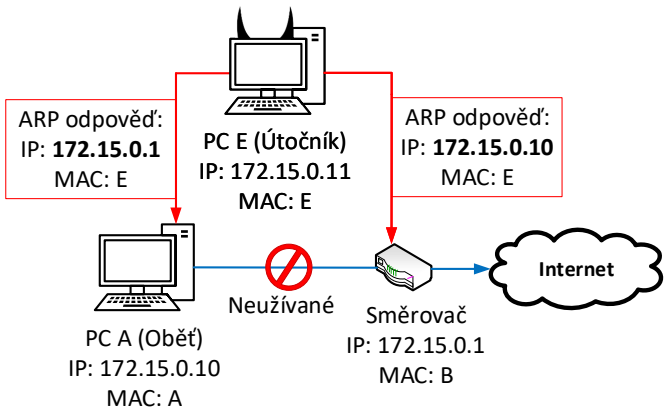
Následující text obsahuje přehled kybernetických útoků, které jsou realizovány na vrstvách L2 až L4 modelu OSI/ISO. Vytvořená analýza se zaměřuje výhradně na útoky, které je možné detekovat na základě vytvořených vzorů (detekce využívající signatury). Kybernetické útoky, které jsou detekovány na bázi modelu (detekce využívající anomálie) budou obsahem navazujícího článku z důvodu omezení počtu stran.

elektrorevue
ISSN 1213 - 1539

2.1 Podvržení ARP zpráv

Protokol ARP (Address Resolution Protocol) slouží k získání linkové adresy síťového rozhraní (MAC - Media Access Control) příjemce ve stejné podsíti pomocí známé IP (Internet Protocol) adresy [2]. ARP nedisponuje bezpečnostním mechanismem (př. kontrola autentičnosti), a proto jeho všesměrové dotazy a odpovědi může kdokoli podvrhnout (útok ARP spoofing/poisoning). Útočník tímto způsobem získá přístup k datům uživatele, který je nevědomky odesílá útočníkovi.

Útoky založené na napadení ARP protokolu modifikují nebo vytváří falešné ARP zprávy (požadavky a odpovědi). Takto dochází k přesměrování komunikace uvnitř sítě LAN (Local Area Network) [3]. Útočník se může vydávat za zařízení s hledanou IP adresou a přesvědčit tak odesílatele, že on je hledaným příjemcem. Útočník toho může docílit dvojím způsobem, a to odesíláním ARP dotazu, nebo ARP odpovědi. Tyto podvržené zprávy musí být útočníkem periodicky odesílány, jinak dochází k samovolnému opravení ARP tabulky pomocí nepodvržených ARP zpráv v LAN. V případě, kdy útočník „otráví“ ARP tabulku obou uživatelů, veškerá jejich komunikace probíhá přes něj a stává se tak snadno čitelnou či modifikovatelnou. Výsledkem je realizace MitM (Man in the Middle). Schéma útoku MitM využívající otravu ARP tabulky je uveden na obrázku 1. Komunikující strany jsou označeny jako Oběť, Směrovač a Útočník. Útočník periodicky vysílá podvrženou ARP odpověď Oběti i Směrovači (označují červené šipky), čímž dosahuje MitM. Další případ představuje „otrávení“ ARP tabulky jednostranně (přesměrování pouze jednoho směru komunikace), například přesměrování Oběti na vlastní webový server. Útočník „otráví“ jen ARP tabulku Oběti a útok je označován jako „Host impersonation attack“. Dalším možným použitím tohoto útoku je realizace odepření služby. V tomto případě, útočník cíleně zahazuje datovou komunikaci uživatele pro specifickou službou, dopadem je že daná služba je pro uživatele nedostupná. Obecně jsou takovéto útoky označovány jako útoky cílené na odepření služeb (DoS - Denial of Service).



Obrázek 1: Provedení MitM a následný odposlech či změna procházejících dat.

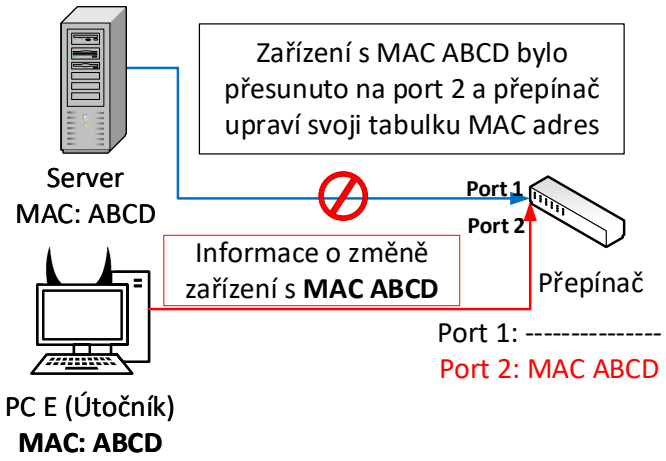
Protiopatření má za cíl zabránit modifikovanému ARP požadavku průchod sítí LAN. Lze využit bezpečnostní funkci síťových přepínačů nazývanou DHCP (Dynamic Host Configuration Protocol) Snooping [4]. Tato funkce primárně zabezpečuje protokol DHCP tím, že zahazuje DHCP rámce, které přichází od nedůvěryhodných DHCP serverů. DHCP Snooping může pomoci i při detekci modifikovaných ARP zpráv. Vytváří tzv. DHCP Snooping Binding table, což je tabulka obsahující svázané IP a MAC adresy jednotlivých zařízení v síti LAN, které byly přiřazeny důvěryhodným DHCP serverem. Dynamickou kontrolu ARP požadavků obstarává Dynamic ARP Inspection a jejich obsah porovnává s vytvořenou DHCP Snooping Binding table. Pokud obsah požadavku nesouhlasí, dochází k jeho zahození. Dynamic ARP Inspection pro kontrolu svázaných adres může využít také statickou tabulku, která je manuálně nakonfigurovaná. Manuální konfigurace je však časově náročná úloha a nevhodné řešení při středních a velkých sítích.

Další možnou formou protiopatření je úprava samotného ARP protokolu a vytvoření zabezpečeného S-ARP (Secure Address Resolution Protocol). Tento navržený protokol a bezpečnostní přístup byl představen v článku [5] roku 2003. Protokol S-ARP zajišťuje autentizaci zpráv za pomocí asymetrické kryptografie a infrastruktury veřejných klíčů PKI (Public Key Infrastructure). Veškerá zařízení v síti LAN disponují vlastním veřejným i soukromým klíčem a certifikátem pro ověření jejich identity. Identitu představuje IP adresa. Certifikát také obsahuje IP a MAC adresu důvěryhodné stanice, která představuje AKD (Authoritative Key Distributor), neboli certifikační autoritu distribuující klíče pro tento protokol. Odpověď na ARP požadavek je podepsána soukromým klíčem odpovídajícího uživatele. Dotazující se stanice ověří podpis veřejným klíčem uživatele obsaženým uvnitř jeho certifikátu. Pokud certifikát neobsahuje veřejný klíč, je vyžádán od AKD. Odpovědi AKD jsou také podepsané. Pokud se podpis neshoduje, ARP odpověď je zahozena. Tvorbu digitálního podpis zajišťuje algoritmus DSA (Digital Signature Algorithm). Možnou hrozbu představuje Reply attack, avšak tomu je zamezeno pomocí časového údaje (razítka). Časové razítko distribuuje AKD a všechny stanice uvnitř sítě musí být časově synchronizovány.

2.2 Podvržení linkové adresy

Tyto útoky využívají možnosti snadného podvržení linkové adresy (MAC Address spoofing) a tím pádem se útočník vydává za někoho jiného. MAC adresa je teoreticky jedinečný identifikátor zařízení na L2 vrstvě, na jejímž základě lze doručit data od odesílatele k příjemci v LAN. Na základě tohoto chybného předpokladu, existence unikátního identifikátoru lze také řídit přístup do sítě LAN pomocí funkce filtrování na základě linkových adres (router má aktivovanou funkci MAC filtering). Tímto způsobem dojde k odepření přístupu do sítě zařízením, která nejsou uvedena v seznamu [6]. Toto za-

elektrorevue
ISSN 1213 - 1539



Obrázek 2: Princip útoku podvržením linkové adresy.

bezpečení lze jednoduše obejít právě pomocí útoku, který podvrhne linkovou adresu legitimního uživatele služby. Útočník nejprve odhalí MAC adresu legitimního uživatele s povoleným přístupem a to za pomoci softwarového nástroje např. Wireshark. V druhém kroku si útočník změní MAC adresu a vydává se za legitiního uživatele. Prakticky všechny operační systémy umožňují změnu MAC adesy. Podvržení linkové adresy lze také využít k provedení útoku na odepření služby. Útočník se vydává za stanici uvnitř sítě, ke které legitimní uživatelé hodlají přistoupit a daný požadavek o přístup zahodí [7]. Průběh útoku graficky znázorňuje obr. 2. Zde je červenou šipkou znázorněno odeslání informace o změně zařízení s MAC adresou ABCD, tedy adresou patřící Serveru.

Protiopatřením je opět DHCP Snooping [4]. Tato funkce byla popsána v předešlé části 2.1, a proto již nebude znovu představena. Jediným rozdílem je funkce IP Source Guard, která zde nahrazuje Dynamic ARP Inspection. Pro odhalení MAC address spoofing je nutné kontrolovat a porovnávat všechny přijímané rámce obsahující MAC adresu s DHCP Snooping Binding table. IP Source Guard kontroluje IP i MAC adresy. Podvržení linkové adresy lze zabránit i pomocí „odlehčených autentizačních agentů“, jak popisuje práce [8]. Zabezpečení pro celou síť LAN nastavuje autentizační server a přístup do této sítě je povolen pouze s validním agentem na klientském zařízení.

