Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.9
DOI: https://doi.org/10.24867/19BE02Salic

TUNELIRANJE PROTOKOLIMA KOJIMA TO NIJE OSNOVNA NAMENA

TUNNELING WITH PROTOCOLS FOR WHICH THIS IS NOT THE PRIMARY PURPOSE

Dimitrije Salić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *Rad obuhvata opis principa procesa tuneliranja i osnovne tipove metoda tuneliranja. Pored toga, sadrži prikaz protokola tuneliranja koji se najčešće koriste u ovu svrhu, sa opisom njihovog načina funkcionisanja, a isto tako i prikaz protokola koji se takođe mogu koristiti u ovu svrhu, iako im to nije osnovna namena. Upravo s tim u vezi, opisani su mogući maliciozni napadi korišćenjem istih, ali i alati pomoću kojih je moguća njihova detekcija i prevencija. Na kraju, detaljno je analiziran primer implementacije tuneliranja korišćenjem upravo jednog od protokola kojem to nije osnovna namena – ICMP protokolom. Prilikom implementacije, korišćen je alat Icmpsh, a spomenuti su i alternativni alati. Odabran je iz razloga što ne zahteva administrativne privilegije da bi se pokrenuo na „žrtvinoj“ mašini i lako je prenosiv.*

Ključne reči: *Reverzni proksi, Server, Konfiguracija*

Abstract – *This paper includes a description of the principles of the tunneling process and the basic types of tunneling methods. In addition, it contains an overview of the tunneling protocols most commonly used for this purpose, with a description of how they work, as well as an overview of the protocols that can also be used for this purpose, although this is not their primary purpose. In this regard, possible malicious attacks using them are described, as well as tools that can be used to detect and prevent them. Finally, an example of tunneling implementation is presented in detail using one of the protocols for which tuneling is not the main purpose - ICMP protocol. During the implementation, the Icmpsh tool was used, and alternative tools were mentioned. This tool was chosen because it does not require administrative privileges to be run on the "victim's" machine and is very portable.*

Keywords: *Tunneling, Protocols, Attacks*

1. UVOD

Komunikacija putem Interneta, bilo koristeći računare ili pametne telefone, postala je deo svakodnevice ljudima širom sveta. Zahvaljujući Internetu moguće je komunicirati sa bilo kim, u bilo koje vreme, gde god se osoba nalazila.

Opšte su poznate pogodnosti i nove mogućnosti koje je online komunikacija donela ljudima, a bez kojih bi u današnje vreme, čini se, bilo nemoguće živeti.

Informacije koje se prenose putem Interneta, odnosno bilo koja dva digitalna uređaja, prenose se pomoću protokola.

Tema ovog rada su protokoli tuneliranja i primer njihove implementacije. U drugom poglavlju biće opisan uvod u proces tuneliranja i osnovni pojmovi, a takođe biće i istaknuta veza između tuneliranja i VPN-a (Virtual Private Network). U trećem poglavlju opisani su protokoli tuneliranja, kako oni koji se često koriste, tako i oni kojima to nije osnovna namena. Tokom razrade protokola kojima tuneliranje nije osnovna namena, biće takođe navedeni i načini za njihovu detekciju i prevenciju od napada. Četvrto poglavlje sadržaće prikaz primera implementacije tuneliranja korišćenjem protokola kojem to nije osnovna namena, dok će peto poglavlje predstavljati zaključak rada.

2. UVOD U PROCES TUNELIRANJA

U fizičkom svetu tuneliranje predstavlja probijanje barijera i prolazak preko terena koji se inače ne može preći. Slično, u računarskom svetu, tuneliranje predstavlja transport podataka kroz mrežu koristeći protokole koje ta mreža ne podržava [1].

Protokol tuneliranja je komunikacioni protokol koji omogućava transport podataka iz jedne mreže u drugu. To uključuje omogućavanje slanja komunikacija privatne mreže putem javne mreže (kao što je Internet) kroz proces koji se naziva enkapsulacija [10].

Podaci koji putuju mrežom podeljeni su na pakete. Paketi se sastoje iz dva dela:

1. Header (zaglavlje) - ukazuje na odredište paketa

i koji protokol koristi

2. Payload (sadržaj) - predstavlja stvarni sadržaj paketa.

Enkapsulirani paket je u suštini paket unutar drugog paketa. U enkapsuliranom paketu, zaglavlje i sadržaj prvog paketa idu unutar odeljka sadržaja okolnog paketa, pa tako originalni paket sam po sebi postaje sadržaj [1].

