



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ

DEPARTMENT OF INFORMATION SYSTEMS

DNS SPOOFING POMOCOU DNSMASQ

DNS SPOOFING WITH DNSMASQ

SEMESTRÁLNÍ PROJEKT

TERM PROJECT

AUTOR PRÁCE

AUTHOR

RADOSLAV PÁLENÍK

VEDOUCÍ PRÁCE

SUPERVISOR

Mgr. Ing. PAVEL OČENÁŠEK, Ph.D.

BRNO 2021

Abstrakt

Práca vytvorená pre zadanie „*Analýza komunikace s DNS serverem*“

Abstract

Thesis made for assignment „*DNS server communication analysis*“

Kľúčové slová

DNS, DNS spoofing, útok Man in the middle, dnsmasq

Keywords

DNS, DNS spoofing, Man in the middle attack, dnsmasq

Citácia

PÁLENÍK, Radoslav. *DNS spoofing pomocou dnsmasq*. Brno, 2021. Semestrální projekt. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Mgr. Ing. Pavel Očenášek, Ph.D.

DNS spoofing pomocou dnsmasq

Prehlásenie

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Očenaška. Další informace mi poskytl... Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....

Radoslav Páleník

5. mája 2021

Podakovanie

Ďakujem.

Obsah

1	Funkcionalita DNS a jeho bezpečnosť	2
2	Odchyt komunikácie a zmena dotazu	3
2.1	Príprava	3
2.1.1	dnsmasq.conf	3
2.1.2	dnsmasq.hosts	3
2.1.3	Spustenie Dnsmasq	4
2.2	Realizácia a analýza útoku	4
3	Zhodnotenie výsledkov	5
	Literatúra	6

Kapitola 1

Funkcionalita DNS a jeho bezpečnosť

Systém DNS poskytuje v internetovom prostredí jednu z najzákladnejších služieb. Jeho úlohou je udržiavať a poskytovať hierarchický systém prekladov zaregistrovaných doménových mien, subdomén, mailových serverov domén, a i. na IP adresy a naopak[7]. Služba DNS pracuje na protokole č.53 a komunikuje primárne pomocou protokolu UDP.

Funkčnosť tejto služby môže byť však ovplyvnená treťou stranou, ktorá sa môže snažiť službu buď znefunkčniť, alebo ju použiť vo svoj vlastný prospech tak, aby od obete získala citlivé, zneužiteľné údaje(napr.: prístupové údaje k internet bankingu, mailovej schránke, atď.).

Takéto údaje sa dajú získať napríklad pomocou *DNS spoofingu*[6], ktorého útok je predmetom tejto práce. Jedná sa o techniku, pri ktorej útočník vytvára vlastnú inštanciu DNS serveru, ktorú podvrhuje normálnym užívateľom inkriminovanej siete. Tento server preberá preklady doménových názvov od legitímneho DNS serveru pričom prekladu domén, na ktoré je útok cielený vymieňa za podvrhnuté IP adresy kontrolované útočníkom.

Kapitola 2

Odchyt komunikácie a zmena dotazu

2.1 Príprava

V práci sa postupovalo podľa [3] s pomocou nástroja **dnsmasq**[1] spúšťaného na operačnom systéme Ubuntu 20.04. Pre potreby zachytenia komunikácia bol použitý program Wireshark[5]. Pre fungovanie **dnsmasq** je potrebné vytvoriť dva konfiguračné súbory v adresári `/etc/`:

- **dnsmasq.conf** obsahuje konfiguráciu útočnickovho DNS serveru
- **dnsmasq.hosts** obsahuje preklady na falošné stránky definované útočníkom

2.1.1 dnsmasq.conf

Pre potreby útoku bol server nakonfigurovaný nasledovne:

no-daemon Vlákno procesu nebude presmerované na pozadie
log-queries Vypis logu dotazov a prekladov
no-dhcp-interface= Vypnutie poskytovania služby DHCP serverom
server=8.8.8.8 DNS server pre nemenú DNS premávku
no-hosts Ignorovanie predvoleného konfiguračného súboru 'host'
addn-hosts=/etc/dnsmasq.hosts Host súbor s nahradenými prekladmi domén, ktoré chce útočník presmerovať

2.1.2 dnsmasq.hosts

Podvrhnuté záznamy v súbore sú v tvare:

IP-adresa doménové-meno [alternatívne-doménové-mená]

V testovanom scenári vypadal súbor **dnsmasq.hosts** nasledovne:

23.23.23.23 www.facebook.com facebook.com
18.18.18.18 www.google.com

2.1.3 Spustenie Dnsmasq

Pre spustenie je potrebná mať nastavené správne oprávnenia na spúšťanie súborov, alebo spúšťať program pomocou príkazu `sudo`. S vyššie uvedenými konfiguračnými súbormi sa pre potreby práce spúšťa proces ako:

```
[sudo] dnsmasq
```