2.3 Přeskakování virtuální LAN

VLAN (Virtual Local Area Network) představuje virtuální lokální síť [9]. LAN je takto rozdělena do více VLAN, které logicky rozdělují síť a zařízení uvnitř. Komunikace dvou zařízení uvnitř různých VLAN je zakázaná a přepínač uvnitř sítě tyto pakety zahazují. Kybernetický útok označovaný jako přeskakování VLAN (VLAN hopping) má za cíl oklamání přepínače v síti tak, aby útočník získal přístup do jiné VLAN, než do které sám přísluší. Přístupem je myšlena komunikace se zařízením jiné VLAN [10, 11].

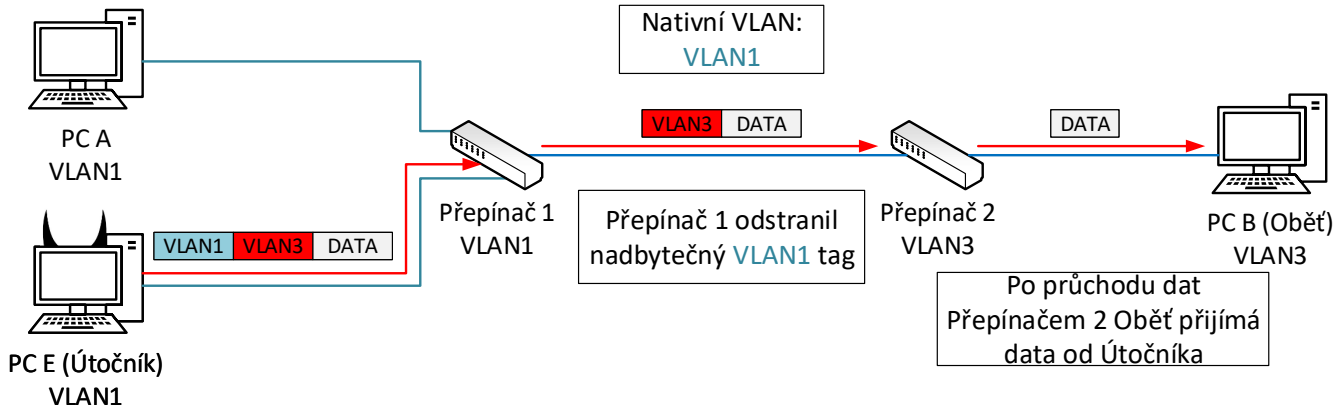
Princip útoku využívajícího přidání druhé značky (Double tagging) [10, 11], zobrazuje obrázek 3. Útočník chce odeslat data do *VLAN 3*, která je za běžných podmínek nedosažitelná. Pokud by datové rámce poslal pouze se značkou *VLAN 3* (802.1Q *tag*), přepínač by je ihned zahodil. Z tohoto důvodu útočník přidá k datovým rámcům ještě jednu značku, datové rámce tak mají dvě značky *VLAN 1* (povolená) a *VLAN 3* (nepovolená). První, přepínačem kontrolovaná značka, bude platný pro útočníkovi příslušnou *VLAN 1* a to způsobí předání rámce dál a odstranění značky. Rámec ale stále nese druhou značku, která ukazuje na cílovou VLAN označenou *VLAN 3*. Následující přepínač detekuje značku nesoucí hodnotu *VLAN 3* a rámec předá do cílené *VLAN 3*. Pro tento útok je klíčové, aby cesta k cílovému uživateli vedla alespoň přes dva přepínače. Dalším požadavkem je, aby značka označující VLAN útočníka a nativní VLAN přepínače byla nastavena na stejnou VLAN, v tomto případě *VLAN 1*. Pokud jsou obě hodnoty stejné, přepínač vyhodnotí značku jako nadbytečnou, a proto dochází k jejímu odstranění. Útočník je v tomto případě značně omezený, protože data může skrze síť jen odesílat, a tak může přikročit například k DoS útoku. Obrázek znázorňuje předání útočníkem generovaná data skrze dva přepínače, které odstraní jim příslušnou značku.

Druhým útokem patřícím do kategorie přeskakování virtuální LAN je podvržení přepínače (Switch spoofing) [10]. Útočník se vydává za přepínač a sjednává přenosy, což mu umožní přijímat a přeposílat rámce mezi odlišnými VLAN. Provedení je závislé na módu přepínače. Rámce DTP (Dynamic Trunking Protocol) slouží pro určení módu, ve kterém bude probíhat přenos rámců mezi dvěma sousedními přepínači. Útočník odešle DTP rámce přepínači a snaží se jej přesvědčit, že je novým přepínačem v síti. Pokud je přesvědčovaný přepínač v módu *Dynamic Auto, Dynamic Desirable, Trunk*, schválí útočníka jako nový přepínač a naváže s ním spojení. Útočník nyní, nehledě na vlastní příslušnost určité VLAN, může odesílat rámce do kterékoliv VLAN. V takovémto případě je možné vytvořit spojení s „Obětí“, a komunikovat bez zabezpečovacích protokolů vyšší, 3. vrstvy ISO/OSI. Naopak útok není realizovatelný v případě, kdy je přepínač v módu *Access*, a tedy všechny příchozí DTP rámce sousedních přepínačů zahazuje.

Protiopatření proti výše popsanému útoku lze realizovat definováním nepoužívané VLAN a její přiřazení jako nativní pro všechny přenosové cesty mezi přepínači [11, 12]. Toto nastavení způsobí, že všechny přepínače budou brát nativní značku nepoužívané VLAN. Útočník tak nemůže provést **Double tagging**, protože přepínač nevyhodnotí jeho *tag* jako redundantní. Další možností je změna protokolu používající *tag*, například na protokol ISL (Inter-Switch Link Protocol) [11].

Protiopatření proti **Switch spoofing** již bylo zmíněno v popisu útoku. Nejsnazší možností je zamezení dynamickému ustanovení přepínačů skrze DTP a nastavit jejich mód na *access*.

elektrorevue
ISSN 1213 - 1539



Obrázek 3: Průchod rámce do nepřístupné VLAN pomocí Double tagging útoku.

2.4 Zahlcení směrovací tabulky CAM

CAM (Content Addressable Memory) je fyzická paměť přepínače obsahující stejnojmennou tabulku, na základě které přepínač přepíná datovou komunikaci [12]. Tato tabulka obsahuje svázané MAC adresy koncových zařízení s příslušnými fyzickými porty přepínače, na které jsou stanice připojena. Přepínač zpracovává příchozí rámce podle cílové MAC adresy obsažené v hlavičce datového rámce a to porovnáním s údaji obsažené v CAM tabulce a následným přepnutím rámce na cílový port. Každé nově připojené zařízení k portu přepínače je dynamicky přidáno do tabulky.

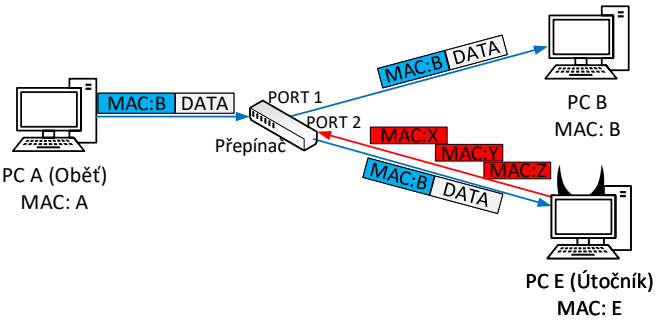
Útok cílený na zahlcení tabulky CAM (CAM overflow/ MAC flooding) je realizován následujícím způsobem. Útočník je připojen k přepínači a generuje velké množství falešných MAC adres. Tímto oznamuje přepínači nově připojená zařízení do sítě umístěná na jeho portu. Každé toto oznámení nese jinou MAC adresu a přepínač si ukládá vždy nový záznam do tabulky CAM. Jakmile dojde k „zahlcení“ přepínače záplavou nových záznamů a přepínač nedisponuje již volnou pamětí, musí odstraňovat nejstarší záznamy uložené v CAM tabulce a nahrazovat je novými. Ve stejnou chvíli přechází směrovač do stavu *fail safe mode*, známého také jako *hub mode*. Kvůli přehlcení CAM tabulky dochází k degradaci přepínače na úroveň rozbočovače, přepínač není nadále schopen využívat svoji CAM tabulku a kopíruje veškeré příchozí datové rámce na všechny své porty. Útočník je nyní schopen pasivně odposlouchávat probíhající komunikaci na všech portech přepínače a získává citlivé informace o všech koncových zařízeních nacházejících se uvnitř stejné sítě LAN. Zmíněný útok lze také označit za útok hrubou silou [13]. Průběh útoku je znázorněn na obrázku 4, kde PC A a PC B jsou komunikující strany a PC E představuje útočníka. První útočníkův krok, kdy zasílá falešná oznámení o nových zařízeních, je označen červenou šipkou. Následně dochází k degradaci směrovače na rozbočovač. Oběť (PC A) následně odesílá data příjemci (PC B), která přechází skrze všechny porty směrovače (označeno modrou šipkou). Odeslaná data obdrží nejen příjemce (PC B), ale i útočník (PC E).