Enkapsulacija je korisna za šifrovane mrežne veze. Enkripcija je proces šifrovanja podataka na takav način da se oni mogu dešifrovati samo pomoću tajnog ključa za šifrovanje. Proces dekriptovanja naziva se dešifrovanje. Ako je paket potpuno šifrovan, uključujući i zaglavlje, mrežni ruteri neće moći da proslede paket do njegovog odredišta jer nemaju ključ i ne mogu da vide njegovo zaglavlje. Umotavanjem šifrovanog paketa u drugi nešif-

---

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Željko Vuković, docent.

rovani paket, paket može da putuje kroz mreže kao i obično [1].

2.1. VPN (Virtual Private Network)

VPN (Virtal Private Network) obezbeđuje medijum za razmenu podataka preko Interneta ili bilo koje druge javne mreže koristeći tuneliranje [11].
Za stvaranje tunela potrebno je sledeće [11]:

- *Protokol operatera* - odnosi se na mrežni transportni protokol koji podržava tranzitna mreža. Na primer, PPP (Point to Point Protocol) se koristi kao protokol nosioca u tranzitnim mrežama zasnovanim na IP-u.
- *Protokol enkapsulacije* - odnosi se na protokol koji se koristi za enkapsulaciju sadržaja paketa podataka. GRE (Generic Routing Encapsulation), PPTP (Point to Point Tunneling Protocol), L2F (Layer 2 Forwarding Protocol) i L2TP (Layer Two Tunneling Protocol) su primeri protokola za enkapsulaciju.
- *Protokol putnika* - odnosi se na protokol koji koriste mreže koje su povezane tunelom. Koristi ga paket podataka, koji je enkapsuliran pomoću protokola za enkapsulaciju. IP (Internet Protocol) i IPX (Internet network Packet Exchange) su primeri putničkih protokola.

2.2. Tipovi metoda tuneliranja

Tip VPN-a koji koristi preduzeće određuje metod tuneliranja koji se koristi u VPN-u. VPN veza može biti ili Site-to-Site VPN veza, uspostavljena između dve mreže, ili Remote Access VPN veza, između udaljenog klijenta i VPN servera na korporativnom intranetu.
Postoje dve vrste metoda tuneliranja koje odgovaraju ovim VPN vezama, i to su sledeće:

1. ***End-to-End tunneling*** (slika 1) - povezuje lični računar udaljenog korisnika i VPN server, koji deluje kao gateway između Interneta i korporativne LAN mreže preduzeća. Koristi se u Remote Access VPN vezi. Procedure tuneliranja, kao što su enkapsulacija i dekapsulacija podataka, sprovode se na krajnjim tačkama tunela. Softver VPN klijenta enkapsulira pakete podataka pre nego što ih pošalje preko tunela do VPN servera. VPN server dekapsulira podatke pre nego što ih prosledi na korporativni LAN [11].

2. ***Node-to-Node tunneling*** (slika 2) - povezuje gateway uređaje koji se nalaze na ivici dve privatne mreže. Koristi se u Site-to-Site VPN vezi. Gateway uređaj može biti ruter, firewall ili neki sličan uređaj koji deluje kao VPN server. U ovom podešavanju, VPN klijent je udaljeni korisnik koji se nalazi na LAN-u preduzeća. Tunel se proteže od jednog mrežnog prolaza do drugog i ne proteže se do računara udaljenog korisnika. Gateway uređaj na ivici LAN-a enkapsulira podatke primljene sa računara unutar LAN-a i vrši enkapsulaciju pre nego što ih pošalje preko tunela. Gateway uređaj na drugom kraju tunela dekapsulira podatke pre nego što ih prosledi na LAN [11].