2.2 Realizácia a analýza útoku

Počas odchyty komunikácie posielala klient DNS dotazy na svoj `localhost` na ktorom je spustený lokálny DNS server(`dnsmasq`) pomocou utility `dig`[4]. Dotazované boli domény uvedené v 2.1.2 v dvoch tvaroch; spolu s prefixom „`www.`“, alebo bez neho.

```
rado@Rado:/mnt/c/Users/Rado$ dig @localhost google.com +short
172.217.23.238
rado@Rado:/mnt/c/Users/Rado$ dig @localhost www.google.com +short
18.18.18.18
rado@Rado:/mnt/c/Users/Rado$ dig @localhost facebook.com +short
23.23.23.23
rado@Rado:/mnt/c/Users/Rado$ dig @localhost www.facebook.com +short
23.23.23.23
```

Obr. 2.1: Dotazovanie pomocou príkazu `dig`

Na obrázku 2.1 je vidieť podvrhnutie falošnej adresy v odpovedi na dotaz pri zachytení hľadaného doménového mena. V prípade že sa nejednalo pre server o odchyťávanú komunikáciu, bola takáto komunikácia ďalej posunutá DNS serveru uvedenému v 2.1.1. Spracovanie takejto komunikácie je možné vidieť na 2.2. V opačnom prípade server spracuje dotaz vyhľadáním príslušného prekladu podľa súboru `dnsmasq.hosts`(2.1.2) a sám reaguje na prijatý dotaz.

```
dnsmasq: query[A] google.com from 127.0.0.1
dnsmasq: forwarded google.com to 8.8.8.8
dnsmasq: forwarded google.com to 172.25.96.1
dnsmasq: reply google.com is 172.217.23.238
dnsmasq: query[A] www.google.com from 127.0.0.1
dnsmasq: /etc/dnsmasq.hosts www.google.com is 18.18.18.18
dnsmasq: query[A] facebook.com from 127.0.0.1
dnsmasq: /etc/dnsmasq.hosts facebook.com is 23.23.23.23
dnsmasq: query[A] www.facebook.com from 127.0.0.1
dnsmasq: /etc/dnsmasq.hosts www.facebook.com is 23.23.23.23
```

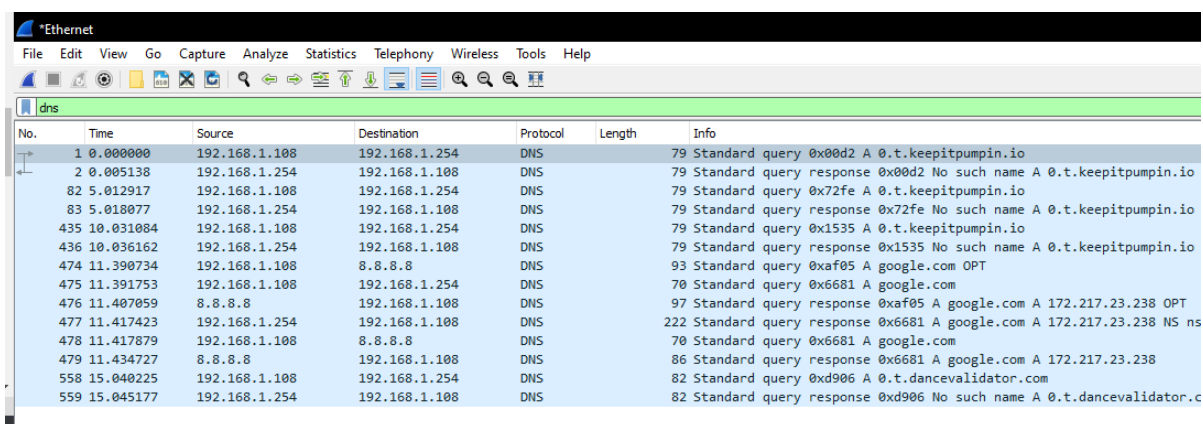
Obr. 2.2: Debugovací výstup programu `dnsmasq`

Kapitola 3

Zhodnotenie výsledkov

Cieľom útoku bolo pokúsiť sa vložiť medzi užívateľa a jeho preferovaný DNS server prostredníka, ktorý je schopný pozmeniť ich komunikáciu. Samotný odchyt komunikácie a jeho zmena sa nejakví ako náročná časť pri plánovaní takéhoto útoku. Je to spôsobené hlavne tým že DNS neposiela nejak zašifrované dotazy, a teda celá jeho komunikácia je čitateľná, čo využíva pravé server dnsmasq ktorý vie ľahko zistiť ktorú komunikáciu má odchytiť a nahradiť vlastnou odpoveďou.