Protiopatření může poskytovat rozšíření omezené kapacity CAM a zabránění jejího úplného využití. Toho lze dosáhnout nastavením zabezpečení portů, kdy je možné ke každému z portů připojit pouze omezené množství zařízení [4, 13]. Například přepínače od společnosti CISCO disponují vlastností nazvanou *Port Security*, pomocí které lze definovat maximální množství zařízení připojených k portům. Tato vlastnost umožňuje vybrat přepínačem realizovanou akci v případě, když dojde k porušení nastaveného pravidla na jednom z aktivních portů [14]. Na výběr jsou dvě základní reakce.

- **Restrict** - Po dovršení nastaveného limitu dochází k zahazování všech příchozích rámců s neznámou MAC adresou. Rámce nesoucí známou MAC adresu jsou povoleny. Incident je zaznamenán a dochází k vyvolání upozornění pro správce sítě.

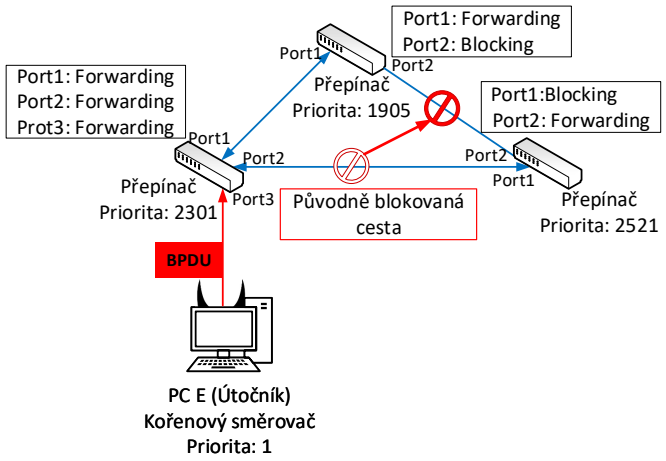
- **Shutdown** - Chování stejné jako u předchozí akce, avšak po porušení pravidla je port vypnut a veškerá komunikace je zakázána.

Zmíněného zvýšení kapacity CAM tabulky přepínače lze dosáhnout alokací paměti z fyzického serveru disponujícího velkými paměťovými možnostmi. Přepínač by takto mohl



Obrázek 4: Zaplavení přepínače během komunikace a výsledná degradace na rozbočovač, který kopíruje příchozí data na veškeré porty.

elektrorevue
ISSN 1213 - 1539



Obrázek 5: Podvržené BPDU od útočníka.

pracovat s CAM tabulkou umístěnou na serveru a v případě útoku by ohrožení oznámil správci sítě, který by mohl na jeho základě patřičně reagovat a provedení útoku zabránit. Ovšem definování zabezpečení portů je snazší, méně nákladné a nevyžaduje okamžitý zásah pověřené osoby.

2.5 Útok na Spanning Tree Protocol

STP (Spanning Tree Protocol) je síťový protokol zamezující tvorbě smyček v topologii sítě [15]. STP protokol neobsahuje opět žádné autentizační metody. Útočník tak může bez problémů odchytit všesměrově vysílaný BPDU (Bridge Protocol Data Unit) rámec a upravit jej za účelem získání nejvyšší priority, což povede k jeho zvolení jako **Root Bridge** a veškerá data budou předávána přes něj.

Nejvyšší prioritu uvnitř BPDU je hodnota 1 [16]. Odeslaný rámec je validní a přepínače útočníka přijmou jako nový **Root Bridge**. Útočník zvolený kořenovým přepínačem takto získá celou síť LAN, nebo konkrétní VLAN. Veškerá data prochází skrze **Root Bridge**, v tomto případě přes útočníka. Ten může rámce zachytávat a upravovat, tedy realizovat MitM. DoS (Denial of Service) přichází také v úvahu. V takovém případě by útočník blokoval veškeré rámce směřující k určité stanici nebo do konkrétní podsítě. Útočníkem vynucenou změnu **Root Bridge** znázorňuje obrázek 5. Zde je červenou šipkou znázorněno odeslání upraveného BPDU rámce. Přepínač dále předal BPDU a útočník byl ostatními přepínači zvolen jako **Root Bridge**. Výsledkem je změna blokované cesty, tedy přepnutí stavu portů u všech přepínačů.

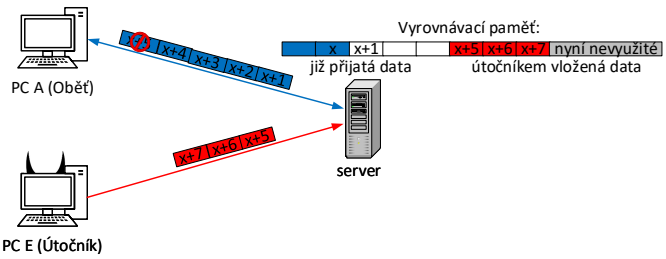
Protiopatřením v tomto případě by mohlo být vypnutí STP, což není doporučováno. Cisco přepínače obsahují připravená protiopatření proti STP útoku [12]. Jedním je BPDU Guard. Hraniční přepínače mají na portech, ke kterým jsou připojeni koncoví uživatelé, nastavený mód PortFast. Tento mód zabraňuje zařízením připojeným k tomuto portu jakýmkoliv způsobem ovlivnit STP topologii. Pokud na port v módu PortFast příjde BPDU, přepínač změní stav na *Disabled*. Následně dojde k vytvoření záznamu o příchozím BPDU, který nepronikne dále do sítě. Druhou možností je Root Guard, která pracuje stejným způsobem a monitoruje port, na kterém pracuje. Pokud příjme BPDU o změně STP topologie, vypne daný port a záznam zanese do logu.

2.6 Únos TCP spojení

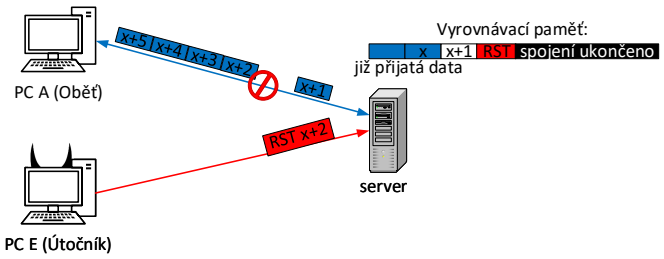
Protokol TCP (Transmission Control Protocol) představuje spojově orientovaný, spolehlivý protokol transportní vrstvy ISO/OSI. Před zahájením přenosu dat dochází k navázání spojení s příjemcem ve třech krocích, takzvaný *three-way handshake* [24]. Záměr únosu TCP spojení (TCP session hijacking) je zmocnit se již navázaného spojení Oběti se serverem využívající znalosti sekvenčního čísla.

Útočník realizující útok musí znát zdrojovou i cílovou IP adresu a zdrojový i cílový port. Nejdůležitější je znalost sekvenčního čísla, od které se útok odvíjí [25]. První kroky tedy vedou k získání těchto informací a útočník se musí nacházet ve stejné síti LAN jako oběť útoku. Pro získání přístupu k přenášeným datům může útočník využít pasivních monitorovacích zařízení nebo přistoupit k ARP spoofingu, viz kapitola 2.1. Dojde-li k odchycení TCP paketu, útočník nabyté informace využije ke zkonstruování vlastního TCP paketu tak, aby obsahoval stejné informace jako od Oběti. Pouze sekvenční číslo je vyšší než u odchyceného paketu. Správné nastavení sekvenčního čísla je důležité, aby nebyl podvržený TCP paket zahozený serverem. Podmínkou je, aby sekvenční číslo bylo vyšší, než je číslo aktuálně příchozího paketu. Zároveň nesmí přesahovat maximální hodnotu vyrovnávací paměti (buffer). Pokud by bylo sekvenční číslo podvrženého paketu nižší, než aktuálně očekávané číslo, dojde k jeho zahození. Překročí-li velikost vyrovnávací paměti, k zahození paketu dojde také. V ideálním případě, kdy je sekvenční číslo určeno správně, dojde k uložení podvrženého paketu do vyrovnávací paměti. K vyhodnocení útočníkova paketu nedochází ihned, ale server čeká na zatím nedoručená data. Jakmile se data doplní, server vykoná útočníkův požadavek a předpokládá, že se jedná o originální požadavek od klienta. Klientem odeslané pakety kolidují sekvenčním číslem s již přijatými pakety od útočníka. Spojení na straně klienta čeká na potvrzení odeslaných paketů a jejich odeslání opakuje z předpokladu, že paket nedorazil k serveru. Ovšem server pakety zahazuje, protože je považuje za již přijaté, a tak dojde k rozpojení klientova spojení. Takto získá útočník kontrolu nad spojením klienta a útok je úspěšně dokončen, viz obr. 6. Zde jsou modře zvýrazněné pakety, které odesílá oběť. Červeně zvýrazněné pakety nesou správně určené sekvenční číslo. Vyrovnávací paměť serveru zobrazuje již přijaté pakety od Oběti (modré) a pozici, kam se zařadí pakety od útočníka (červené). Před zpracování paketů od útočníka se čeká na jim předcházející. Následně dochází k zahození paketu Oběti s označením $x + 5$.

elektrorevue
ISSN 1213 - 1539



Obrázek 6: Představení TCP hijacking útoku a získání existujícího spojení.