3. PROTOKOLI TUNELIRANJA

Neki od protokola koji se najčešće koriste za tuneliranje su sledeći:

- IP in IP
- GRE
- OpenVPN
- SSTP
- IPSec
- L2TP

IP in IP je protokol za IP tuneliranje koji enkapsulira jedan IP paket u drugi IP paket. Da bi se enkapsulirao IP paket u drugi IP paket, dodaje se spoljno zaglavlje sa izvornim IP-ijem, ulaznom tačkom tunela, i odredišnim IP-ijem, izlaznom tačkom tunela. Unutrašnji paket je neizmenjen (osim TTL polja, koje se smanjuje). Polja „Ne fragmentiraj“ i „Tip usluge“ treba da se kopiraju u spoljašnji paket. Ako je veličina paketa, uključujući spoljno zaglavlje, veća od MTU putanje, enkapsulator fragmentira paket. Dekapsulator će ponovo sastaviti paket [12].

Generička enkapsulacija rutiranja (GRE) je protokol za tuneliranje koji može da enkapsulira širok spektar protokola mrežnog sloja unutar virtuelnih veza od tačke do tačke ili veza od tačke do više tačaka preko mreže Internet protokola [13].

OpenVPN je sistem virtuelne privatne mreže (VPN) koji primenjuje tehnike za kreiranje bezbednih veza od tačke do tačke ili od lokacije do lokacije u rutiranim konfiguracijama i objektima za daljinski pristup. Implementira i klijentske i serverske aplikacije [14].

Secure Socket Tunneling Protocol (SSTP) je oblik tunela virtuelne privatne mreže (VPN) koji obezbeđuje mehanizam za transport PPP saobraćaja kroz SSL/TLS kanal. SSL/TLS obezbeđuje bezbednost na nivou transporta uz pregovaranje ključa, šifrovanje i proveru integriteta saobraćaja. Upotreba SSL/TLS-a preko TCP porta 443 (podrazumevano, port se može promeniti) omogućava SSTP-u da prođe kroz skoro sve firewall-ove i proksi servere osim preko proverenih veb proksija [15].

Internet Protocol Security (IPSec) je bezbedni paket mrežnih protokola koji potvrđuje autentičnost i šifruje pakete podataka kako bi obezbedio bezbednu šifrovanu komunikaciju između dva računara preko mreže Internet protokola. Koristi se u virtuelnim privatnim mrežama (VPN) [16].

Layer 2 Tunneling Protocol (L2TP) je proširenje Point-to-Point protokola (PPTP) koji koriste provajderi internet usluga (ISP) da bi omogućili virtuelne privatne mreže (VPN). Da bi se osigurala bezbednost, L2TP mora da se oslanja na protokol za šifrovanje da bi prošao unutar tunela [17].

3.1 Protokoli kojima tuneliranje nije osnovna namena

Kao što je već pomenuto, postoje protokoli koji se mogu koristiti za tuneliranje, iako im to nije osnovna namena. Neki od najpoznatijih su navedeni u nastavku:

1. *ICMP* (Internet Control Message Protocol)
2. *DNS* (Domain Name System)

3.1.1. IMCP tuneliranje

ICMP tuneliranje je tehnika napada komandi i kontrole (C2) koja tajno propušta maliciozni saobraćaj kroz odbranu perimetra. Maliciozni podaci koji prolaze kroz tunel skriveni su unutar ICMP echo zahteva i odgovora koji izgledaju normalno [2].

U ICMP datagram se mogu umetnuti različiti tipovi malicioznih podataka, od malih količina koda do velikog enkapsuliranog HTTP, TCP ili SSH paketa. Datagram je sličan paketu, ali datagrami ne zahtevaju uspostavljenu vezu ili potvrdu da je prenos primljen (za razliku od protokola zasnovanih na povezivanju kao što je TCP). ICMP datagrami uključuju odeljak podataka koji može da nosi sadržaj bilo koje veličine [2].

Ipak, svakako da postoje nedostaci kada je u pitanju ova tehnika. Neki operativni sistemi zahtevaju privilegije root ili lokalnog administratora za kreiranje prilagođenih ICMP datagrama, a napadaču može biti teško da stekne te privilegije. Pored toga, ICMP tuneliranje kroz firewall ili rutere za prevođenje mrežnih adresa (NAT) takođe predstavlja izazov, jer ovi uređaji filtriraju ICMP echo odgovore koji nemaju odgovarajući zahtev. U ovim slučajevima, ICMP tuneliranje možda neće biti tako pouzdano kao druge metode tuneliranja protokola [2].

