DNS

ISA - Laboratorní cvičení č.3

Vysoké učení technické v Brně

`https://github.com/nesfit/ISA/tree/master/dns-security`

Cíl laboratorního cvičení

- Seznámit se s systémem DNS.
- Prozkoumat data přenášená v protokolu DNS, DNS over HTTPS pomocí programu Wireshark.
- Rozšifrovat zachycenou komunikaci z prohlížeče (Firefox).
- Nastavit šifrovanou komunikaci DNS over TLS.
- Nastavit šifrovanou komunikaci DNS přes DNS over TLS a zároveň filtrace DNS reklamních a malware domén.

Pokyny

- Pro práci v cvičení budeme používat virtuální stroj v programu VirtualBox[1]. Pokud z předchozích cvičení máte provedeny nějaké změny ve virtuálním stroji, obnovte ho do výchozího stavu.
- Před zahájením cvičení si vytvořte snapshot virtuálního stroje za pomoci menu *Machine* → *Take snapshot* pro snadný návrat k výchozímu stavu.
- Odpovědi pište do odpovědního archu `protokol.md` který odevzdáte do WIS-u. Dostupný je na adrese `https://github.com/nesfit/ISA/blob/master/dns-security/protokol.md`.
- Do WIS-u budete také odevzdávat všechny zachycené `pcap` soubory.
- Uživatelé a hesla pro přihlášení: `user - user4lab`, `root - root4lab`.
- Přihlaste se jako uživatel `user`. Veškeré potřebné příkazy následně spouštějte jako `root`.

1 Překlad DNS dotazů

1. Spusťte program Wireshark (vždy jako `root` z příkazové řádky příkazem `wireshark &`) a začněte zachytávat komunikaci na rozhraní, pomocí kterého jste připojeni k Internetu (`enp0s3`).
2. Otevřete terminál a pomocí příkazu `nslookup -type=ns vutbr.cz` zjistěte autoritativní DNS servery pro doménu `vutbr.cz` a zapište je do odpovědního archu.
3. Zastavte zachytávání komunikace v programu Wireshark. Zachycený provoz uložte do souboru `cv3-dns.pcap`, který budete odevzdávat.

[1] `https://nes.fit.vutbr.cz/isa/ISA2020.ova`

4. V zachyceném provozu nalezněte pakety obsahující komunikaci Vámi provedeného dotazu na doménu `vutbr.cz` a prozkoumejte je.

5. Do odpovědního archu zapište *display filter*, kterým vyfiltrujete pouze pakety související s DNS provozem.

6. Kolik paketů souvisejících s Vaším dotazem na doménu bylo zachyceno? Číslo zapište do odpovědního archu.

7. Byl proveden rekurzivní nebo iterativní DNS dotaz? Jak jste to zjistili ze zachyceného provozu? Zapište do odpovědního archu.

8. Na jakou IP adresu směřoval paket s DNS dotazem? Komu náleží tato IP adresa? Pokud netušíte, jakému zařízení IP adresa náleží, zkuste se podívat na virtuálním systému do souboru `/etc/resolv.conf` a/nebo v příkazové řádce hostujícího operačního systému zadejte příkaz `ipconfig /all` (v případě OS Windows) a prohlédněte si výpis.

2 Zabezpečení a překlad pomocí DNS over HTTPS

1. Spusťe prohlížeč Firefox.

2. V prohlížeči přistupte do `Preferences` pak sescrollujte dolů na položku `Network Settings` a klikněte na tlačítko `Settings`. V dialogovém okně najděte položku `Enable DNS over HTTPS` a zaškrtněte. Provider nastavte na `Custom` a vyplňte nově vzniklé pole tímto url `https://odvr.nic.cz/doh`.

3. Potvrďte změny kliknutím na tlačítko `OK` a prohlížeč zavřete.

4. Spusťte program Wireshark jako uživatel `root` z terminálu příkazem `wireshark &` a začněte zachytávat provoz na všech rozhraních.

5. Pro pozdější rozšifrování HTTPS komunikace z prohlížeče je nutné nastavit proměnnou prostředí `SSLKEYLOGFILE=<cesta_k_souboru>`, na kterou prohlížeče Firefox, Chrome a případně další reagují.

6. Otevřete terminál a jako uživatel `user` zadejte `export SSLKEYLOGFILE=/home/user/Desktop/keylogfile.log`.

7. Následně ve stejném okně terminálu, ve kterém jste nastavili proměnnou prostředí `SSLKEYLOGFILE`, spusťte jako uživatel `user` prohlížeč Firefox příkazem `firefox &`.

8. Přistupte na pár webových stránek, které Vás napadnou. Následně prohlížeč zavřete a tuto akci ještě jednou či vícekrát zopakujte, pokaždé ideálně s jinými webovými stránkami. Nakonec prohlížeč zavřete.