Obrázek 7: Vynucené ukončení spojení se serverem zneužitím RST paketu.

Základní metoda protiopatření spočívá ve využití protokolu TLS (Transport Layer Security) viz přehled protiopatření v práci [26]. Protokol TLS představuje zabezpečený protokol pro síťovou komunikaci uživatele se vzdáleným webovým serverem a útočník tak není schopen odchytit sekvenční čísla spojení. Při použití nezabezpečeného TCP spojení je detekce tohoto útoku obtížná z důvodu shody podvrženého a originálního paketu [25]. Pro ostatní protokoly využívající TCP spojení je důležité využívat také zabezpečené varianty např. pro vzdálenou správu serveru využít protokol SSH (Secure Shell).

2.7 Otrava TCP spojení pomocí RST paketu

Předcházející útok pojednával o možnosti získání a ovládnutí existujícího TCP spojení. V některých situacích však útočníkovi stačí pouze ukončit TCP spojení a nepotřebuje ho ovládnout. K tomuto účelu může použít paket nesoucí příznak RST (reset). Pokud server příjme tento paket znamená to pro něho oznámení, že odesílatel přerušuje spojení a spojení je okamžitě ukončeno. Příznak RST byl vyvinut pro ukončení spojení v případě neočekávané chyby. Pokud útočník vytvoří paket s RST příznakem, který by mohl být odeslaný jednou z komunikujících stran, bude akceptován a proveden [25]. Útočník se v tomto útoku potýká se stejnými problémy jako v případě TCP hijacking 2.6. Musí odchytit paket probíhajícího spojení a získat zdrojovou i cílovou IP adresu spolu s odpovídajícími komunikačními porty a sekvenčním číslem. Záleží na nastavení zařízení. V některých případech zařízení přijímají RST paket vždy, i bez ohledu na již použité sekvenční číslo [27]. Podvržený TCP paket s příznakem RST server příjme. Pokud všechna útočníkem podvržená data souhlasí, paket je vyhodnocen a dojde k ukončení spojení. Zneužití RST paketu zobrazuje obrázek 7. Zde je červeně naznačený RST paket odesílaný útočníkem, který jej posílá během probíhající komunikace Oběti se serverem, označené modře. Pokud server obdrží RST paket, nebude čekat na přijetí paketu s označením $x + 1$ a spojení bude okamžitě ukončeno. V opačném případě dojde k ukončení spojení po paketu $x+1$ a následující pakety budou ztraceny z důvodu přerušeného spojení.

Protiopatření jsou v tomto případě útoku stejné s předchozím a to využití zabezpečení nad TCP protokolem. Problém je u zabezpečeného protokolu SSH. V předchozím případě tento protokol poskytoval protiopatření proti odcezení TCP spojení díky svému šifrovanému obsahu a útočník neznal tajný klíč a nemohl tedy data dešifrovat. V tomto případě však dešifrovat data není nutné, stačí pouze získat data z hlavičky a odeslat příznak RST. To je možné na základě umístění SSH protokolu uvnitř transportní vrstvy ISO/OSI modelu, díky čemu jsou pouze data uvnitř TCP paketu šifrována, nikoliv hlavička paketu [25]. Protokol SSH tedy není odolný proti tomuto útoku. Z tohoto důvodu např. směrovače firmy *Juniper* disponují nastavením, při kterém směrovač požaduje opětovné zaslání všech příznaků RST i SYN [28]. Obdrží-li během komunikace příznak RST, odesílateli (Oběť) odešle ACK příznak. Pokud Oběť opravdu zaslala paket RST, odešle jej znovu a nyní dojde k vynucenému ukončení spojení.

2.8 Útoky na směrovací protokoly

Síťová komunikace u středních a velkých sítích je řízena směrovači, které sdílí své informace o jim známých cestách uložených ve směrovací tabulce. K dosažení cílové stanice se využívají směrovací protokoly pro dynamickou výměnu informací. Směrování uvnitř sítě (Intradomain routing) spravují například protokoly RIP (Routing Information Protocol) [41] a OSPF (Open Shortest Path First) [43]. Nachází-li se cíl komunikace v odlehlé oblasti, pakety musí projít skrze odlišné sítě LAN (autonomní systémy – AS). Každá síť je reprezentována hraničním směrovačem, který takovéto pakety předává dalším hraničním směrovačům. Směrování mezi autonomními sítěmi (Interdomain routing) realizuje například protokol BGP (Border Gateway Protocol) [45].

RIPv2 má možnost autentizace pomocí až 16 znaků dlouhého hesla ve formátu otevřeného textu nebo pomocí hashovací funkce MD5. Autentizace pomocí hesla je vybrána jako výchozí možnost v případě, že protokol využívá autentizace směrovačů [41]. Takto realizovaná autentizace však není bezpečná, protože heslo je obsaženo uvnitř každého odeslaného RIP paketu. Protokol RIP využívá vektor vzdáleností (distance vector), jehož směrovací metrikou je počet skoků (hop count) [42]. Každý směrovač, kterým paket musí projít, představuje jeden skok a maximální počet skoků je 16 (0-15). Vyšší hodnota udává nedosažitelný cíl (unreachable). Protokol nehledí na jiné vlastnosti přenosových cest, což značí nevýhodu

elektrorevue
ISSN 1213 - 1539

v případě, kdy uvnitř sítě nemají veškerá spojení stejné vlastnosti. Zařízení užívající RIP protokol rozesílají každých 30 vteřin své směrovací informace, tedy vlastnosti a údaje o cestách v síti. Pro útok na tento protokol stačí odchycený a upravený informační paket. Útočník upravené informační pakety odesílá na směrovač ke kterému je přímo připojený. Směrovač uloží falešné informace do své směrovací tabulky a poté je rozesílá okolním směrovačům. Útok je poměrně snadný a výsledkem je útočník definovaná cesta. Může například všechna data směrovat skrze směrovač pod vlastní kontrolou a ovlivňovat průchozí data.

Další protokol **OSPF** (Open Shortest Path First) vybírá přenosovou cestu na základě šířky pásma (bandwidth), tedy přenosové rychlosti udávané v bitech za sekundu (bps) [42]. Čím větší šířka pásma, tím nižší cena cesty. Směrovače uvnitř sítě generují LSA (Link-State Advertisement) oznámení obsahující informace o topologii sítě. Každý směrovač si sám vytváří mapu sítě. Autentizační metody jsou stejné jako v případě protokolu RIPv2 (heslo přenášené v otevřené podobě nebo jeho otisk MD5) [43]. Ve výchozím nastavení OSPF nevyužívá autentizační mód. Naopak každý směrovač obsahuje mechanizmus označovaný jako *fight-back mechanism* [44]. Tento mechanizmus se „brání“ proti lživým zprávám. Obdrží-li směrovač LSA ve kterém jsou nepravdivé údaje, vyšle vlastní LSA, které opravuje tento falešný záznam. Nejedná se o zabezpečovací mechanizmus, avšak práci útočníka značně ztíží. Pro představení útoků byl zvolen útok podvržení přilehlého zařízení (**Adjacency Spoofing Attack**) [44]. Útočník využívá počítač připojený ke směrovači pracující s OSPF protokolem. Každý směrovač vysílá všesměrově *Hello* pakety a vysílání periodicky opakuje pro zjištění nových sousedních zařízení. Útočníkem odchycený *Hello* paket nese informace o směrovači na který je připojený. Následně je nutné, aby útočník se směrovačem navázal spojení. Poté přesvědčí směrovač o tom, že útočníkova stanice je nový směrovač uvnitř sítě. Proto vyšle *Hello, DB Description, LS Update, LS Acknowledge* pakety. Jakmile je směrovač přesvědčen, přidá útočníkovu stanici do své směrovací tabulky a dále na útočníka pohlíží jako na směrovač. Nyní může útočník vytvářet falešné LSA a odesílat falešné informace o změně topologie sítě. Směrovače si falešné LSA uloží do směrovací tabulky a útočník tak může realizovat útok mužem uprostřed, podvržení DNS serveru a jiné [44].

Další možností je určení vybraného směrovače jako nedosažitelného a způsobit tak DoS (útok je aplikovatelný obecně na všechny směrovací protokoly). Tento útok bývá označovaný jako otrava routování (**Route poisoning**). Podstatou je rozeslání falešné informace o již nedostupných směrovacích cestách uvnitř sítě. Standardizované protokoly mají způsob pro označení nedostupných cest. V případě OSPF se jedná o nastavení LS Age na maximální hodnotu 3600 vteřin. Obdrží-li směrovač LSA oznámení nesoucí údaj LS Age s maximální hodnotou, považuje tuto cestu za „otrávenou“ a odebere ji ze své směrovací tabulky.

BGP (Border Gateway Protocol) nastavuje cenu cesty ve 13 krocích a podrobné informace obsahuje CISCO dokumentace viz [45]. Důležitou poznámkou je, že BGP nehledí na jednotlivé směrovače, ale na autonomní sítě kterými komunikace bude směrována. BGP protokol byl vytvořen na základě důvěry v prostředí sítě Internet. Proto neobsahuje žádné metody autentizace komunikujících stran [46]. Jako útok byl vybrán únos BGP (**BGP hijacking**). Jedná se o útok, kdy útočník využívá směrovač komunikující pomocí BGP protokolu a vyšle oznámení, když je nová směrovací cesta k dispozici. Zná-li adresu sítě, kterou chce napadnout, přiřadí svému směrovači stejnou IP adresu. Následně vysílá falešné BGP informační pakety, že vlastní danou síť s levnější cestou. Další možný útok využívá skutečnosti, že komunikující směrovače pomocí BGP protokolu využívají TCP [47]. Útočník tedy může realizovat útoky typu zaplavení pakety SYN 3.3, únos SYN 2.6 a další.