Kada je u pitanju detekcija ICMP tunelskog saobraćaja, ovaj saobraćaj može biti teško otkriti. Softver može legitimno da verifikuje validne mrežne veze pomoću eho poruka koje imaju neuobičajeno opterećenje. Da bi se proverilo da li je sadržaj maliciozan, nešifrovani sadržaji u ICMP porukama mogu se pažljivije ispitati pomoću alata kao što je Wireshark. Treba imati na umu da napadač i dalje može da šifruje podatke kako bi izbegao otkrivanje [2].

Extrahop reveal(x) automatski detektuje ponašanje ICMP tunela tako što identifikuje neobičan broj ICMP echo zahteva koje uređaj šalje tokom vremena, pri čemu svaki zahtev sadrži jedinstveno opterećenje. Normalni ICMP echo zahtevi obično uključuju statički sadržaj koji se ponavlja u više zahteva [2].

3.1.2. DNS tuneliranje

DNS tuneliranje je napad koji je teško otkriti. Ovakav napad usmerava DNS zahteve ka serveru napadača, obezbeđujući im prikriveni komandni i kontrolni kanal i putanju za eksfiltraciju podataka [8]. DNS tuneliranje prikazano je na slici 10.

DNS je dobar kandidat za uspostavljanje tunela, što je termin za sajber bezbednost za protokolarnu vezu koja enkapsulira payload koji sadrži podatke ili komande i prolazi kroz odbranu perimetra. U suštini, DNS tuneliranje sakriva podatke unutar DNS upita koji se šalju serveru koji kontroliše napadač. DNS saobraćaju je generalno dozvoljeno da prolazi kroz odbranu perimetra, kao što su firewall-ovi, koji obično blokiraju ulazni i odlazni maliciozni saobraćaj [8].
Tipični slučajevi napada uključuju [9]:

- *Eksfiltracija podataka* - sajber kriminalci izvlače osetljive informacije preko DNS-a. Ovo nije najefikasniji pristup za dobijanje podataka sa računara „žrtve“, s obzirom na svo dodatno kodiranje i troškove, ali funkcioniše.
- *Komanda i kontrola (C2)* - sajber kriminalci koriste DNS protokol za slanje jednostavnih komandi za, na primer, instaliranje trojanskog programa za daljinski pristup (RAT).
- *IP-over-DNS tuneliranje* - neki uslužni programi su možda aktuelizovali IP stek preko konvencije o reakciji DNS upita. Ovo čini maliciozne akcije jednostavnijim.

DNS tuneliranje koristi DNS protokol za tuneliranje malicioznog payload-a i različitih podataka preko klijent-server modela. Ovo obično uključuje sledeće korake [9]:

1. Sajber kriminalac registruje domen, na primer malsite.com. DNS server usmerava ka serveru sajber kriminalca, gde je instaliran softver za tuneliranje malicioznih softvera.
2. Sajber kriminalac zaražava računar malicioznim softverom, koji prodire u firewall organizacije. DNS zahtevima je uvek dozvoljeno da ulaze i izlaze iz firewall-a, tako da je zaraženom računaru dozvoljeno da šalje upite DNS resolver-u. DNS resolver zatim šalje zahteve za IP adrese serverima najvišeg nivoa i root domena.
3. DNS resolver usmerava upite ka serveru sajber kriminalca, gde se implementira program tuneliranja. Tako se stvara veza između sajber kriminalca i „žrtve“ preko DNS resolver-a. Napadač može da koristi ovaj tunel za zlonamerne ciljeve, kao što je eksfiltracija informacija. Ne postoji direktna veza između sajber kriminalca i „žrtve“, pa je teže ući u trag računaru sajber kriminalca.

Kada je u pitanju detekcija malicioznih DNS napada, ono što predstavlja problem jeste da i tipičan DNS mrežni saobraćaj može biti bučan, što otežava razlikovanje sumnjivih ili neobičnih DNS upita od onih legitimnih [8].

ExtraHop reveal(x) automatski otkriva neobične promene u DNS saobraćaju na osnovu ponašanja uređaja tokom vremena, postavljajući upite koje treba istražiti. Branitelj može istražiti DNS upit sa kartice za otkrivanje [8].