Pokiaľ by chcel užívateľ jeho DNS komunikáciu zašifrovať, musel by použiť služby ako DNS over HTTPS alebo DNS over TLS [2]. Tieto služby komunikáciu na momentálne používanej sieti síce zašifrujú, no posúvajú tento problém len k tretej strane so znakom dôvery že u nej táto komunikácia nebude zneužitá.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.108	192.168.1.254	DNS	79	Standard query 0x00d2 A 0.t.keepitpumpin.io
2	0.005138	192.168.1.254	192.168.1.108	DNS	79	Standard query response 0x00d2 No such name A 0.t.keepitpumpin.io
82	5.012917	192.168.1.108	192.168.1.254	DNS	79	Standard query 0x72fe A 0.t.keepitpumpin.io
83	5.018077	192.168.1.254	192.168.1.108	DNS	79	Standard query response 0x72fe No such name A 0.t.keepitpumpin.io
435	10.031084	192.168.1.108	192.168.1.254	DNS	79	Standard query 0x1535 A 0.t.keepitpumpin.io
436	10.036162	192.168.1.254	192.168.1.108	DNS	79	Standard query response 0x1535 No such name A 0.t.keepitpumpin.io
474	11.390734	192.168.1.108	8.8.8.8	DNS	93	Standard query 0xaf05 A google.com OPT
475	11.391753	192.168.1.108	192.168.1.254	DNS	70	Standard query 0x6681 A google.com
476	11.407059	8.8.8.8	192.168.1.108	DNS	97	Standard query response 0xaf05 A google.com A 172.217.23.238 OPT
477	11.417423	192.168.1.254	192.168.1.108	DNS	222	Standard query response 0x6681 A google.com A 172.217.23.238 NS ns
478	11.417879	192.168.1.108	8.8.8.8	DNS	70	Standard query 0x6681 A google.com
479	11.434727	8.8.8.8	192.168.1.108	DNS	86	Standard query response 0x6681 A google.com A 172.217.23.238
558	15.040225	192.168.1.108	192.168.1.254	DNS	82	Standard query 0xd906 A 0.t.dancevalidator.com
559	15.045177	192.168.1.254	192.168.1.108	DNS	82	Standard query response 0xd906 No such name A 0.t.dancevalidator.c

Obr. 3.1: Komunikácia zachytená pomocou programu Wireshark s filtrovaním DNS datagramov

Ako vidieť na 3.1, komunikácia ktorá bola zachytená pomocou programu dnsmasq sa zo zariadenia neposunula na žiadne iné zariadenie, čo pri útoku zabezpečí krytie pre server vložený do inkriminovanej siete.

Zložitejšie na tomto útoku však je zaujať pozíciu ako Man-in-the-middle[8] pre daný server, aby mohol danú sieť infiltrovať a mal možnosť posielat odpovede pre hostov na zadané stránky. Zaujatie takejto pozície na pomery tejto práce nebolo možné realizovať. Taktiež je potrebné mať pripravenú infraštruktúru, na ktorú má byť obeť presmerovaná.

Literatúra

- [1] *Dnsmasq*. Dostupné z: <https://thekelleys.org.uk/dnsmasq/doc.html>.
- [2] CLOUDFLARE. *DNS over TLS vs. DNS over HTTPS: Secure DNS*. Dostupné z: <http://www.cloudflare.com/learning/dns/dns-over-tls/>.
- [3] HECKEL, P. C. *How To: DNS spoofing with a simple DNS server using Dnsmasq*. Jul 2013. Dostupné z: <https://blog.heckel.io/2013/07/18/how-to-dns-spoofing-with-a-simple-dns-server-using-dnsmasq/>.
- [4] INTERNET SYSTEMS CONSORTIUM, INC. *Dig(1) - Linux man page*. Dostupné z: <https://linux.die.net/man/1/dig>.
- [5] THE WIRESHARK TEAM. *Wireshark · Go Deep*. 2021. Dostupné z: <https://www.wireshark.org/>.
- [6] WIKIPEDIA CONTRIBUTORS. *DNS spoofing* — *Wikipedia, The Free Encyclopedia*. 2021. [Online; accessed 4-May-2021]. Dostupné z: https://en.wikipedia.org/w/index.php?title=DNS_spoofing&oldid=1018614964.
- [7] WIKIPEDIA CONTRIBUTORS. *Domain Name System* — *Wikipedia, The Free Encyclopedia*. 2021. [Online; accessed 5-May-2021]. Dostupné z: https://en.wikipedia.org/w/index.php?title=Domain_Name_System&oldid=1016463086.
- [8] WIKIPEDIA CONTRIBUTORS. *Man-in-the-middle attack* — *Wikipedia, The Free Encyclopedia*. 2021. [Online; accessed 4-May-2021]. Dostupné z: https://en.wikipedia.org/w/index.php?title=Man-in-the-middle_attack&oldid=1020124191.