Protiopatření přináší v tomto případě převážně snadná řešení. Zájem útočníka je dle popisu vždy cílen na odchycené pakety a jejich následnou úpravu. Nabízí se tedy využít algoritmus pro vyjednání klíčů, například Diffi-Hellman [47]. Komunikující strany se domluví na tajném klíči a mohou tak použít například kryptografický algoritmus AES (Advanced Encryption System) pro šifrování zpráv či jiný algoritmus využívající symetrickou kryptografii. Další možností pro BGP spojení je využití protokolu IPsec. Ten není součástí BGP protokolu, avšak lze pomocí něj ochránit navázané TCP spojení.

3 Útoky cílené na odepření služeb

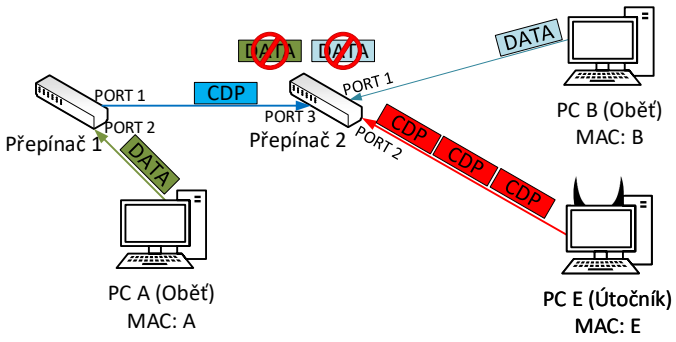
3.1 Zneužití Cisco Discovery protokolu

Přepínače společnosti CISCO využívají protokol CDP (Cisco Discovery Protocol) ke sdílení informací o ostatních, přímo připojených, zařízeních [17]. CDP rámce jsou odesílané periodicky, na multicast adresu a skrze každý port přepínače. Ihned po obdržení prvního CDP rámce si přepínač vytváří tabulku obsahující sousedící zařízení.

Ve výchozím nastavení přepínačů jsou veškerá data CDP protokolu přenášena v otevřené podobě. Útočníkovým cílem je upravení CDP zpráv a oznámit přepínači, že bylo připojeno do sítě nové zařízení. Útočník je následně považován za nový přepínač v síti. Přínosem pro útočníka jsou informace o přímo připojených zařízeních.

Hlavní cíl zneužití CDP představuje odepření služeb a zahlcení sousedních zařízení [19]. Útočník vygeneruje záplavu CDP rámců , kterými zahltí přepínač tak, že nedokáže zpracovávat žádné příchozí rámce. Uživatelé, jejichž komunikace prochází skrze napadený přepínač, neobdrží odpověď a veškeré služby jsou pro ně nedostupné [18]. Výsledek tohoto útoku nemusí nutně končit dosažením odepření služeb. Jak bylo popsáno v kapitole 2.4, zahlcený přepínač může být degradován na rozbočovač a následně rozesílá veškerou komunikaci všesměrově namísto zahození. Výsledek útoku využívající záplavu CDP rámců je závislý na verzi operačního systému přepínače [19]. Tento útočníkův přístup způsobí škody pouze na

elektrorevue
ISSN 1213 - 1539



Obrázek 8: DoS jako výsledek zaplavení CDP rámci.

jednom, přímo připojeném zařízení. Pokud by však získal přístup k přepínači, ke kterému jsou připojené další přepínače, rozsah škod bude násobný. Díky všesměrovému přeposílání CDP rámců by bylo možné zaplavit všechny okolní přepínače bez přidaného úsilí. Obrázek 8 znázorňuje útočníkem realizovaný DoS. Červeně jsou znázorněny útočníkem generované CDP rámce vedoucí k zahlcení přepínače 2. Přepínač 1 odesílá jeden korektní CDP rámec. Oběti (PC A i PC B) následně odesílají data přepínači 2, který je následně zahazuje.

Protiopatření proti zneužití CDP je zakázat používání CDP protokolu na přepínačích CISCO uvnitř sítě LAN [20]. Zakázání protokolu lze nastavit globálně pro všechna zařízení v síti, nebo na konkrétních portech přepínače. Koncové stanice, připojené na zabezpečený port, nemohou vysílat CDP rámce a ovlivnit tak přepínač. Pokud útočník získá fyzický přístup ke směrovači, může své zařízení přepojit na jiný port přepínače.

3.2 Záplava ICMP

Internet Control Message Protocol (ICMP) je protokol sloužící pro oznamování chybových stavů nebo dotazů síťové vrstvy ISO/OSI. Dotaz sestává z požadavku a odpovědi [21]. Útočník může protokol ICMP zneužít např. k zahlcení cílové stanice velkým množstvím PING dotazů. PING slouží jako nástroj pro ověření dostupnosti cílové stanice. Bez hlavičky IP protokolu dosahuje ve výchozím nastavení velikosti 32/64 bajtů. Cílem útoku je tedy vyslat množství ICMP paketů dostatečné k zahlcení Oběti a úspěšně realizovat DoS.

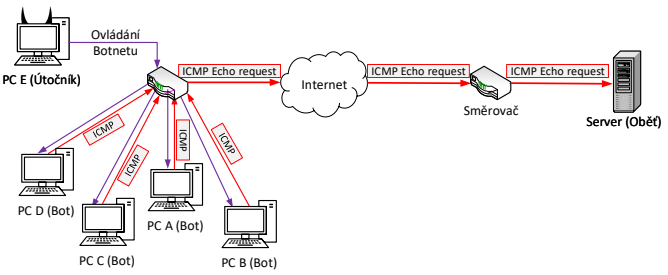
Velikost odeslaného ICMP paketu lze upravit. Útočník je schopný zvolit nejbližší maximálně možnou velikost paketu, což představuje 2^{16} bajtů. V tomto případě se však nejedná o záplavový útok, ale o tak zvaný PING of death, neboli PING smrti [22]. Zaplavit Oběť s využitím jednoho komunikačního uzlu, který útočník vlastní, je velmi obtížné. Přistoupí tedy k využití sítě Botnet, která představuje síť infikovaných zařízení. Takovouto síť má útočník pod kontrolou a využívá ji pro realizaci DDoS (Distributed Denial of Service) útoku. Realizace záplavy pakety ICMP (ICMP Flood) probíhá způsobem, kdy útočník z množství zařízení generuje ICMP pakety (například zmíněný PING). Velkým množstvím těchto paketů se snaží zahltit výpočetní prostředky kterými Oběť disponuje. Pokud je celková propustnost komunikační linky využita pro přijímání ICMP dotazů a generování ICMP odpovědí, legitimní provoz nemá dostatek prostředků pro správnou funkci. Jedná-li se o službu serveru, ta se stane nedostupnou všem uživatelům snažícím se o přístup. Nastává útočníkem žádané odepření služby. Využití sítě Botnet znázorňuje obrázek 9. Zde je fialovou šipkou znázorněno ovládání Botnetu útočníkem. Nemusí se jednat jen o jednu lokální síť, která je infikovaná. Útočník tak může nakládat s více zařízeními napříč mnoha sítím. Každý Bot v síti odesílá ICMP paket, znázorněno červeně. Oběť zahlcená takovýmto množstvím paketů není nadále schopná provozu.

Protiopatření proti útoku záplavou ICMP pakety přináší například nastavení signatury, která představuje frekvenční pravidlo, tedy definovaný počet povolených ICMP zpráv za časový okamžik [23]. Síťové prvky jsou včetně firewallů nastaveny na filtraci ICMP provozu včetně neodpovídání na dotaz PING z důvodu možného použití k zesílení DoS útoku.

3.3 Záplava SYN/TCP zaplavení

Základem útoku zaplavení pakety SYN (Syn flood), označovaný také jako zaplavení TCP (TCP flooding), je využití omezené velikosti fronty datových struktur TCB (Transmission Control Block). TCB představuje datovou strukturu dočasně uchovávající detaily navázaného spojení ze strany klienta [25]. Záznam jednostranně navázané komunikace (TCB) je uložen do fronty, do navázání spojení ze strany serveru a záznam o oboustranném spojení je poté přesunut do paměti. Pokud útočník zaplní povolený počet TCB, další pokusy o navázání spojení jsou ignorovány a dochází k DoS.

Útočník nejprve vyšle paket nesoucí příznak SYN. Server odpovídá pakety SYN a ACK. TCB záznam vkládá do fronty. Dále jen čeká na odpověď od útočníka, která však není úmyslně vytvořena. Uložený záznam o částečné komunikaci existuje pouze omezenou dobu, poté je z paměti vymazán, avšak tento časový úsek lze

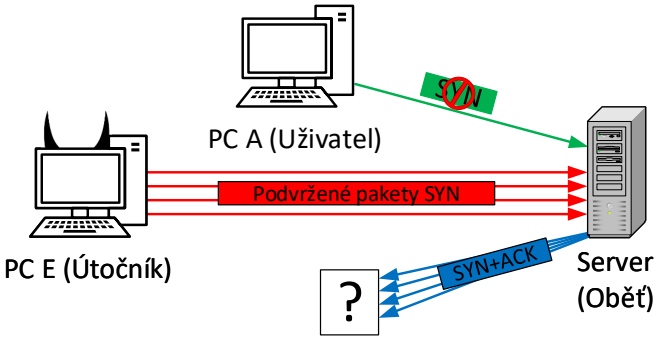


Obrázek 9: Realizace zaplavení serveru ICMP žádostmi s pomocí Botnetu.