4. PRIMER IMPLEMENTACIJE

Kao što je već pomenuto, osnovna namena ICMP-a je otkrivanje i kontrola problema sa umrežavanjem, tako da se njegova sposobnost da uspostavi kanal podataka između dve mašine često zanemaruje. Štaviše, budući da je ICMP suštinski, dobro uspostavljen deo Internet protokola i protokola koji nije na nivou aplikacije, manje je verovatno da će biti nadgledan tako pažljivo kao što je sučaj sa uobičajenom eksfiltracijom podataka – HTTP, HTTPS, TCP, IMAP itd.

Nakon detaljnog istraživanja, zaključeno je da postoji nekoliko uobičajenih alata za tuneliranje saobraćaja kroz ICMP. Neki od njih su:

1. Icmpsh
2. Ptunnel
3. Icmptunnel

Za implementaciju tuneliranja korišćen je Icmpsh alat, jer ne zahteva administrativne privilegije da bi se pokrenuo na „žrtvinoj“ mašini i lako je prenosiv.

Opisanom implementacijom vršiće se tuneliranje sesije reverzne Shell sesije između naše „napadačke“ Linux mašine i Windows 10 mašine „žrtve“, sa sledećim IP adresama:

- Napadač - 192.168.68.113
- Žrtva - 192.168.68.115

Na samom kraju rada detaljno je opisana i prikazana implementacija tuneliranja.

5. ZAKLJUČAK

Tema rada su protokoli tuneliranja, sa akcentom na protokole koji se mogu koristiti u ovu svrhu, iako im to nije osnovna namena. Detaljno je opisan proces tuneliranja, kao i tipovi metoda tuneliranja. Pored toga, opisani su protokoli tuneliranja, sa njihovim prednostima i nedostacima. Takodje, opisani su mogući napadi korišćenjem protokola tuneliranja, kao i načini njihove detekcije i prevencije. Na kraju rada je dat prikaz implementacije tuneliranja korišćenjem ICMP protokola tuneliranja, kojem ovo nije osnovna namena.

6. LITERATURA

[1] Cloudfare, What is tunneling? | Tunneling in networking (https://www.cloudflare.com/learning/network-layer/what-is-tunneling/)
[2] What is ICMP tunneling and how to protect against it (https://www.extrahop.com/company/blog/2021/detect-and-stop-icmp-tunneling/)
[3] DNS Tunneling – how DNS can be (ab)used by malicious actors (https://unit42.paloaltonetworks.com/dns-tunneling-how-dns-can-be-abused-by-malicious-actors/)
[4] Cloudfare, What is DNS | How DNS works (https://www.cloudflare.com/learning/dns/what-is-dns/)
[5] Working of DNS Server (https://www.geeksforgeeks.org/working-of-domain-name-system-dns-server/)
[6] What is DNS tunneling and how to protect against it (https://www.extrahop.com/company/blog/2020/dns-tunneling-definition-and-protection/)
[7] DNS tunneling: How it works, Detection and Prevention (https://www.neuralegion.com/blog/dns-tunneling/)
[8] 'Setting up a VPN' SkillSoft Press 2002.
[9] What is GRE tunneling? | How GRE tunneling works (https://www.cloudflare.com/learning/network-layer/what-is-gre-tunneling/)
[10] OpenVPN (https://openvpn.net/)
[11] What is L2TP and how does it work (https://www.techtarget.com/searchnetworking/definition/Layer-Two-Tunneling-Protocol-L2TP)
[12] GRE configuration with IPSec (https://systemzone.net/mikrotik-site-to-site-gre-tunnel-configuration-with-ipsec/)
[13] SSTP (https://help.mikrotik.com/docs/display/ROS/SSTP)
[14] Yamaha, L2TP/IPSec (https://www.yamaha.com/products/en/network/techdocs/vpn/l2tp_ipsec/)
[15] DNS tunneling (https://www.cynet.com/attack-techniques-hands-on/how-hackers-use-dns-tunneling-to-own-your-network/)

Kratka biografija

Dimitrije Salić je rođen 02. februara 1997. godine u Novom Sadu. Godine 2016. upisao je Fakultet tehničkih nauka, odsek Računarstvo i automatika. Oktobra 2020. godine je diplomirao. Iste godine upisao je master studije na Fakultetu tehničkih nauka u Novom Sadu, odsek Računarstvo i automatika, studijski program Elektronsko poslovanje. Master rad odbranio je u januaru 2022. godine.