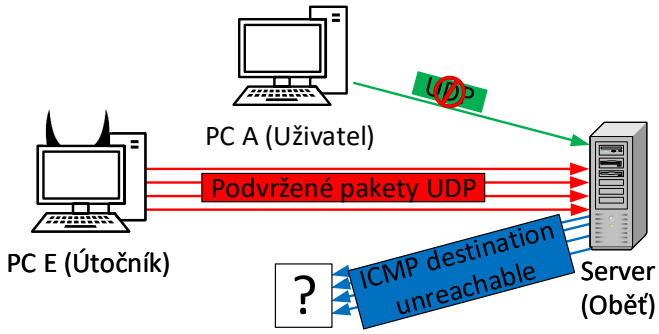
elektrorevue
ISSN 1213 - 1539

využít pro realizaci útoku. Vytvoří-li útočník dostatečné množství navázaných jednosměrných spojení, další pokusy o navázání nových spojení a vytvoření TCB jsou ignorovány. Klientem vyslané pakety SYN jsou zahozeny a server se jeví jako nedostupný. Podmínkou pro provedení útoku je vždy odlišná zdrojová adresa uvnitř SYN paketu. V opačném případě by mohlo dojít k zablokování komponentou Firewall na serveru. Adresy mohou být náhodně generované, což přináší situace jako neexistující adresa, adresa náležící vypnuté stanici nebo například adresa patřící aktivní stanici [29]. Jednat se také může o skupinu zařízení, kterou má útočník pod kontrolou a pro útok využije (Botnet). Pokud útočník vytvoří adresu korespondující s adresou existujícího zařízení, odpověď na serverem odeslané pakety SYN a ACK je paket RST. Útočníkem navázané jednosměrné spojení je existující stanicí odpojeno. Zahlcení serveru příznaky SYN a reakce Serveru jsou znázorněny na obrázku 3.3. Červeně znázorněné pakety nesoucí příznak SYN jsou Obětí (Server) vyhodnoceny a patřičná odpověď útočníkem vybraným „odesílatelům“ je znázorněna modře. Po zahlcení Oběti již uživatel (PC A) není schopen navázat spojení se Serverem, označeno zeleně.

Protiopatření přináší kontrola všech SYN paketů, nebo kontrola při každém nově příchozím paketu. Podvržené SYN pakety za normálních okolností nelze rozeznat od paketů generovaných skutečnými koncovými klienty serveru. Přesáhne-li v daném čase jejich počet stanovenou hranici, funkce vyhodnotí možnost probíhající záplavy pakety SYN. Zmíněná funkce je označována jako **SYN cookies** [25, 30]. Jedná se o techniku, kdy nejsou výpočetní prostředky serveru alokovány ihned při navázání jednocestného spojení. K alokaci dochází teprve pokud server obdrží potvrzovací paket od klienta. **SYN cookies** má ještě jeden důležitý mechanizmus proti podvrženém ACK paketům, které by mohl útočník také vytvářet. Server po obdržení SYN paketu vytvoří hash z příchozích informací SYN paketu a náhodného sekvenčního čísla. Tvorba hashe využívá tajný klíč serveru pro zajištění bezpečnosti. Výsledný hash slouží jako sekvenční číslo paketů SYN a ACK vyslaných serverem. V případě útoku je zdrojová adresa



Obrázek 10: Zaplavení serveru pakety s příznakem SYN.



Obrázek 11: Zaplavení Oběti UDP datagramy.

paketu SYN falešná a paket nikdy nedorazí do cíle. Pokud paket SYN vyslal skutečným klient, odpoví vlastním paketem ACK se zvýšenou hodnotou sekvenčního čísla. Server obdrží odpověď a pro ověření správnosti příchozích údajů opět vypočítá hash a porovná s příchozím. Shodují-li se, vše proběhlo v pořádku a spojení je sestaveno.

3.4 UDP zaplavení

UDP (User Datagram Protocol) je označován jako nespolehlivý protokol transportní vrstvy ISO/OSI. Nenese žádnou odpovědnost za datagramy a jejich pořadí. UDP datagramy jsou odesílány ihned a bez navázání spojení mezi klientem a serverem. Absence navazování spojení zde vytváří možnost pro útočníka realizovat zaplavení UDP (UDP flooding) [31]. Útok spočívá v generování velkého množství UDP paketů, které obsahují podvrženou zdrojovou adresu. Hlavním cílem jsou neaktivní komunikační porty serveru [32], na které útočník odesílá UDP datagramy. Server využívá své prostředky pro reakci na obdržené rámce a dochází tak k DoS.

Útočník odesílá velké množství UDP datagramů na náhodné komunikační porty serveru. Server musí reagovat na všechny přijaté požadavky. V případě požadavku příchozího na neaktivní port, generuje ICMP odpověď *destination unreachable*, cíl nedosažitelný [33]. Protože server reaguje na každý příchozí požadavek, jeho veškerý výpočetní výkon i šířka pásma budou věnovány výhradně UDP datagramům přijatým od útočníka. Dochází k zahlcení Oběti (Serveru) a pro uživatele snažícího se o komunikaci, bude Server nedostupný. Útočník může pro realizaci útoku využít Botnet. Realizaci a odpovědi Serveru znázorňuje obrázek 11. Útočníkem generované pakety (znázorněny červeně) vyvolávají reakci Oběti (znázorněno modře). ICMP pakety od Serveru nemají jistého příjemce. PC A (Uživatel), snažící se o komunikaci s Obětí (Server), je ignorován (znázorněno zeleně).

Protiopatření proti tomuto útoku je velmi složité z důvodu vytváření nelegitimních UDP datagramů nerozeznatelných od běžného provozu. Možností je omezit ICMP odpovědi, což ovšem ovlivní i běžný provoz. Avšak omezení provozu se prokazuje jako dostatečně účinné protiopatření

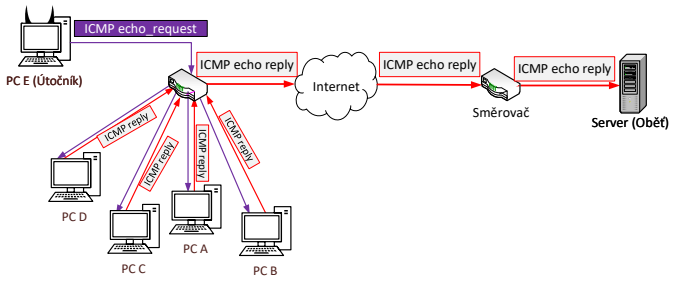
elektrorevue
ISSN 1213 - 1539

[34]. Nastaví-li se omezení příchozích paketů na bezpečnou úroveň pro daný server, předejdeme ohrožení samotného serveru. Cenou je ovlivnění legitimního provozu. Tato metoda je někdy také označována jako *throttling* [35]. Další možností je použití systémů IDS (Intrusion Detection System) nebo IPS (Intrusion Protection System). Systémy obsahují signatury útoku a v momentě jejich rozpoznání a zjištění schody ve vzorem systémy patřičně zareagují a omezí dopad útoku na oběť [36]. Jedním z možných systému IDS/IPS je open source nástroj Suricata [37].

3.5 Útok Smurf

Útoky typu DoS vychází z jednoho počítače s cílem vyčerpat cílovou stanici tak, že nebude schopna odpovídat na požadavky klientů a nadále poskytovat své služby. DDoS představuje rozlohou větší útok a k jeho realizaci spolupracuje více zařízení. Dobrovolně (více útočníků), proti své vůli (útočníkem podmaněné stanice), či nevědomě. **Smurf** je útokem typu DDoS a využívá stanice uvnitř sítě, které nevědomě plní útočníkův cíl a zahlcují oběť útoku.

Funkcionality ICMP, jmenovitě *ICMP echo request*, zneužívá **Smurf** [38]. Po obdržení *ICMP echo request* stanice odpovídá odesílateli pomocí *ICMP echo reply*. Útočník však nestojí o získání odpovědi na odeslaný dotaz, proto podvrhne zdrojovou adresu obsaženou uvnitř *ICMP echo request*. Stanice přijímající tento požadavek, odpoví zařízení jehož IP adresa je uvedena uvnitř pole se zdrojovou adresou [39]. Útočník využívá převážně všesměrového vysílání (Broadcast). Odešle-li útočník *ICMP echo request* na všesměrovou adresu dané sítě (x.x.x.255). Směrovač zpracovávající požadavek jej předá všem zařízením uvnitř sítě, kterých je *N*. Všech *N* zařízení vygeneruje *ICMP echo reply* a odešle na útočníkem podvrženou zdrojovou adresu Oběti. Tímto způsobem může útočník využít více nezávislých sítí a dosáhnout násobně vyššího počtu *ICMP echo reply*. Průběh útoku zobrazuje obrázek 12. Fialovou barvou je znázorněn *ICMP echo request* odesílaný na směrovač, který jej předá všem zařízením uvnitř sítě. Každé zařízení odpovídá *ICMP echo reply*, znázorněno červeně. Vygenerované množství odpovědí zahltí Oběť, která již není schopná zpracovávat jiné požadavky.



Obrázek 12: Realizace DDoS útoku Smurf.

Protiopatření útoku je komplikované z pohledu použitého ICMP protokolu, který je vhodný pro diagnostiku sítě, avšak s výše popsaným rizikem. Řešením může být komponenta firewall filtrující ICMP pakety dle konfigurace, kdy například veškeré ICMP pakety jsou zahazovány [38]. Pravděpodobně nejvyšší váhu má konfigurace sítě od poskytovatele internetových služeb (ISP), kdy sám poskytovatel může vytvořit taková protiopatření, která zabrání útočníkovy jej realizovat. Pokud by ISP (Internet Service Provider) kontroloval zdrojovou adresu uvedenou uvnitř hlavičky příchozích paketů, může zajistit zahození paketu nenáležícího do vlastní sítě. Předejde tak realizaci DDoS útoku **Smurf** [40].

4 Závěr

Tento článek přehledně analyzoval současný stav kybernetických útoků, které jsou realizovány na spojové, síťové a transportní verstě modelu OSI/ISO. Hlavním přínosem článku byla realizovaná podrobná analýza jejíž výsledkem byla tabulka (tabulka A), která představuje přehled známých kybernetických útoků s ohodnocenou složitostí jejich realizace, s hodnocením vážnosti dopadu jejich uskutečnění, způsobu možné detekce a mitigace. Hodnocení složitosti realizace a vážnost dopadu útoku bylo určeny subjektivně. Tabulka obsahuje také rozdělení na vrstvy a reference odkazující na popis útoku včetně způsobu protiopatření. Čtenář je tak schopen velice rychle pochopit základnímu principu útoku a jednoduše vyhledat způsob detekce a protiopatření.

Poděkování

Výzkum byl podpořen projektem MVČR s názvem „Systém distribuovaného dohledu nad síťovým provozem L2/L3 dle vyhlášky č. 317/2014 Sb. a zákona 181/2014 Sb.“ s reg.č. VI20192022149.

Literatura

[1] VERSCHUREN, Jan, René GOVAERTS and Joos VANDEWALLE. 1993. ISO-OSI security architecture. PRENEEL, Bart, René GOVAERTS and Joos VANDEWALLE (eds.). Computer Security and Industrial Cryptography [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, p. 179-192. Lecture Notes in Computer Science. Available at: http://link.springer.com/10.1007/3-540-57341-0_62

[2] XIA, Jing, Zhiping CAI, Gang HU and Ming XU. 2019. An Active Defense Solution for ARP Spoofing in OpenFlow Network. Chinese Journal of Electronics [online]. 28(1), 172-178. Available at: https://digital-library.theiet.org/content/journals/10.1049/cje.2017.12.002

[3] BHIRUD, S. G. and Vijay KATKAR. 2011. Light weight approach for IP-ARP spoofing detection and prevention. In: 2011 Second Asian Himalayas International Conference on Internet (AH-ICI) [online]. IEEE, p. 1-5. Available at: http://ieeexplore.ieee.org/document/6113951/

elektrorevue
ISSN 1213 - 1539

[4] BHAIJI, Yusuf. 2009. Understanding, Preventing, and Defending Against Layer 2 Attacks [online]. Available at: https://www.cisco.com/c/dam/global/en_ae/assets/exposaudi2009/assets/docs/layer2-attacks-and-mitigation-t.pdf

[5] BRUSCHI, D., A. ORNAGHI and E. ROSTI. 2003. S-ARP: a secure address resolution protocol. In: 19th Annual Computer Security Applications Conference, 2003. Proceedings [online]. IEEE, p. 66-74. Available at: http://ieeexplore.ieee.org/document/1254311/

[6] HOFFMAN, Chris. 2017. Why You Shouldn't Use MAC Address Filtering On Your Wi-Fi Router. How-To Geek [online]. Available at: https://www.howtogeek.com/204458/why-you-shouldn%E2%80%99t-use-mac-address-filtering-on-your-wi-fi-router/

[7] BUHR, Andrew, Dale LINDSKOG, Pavol ZAVARSKY and Ron RUHL. 2011. Media Access Control Address Spoofing Attacks against Port Security. In: Proceedings of the 5th USENIX Conference on Offensive Technologies [online]. WOOT'11. San Francisco, CA: USENIX Association. Available at: http://dl.acm.org/citation.cfm?id=2028052.2028053

[8] HUANG, I-Hsuan, Ko-Chen CHANG, Yu-Chi LU and Cheng-Zen YANG. 2010. Countermeasures against MAC address spoofing in public wireless networks using lightweight agents. In: The 5th Annual ICST Wireless Internet Conference (WICON) [online]. Available at: https://ieeexplore.ieee.org/document/5452667

[9] FAN, Huipu, Yizhou DONG, Ming YU and Leonard TUNG. 2013. Security Threats against the Communication Networks for Traffic Control Systems. In: 2013 IEEE International Conference on Systems, Man, and Cybernetics [online]. IEEE, p. 4783-4788. Available at: http://ieeexplore.ieee.org/document/6722569/

[10] ALABADY, Salah A. Jaro. 2008. Design and Implementation of a Network Security Model using Static VLAN and AAA Server. In: 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications [online]. IEEE, p. 1-6. Available at: http://ieeexplore.ieee.org/document/4530276/

[11] LOMNICKÝ, Marek. Analýza a demonstrace vybraných L2 útoků [online]. Brno, 2009 [cit. 2019-10-02]. Dostupné z: http://hdl.handle.net/11012/53857. Diplomová práce. Vysoké učení technické v Brně. Fakulta informačních technologií. Ústav informačních systémů. Vedoucí práce Ondřej Ryšavý.

[12] BULL, Ronny L. ACritical ANALYSIS OF LAYER 2 NETWORK SECURITY IN VIRTUALIZED ENVIRONMENTS. 2016. PhD Thesis. CLARKSON UNIVERSITY. Available at: https://people.clarkson.edu/ bullrl/bullrl_dissertation.pdf

[13] XU, Tong, Deyun GAO, Ping DONG, Chuan Heng FOH and Hongke ZHANG. 2017. Mitigating the Table-Overflow Attack in Software-Defined Networking. IEEE Transactions on Network and Service Management [online]. 14(4), 1086-1097. Available at: http://ieeexplore.ieee.org/document/8057280/

[14] Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)EW: Configuring Port Security. Cisco - Global Home Page [online]. Available at: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.html

[15] Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches. 2006. Cisco Systems [online]. Available at: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html

[16] TREJO, Luis A., Rául MONROY and Rafael LÓPEZ MONSALVO. 2006. Spanning Tree Protocol and Ethernet PAUSE Frames DDoS Attacks: Their Efficient Mitigation [online]. , 1-13. Available at: https://www.semanticscholar.org/paper/Spanning-Tree-Protocol-and-Ethernet-PAUSE-Frames-%3A-Trejo-Monroy/008339f322de9564d8a74f96f7aee670f6ec0cd9

[17] Cisco Discovery Protocol Configuration Guide, Cisco IOS Release 15M&T. Cisco Systems [online]. Available at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html

[18] TANCESKA, Biljana, Mitko BOGDANOSKI and Aleksandar RISTESKI. Simulation Analysis of DoS, MITM and CDP Security Attacks and Countermeasures. Future Access Enablers for Ubiquitous and Intelligent Infrastructures [online]. p. 197-203. Available at: http://link.springer.com/10.1007/978-3-319-27072-2_25

[19] Cisco CDP Advisory. Phenoelit [online]. Available at: http://www.phenoelit.org/fr/misc.html

[20] CDP (Cisco Discovery Protocol). Flylib [online]. Available at: https://flylib.com/books/en/3.418.1.78/1/

[21] UDHAYAN, J. and R. ANITHA. 2009. Demystifying and Rate Limiting ICMP hosted DoS/DDoS Flooding Attacks with Attack Productivity Analysis. In: 2009 IEEE International Advance Computing Conference [online]. IEEE, p. 558-564. Available at: http://ieeexplore.ieee.org/document/4809072/

[22] YIHUNIE, Fekadu, Eman ABDELFATTAH and Ammar ODEH. 2018. Analysis of ping of death DoS and

elektrorevue
ISSN 1213 - 1539

DDoS attacks. In: 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT) [online]. IEEE, p. 1-4. Available at: https://ieeexplore.ieee.org/document/8378010/

[23] CHANG, R.K.C. 2002. Defending against flooding-based distributed denial-of-service attacks: a tutorial. IEEE Communications Magazine [online]. 40(10), 42-51. Available at: http://ieeexplore.ieee.org/document/1039856/

[24] HARRIS, B. and R. HUNT. 1999. TCP/IP security threats and attack methods. Computer Communications [online]. 22(10), 885-897. Available at: https://linkinghub.elsevier.com/retrieve/pii/S014036649900064X

[25] DU, Wenliang. 2019. Attacks on the TCP Protocol. DU, Wenliang. Computer Security: A Hands-on Approach [online]. 2nd ed. p. 46-62. Available at: http://www.cis.syr.edu/ wedu/seed/Book/book_sample_tcp.pdf

[26] VINEETA, Jain, Sahu DIVYA and Tomar DEEPAK. 2015. Session Hijacking: Threat Analysis and Countermeasures [online]. Available at: https://www.researchgate.net/publication/277307339_Session_Hijacking_Threat_Analysis_and_Countermeasures

[27] WEAVER, Nicholas, Robin SOMMER and Vern PAXSON. 2009. Detecting Forged TCP Reset Packets. Proceedings of the Network and Distributed System Security Symposium [online]. San Diego, California, USA, 2009. Available at: https://www.ndss-symposium.org/ndss2009/detecting-forged-tcp-reset-packets/

[28] Protecting Against TCP RST or SYN DoS Attacks. 2014. Juniper networks: TechLibrary [online]. Available at: https://www.juniper.net/documentation/en_US/junose15.1/topics/task/configuration/tcp-rst-syn-dos-attack-protection.html

[29] SCHUBA, C.L., I.V. KRSUL, M.G. KUHN, E.H. SPAFFORD, A. SUNDARAM and D. ZAMBONI. 1997. Analysis of a denial of service attack on TCP. In: Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097) [online]. IEEE Comput. Soc. Press, p. 208-223. Available at: http://ieeexplore.ieee.org/document/601338/

[30] BOGDANOSKI, Mitko, Tomislav SHUMINOSKI and Aleksandar RISTESKI. 2013. Analysis of the SYN Flood DoS Attack. International Journal of Computer Network and Information Security [online]. 5(8), 15-11. Available at: http://www.mecs-press.org/ijcnis/ijcnis-v5-n8/v5n8-1.html

[31] PARTRIDGE, C. and S. PINK. A faster UDP (user datagram protocol). IEEE/ACM Transactions on Networking [online]. 1(4), 429-440. Available at: http://ieeexplore.ieee.org/document/251895/

[32] KOLAHI, Samad S., Kiattikul TRESEANGRAT and Bahman SARRAFPOUR. 2015. Analysis of UDP DDoS flood cyber attack and defense mechanisms on Web Server with Linux Ubuntu 13. In: 2015 International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15) [online]. IEEE, p. 1-5. Available at: http://ieeexplore.ieee.org/document/7081286/

[33] GRABOVSKÝ, Štěpán, Vlastimil ČLUPEK, Milan ŠVEHLÁK and Jan KLIMEŠ. 2018. Síťový generátor DoS útoků. Elektrorevue [online]. 20(3), 68-76. Available at: http://www.elektrorevue.cz/cz/clanky/kybernetika–automatizace–merici-technika/0/sitovy-generator-dos-utoku/

[34] GARG, A. and A.L. NARASIMHA REDDY. 2002. Mitigation of DoS attacks through QoS regulation. In: IEEE 2002 Tenth IEEE International Workshop on Quality of Service (Cat. No.02EX564) [online]. IEEE, p. 45-53. Available at: http://ieeexplore.ieee.org/document/1006573/

[35] SPECHT, Stephen M. and Ruby B. LEE. 2004. Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures. Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems: International Workshop on Security in Parallel and Distributed Systems [online]. 17, 543-550. Available at: www.princeton.edu/ rblee/ELE572Papers/Fall04Readings/DDoSSurveyPaper_20030516_ Final.pdf

[36] MOHAMMED, Lawan A. and Biju ISSAC. 2007. Detailed DoS attacks in wireless networks and countermeasures. International Journal of Ad Hoc and Ubiquitous Computing [online]. 2(3). Available at: http://www.inderscience.com/link.php?id=12417

[37] Suricata. Suricata: Open Source IDS / IPS / NSM engine [online]. Available at: https://suricata-ids.org/

[38] KUMAR, Sanjeev. 2007. Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet. In: Second International Conference on Internet Monitoring and Protection (ICIMP 2007) [online]. IEEE, p. 25-25. Available at: http://ieeexplore.ieee.org/document/4271771/

[39] ZARGAR, Gholam Reza and Peyman KABIRI. 2009. Identification of effective network features to detect Smurf attacks. In: 2009 IEEE Student Conference on Research and Development (SCOReD) [online]. IEEE, p. 49-52. Available at: http://ieeexplore.ieee.org/document/5443345/

elektrorevue
ISSN 1213 - 1539

[40] NAZARIO, Jose. 2008. DDoS attack evolution. Network Security [online]. 2008(7), 7-10. Available at: linkinghub.elsevier.com/retrieve/pii/S1353485808700862

[41] Sample Configuration for Authentication in RIPv2. 2005. Cisco - Global Home Page [online]. Available at: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13719-50.html

[42] DEY, Golap Kanti, Md. Mobasher AHMED and Kazi Tanvir AHMMED. 2015. Performance analysis and redistribution among RIPv2, EIGRP & OSPF Routing Protocol. In: 2015 International Conference on Computer and Information Engineering (ICCIE) [online]. IEEE, p. 21-24. Available at:http://ieeexplore.ieee.org/document/7399308/

[43] Sample Configuration for Authentication in OSPF. 2005. Cisco - Global Home Page [online]. Available at: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13719-50.html

[44] SONG, Yubo, Shang GAO, Aiqun HU and Bin XIAO. 2017. Novel attacks in OSPF networks to poison routing table. In: 2017 IEEE International Conference on Communications (ICC) [online]. IEEE, p. 1-6. Available at: http://ieeexplore.ieee.org/document/7996829/

[45] SBGP Best Path Selection Algorithm. 2016. Cisco - Global Home Page [online]. Available at: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html

[46] RASHEVSKIY, Roman B. and Andrey S. SHABUROV. 2017. ≪BGP-hijacking≫ attacks: Theoretical basis and practical scenarios. In: 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) [online]. IEEE, p. 208-212. Available at: http://ieeexplore.ieee.org/document/7910530/

[47] BUTLER, K., T.R. FARLEY, P. MCDANIEL and J. REXFORD. 2010. A Survey of BGP Security Issues and Solutions. Proceedings of the IEEE [online]. 98(1), 100-122. Available at: http://ieeexplore.ieee.org/document/5357585/

[48] DUA, Gagan, Nitin GAUTAM, Dharmendar SHARMA and Ankit ARORA. 2013. Replay Attack Prevention in Kerberos Authentication Protocol using Triple Password. International journal of Computer Networks & Communications [online]. 5(2), 59-70. Available at: http://www.airccse.org/journal/cnc/5213cnc05.pdf

[49] PATNI, Parth, Kartik IYER, Rohan SARODE, Amit MALI and Anant NIMKAR. 2017. Man-in-the-middle attack in HTTP/2. In: 2017 International Conference on Intelligent Computing and Control (I2C2) [online]. IEEE, p. 1-6. Available at: http://ieeexplore.ieee.org/document/8321787/

[50] CONTI, Mauro, Nicola DRAGONI and Viktor LESYK. 2016. A Survey of Man In The Middle Attacks. IEEE Communications Surveys & Tutorials [online]. 18(3), 2027-2051. Available at: http://ieeexplore.ieee.org/document/7442758/

elektrorevue
ISSN 1213 - 1539

A Příloha - Přehled kybernetických útoků na L2/L3 vrstvě.

Název	Složitost útoku	Dopady útoku	Možnosti detekce	Příklad protiopatření/Mitigace
(L2) ARP spoofing [2, 3]	střední	těžký (MitM)	signatury	DHCP snooping [4] / S-ARP [5]
(L2) MAC Address spoofing [6, 7]	lehká	těžký	signatury	DHCP snooping [4] / autentizační agenti a server [8]
(L2) VLAN hopping [11, 10, 9]	střední	střední	signatury	odlišná nativní VLAN [11, 12]
(L2) CAM overflow [13]	lehká	lehký	signatury	Port Security [14, 13]
(L2) eavesdropping	lehká	lehký	anomálie	MACSec, VPN, šifrování
(L2) data/header manipulation	střední	těžký	anomálie	autentizační funkce (MAC)
(L2) STP Attack [16]	střední	lehký	signatury	BPDU guard [12]
(L2) CDP misusing [18, 19]	lehká	střední	signatury	Zakázaní CDP [20]
(L2) Unauthorized Authentication	střední	těžký	anomálie	SSH, autentizace, fyzický přístup
(L3) ICMP flooding [21]	lehká	střední	signatury	IDS/Honeypot [23]
(L3) eavesdroping	střední	střední	anomálie	IPsec, VPN, šifrování
(L3) data/header manipulation	střední	těžký	anomálie	IPsec/AH protokol, autentizace
(L3) Sybil Attack	střední	střední	anomálie	Ověření nových uzlů
(L3) Battery depletion	střední	lehký	anomálie	IDS
(L3) Route poisoning	střední	střední	signatury	šifrovaná komunikace, autentizace
(L3) General MitM Attack [49]	těžká	těžký	signatury	autentizace [50]
(L1) Signal Jamming	střední	lehký	anomálie	proměnný výkon signálu
(L2, L3) Routing Attacks [44, 46]	střední	střední	signatury	šifrovaná komunikace, autentizace [47]
(L4) TCP Session Hijacking [25]	těžká	těžký	signatury	šifrovaná komunikace [26]
(L4) RST Session Poisoning [25]	střední	střední	signatury	šifrovaná komunikace [25]
(L4) SYN flood [25]	lehká	střední	signatury	SYN cookies [30]
(L4) UDP flooding [32]	lehká	střední	signatury	IDS/IPS [36] /throttling [35]
(L4) Smurf Attack [38, 39]	lehká	střední	signatury	Firewall [38] / blokace na úrovni poskytovatele služeb [40]
(L4) Unauthorized Port Scanning	lehká	střední	anomálie	deaktivace nevyužívaných portů
(L7) Try-and-guess Attacks	střední	těžký	anomálie	pravidelná změna silného hesla
(L7) Replay Attacks [48]	střední	těžký	signatury	proměnná výzva, čas. razítko