9. Následně zastavte zachytávání v programu Wireshark.

10. Zachycenou komunikaci uložte do souboru `cv3-DoH.pcap`, který budete odevzdávat.

11. Představ si sebe jako útočníka, který zachytil neznámou komunikaci do souboru `cv3-DoH.pcap` a nemá k ní žádné další informace. Dokázali byste v tuto chvíli zjistit ze zachyceného DNS provozu, jaké domény byly přes prohlížeč Firefox navštíveny? Proč? Odvěď uveďte do odpovědního archu.

12. V programu Wireshark otevřete `Edit > Preferences` a zde v levém sloupci rozklikněte `Protocols` a zde nalezněte položku `TLS`. Na této kartě je potřeba nastavit `(Pre)-Master-Secret log filename` na váš keylogfile (`/home/user/Desktop/keylogfile.log`). Aplikujte změnu kliknutím na `OK`. Nyní by mělo proběhnout rozšifrování provozu.

13. Pomocí *display filteru* vyfiltrujte pouze TLS provoz. Do odpovědního archu zapište, jaký *display filter* jste zadali. Pokuste se nalézt pakety protokolu DoH (DNS over HTTPS).

14. Pokud se Vám to podařilo, podívejte se jak vypadá obsah paketu.

    - Pokud se vám nepodařilo nalézt pakety s DoH, ve složce `/home/user/doh-pcaps/` naleznete `.zip` soubor po jehož rozbalení objevíte soubor `doh-decrypted.pcapng`. Když ve Wiresharku otevřete tento soubor, měli byste narazit na již dešifrovaný TLS provoz, ve kterém DoH pakety již určitě naleznete.

15. Vyberte si libovolnou zachycenou DoH odpověď a do odpovědního archu opište jeden řádek z položky `Answers`.

16. Jaká je cílová IP adresa pro pakety s DoH dotazy? Jaké doménové jméno patří k této IP adrese? Zapište do odpovědního archu.

17. Před postupem k další části cvičení nezapomeňte otevřít prohlížeč a na stejném místě v `Preferences` položku `Enable DNS over HTTPS` opět vypnout a prohlížeč zavřít.

3 Zabezpečení a překlad pomocí DNS over TLS

1. Deaktivujte SELinux jako uživatel `root` pomocí příkazu `setenforce 0`.

2. Zároveň v souboru `/etc/selinux/config` zkontrolujte a případně upravte řádek s proměnnou `SELINUX` následovně `SELINUX=disabled`. NErestartujte v tuto chvíli počítač.

3. Nainstalujete Unbound DNS caching resolver pomocí příkazu `yum install unbound -y`.

4. V souboru `/etc/unbound/unbound.conf` najděte příslušnou část pro úpravu forward zón (pod řádkem začínajícím `# Forward zones` a přidejte následující:

```
forward-zone:
    name: "."
    forward-ssl-upstream: yes
    # Cloudflare DNS
    forward-addr: 1.1.1.1@853
    forward-addr: 1.0.0.1@853
```

5. Jakmile je soubor upraven, uložte jej a restartujte službu pomocí příkazu `systemctl restart unbound`.

6. Ověřte zdali služba běží bez problémů pomocí `systemctl status unbound`.

7. V souboru `/etc/resolv.conf` nastavte nameserver na IP adresu `127.0.0.1`.

8. Nyní spusťte program Wireshark a spusťte zachytávání na rozhraní, pomocí kterého jste připojeni k Internetu.

9. Pokuste se vygenerovat nějaký DNS provoz pomocí webového prohlížeče, a to konkrétně přístupem na web `idnes.cz`.

10. Vyčkejte než se stránka celá načte a důkladně si ji prohlédněte.
11. Následně zavřete tab s načtenou stránkou i prohlížeč samotný.
12. Zastavte zachytávání provozu. Zachycený provoz uložte jako soubor `cv3-DoT.pcap`, který budete odevzdávat.
13. V programu Wireshark pomocí *display filteru* vyfiltrujte pouze pakety, které využívají port 853 nad protokolem TCP. Jaký filtr přesně jste použili? Zapište do odpovědního archu.
14. Následně vyfiltrujte pakety, které obsahují port 53 nad protokolem TCP nebo UDP. Jaký filtr přesně jste použili zde? Opět zapište do odpovědního archu.
15. Jaká služba běží nad portem 53? Kolik paketů se zdrojovým nebo cílovým portem 53 bylo zachyceno? Odpovězte do odpovědního archu a zamyslete se, proč právě takové číslo.

4 Blokování reklam a další

1. Na začátek souboru `/etc/unbound/unbound.conf` pod řádek obsahující `server:` přidejte následující:

```
interface: 127.0.0.1
port: 5335
do-ip4: yes
do-udp: yes
do-tcp: yes
do-ip6: yes
```

2. Restartujte službu unbound DNS caching serveru pomocí příkazu `systemctl restart unbound`.
3. Pomocí příkazu `systemctl enable unbound` nastavte povolení služby na systému.
4. Stáhněte pi-hole instalační skript pomocí příkazu `wget -O basic-install.sh https://install.pi-hole.net`.[2]
5. Instalační skript si prohlédněte, zdali neobsahuje žádný škodlivý kus zdrojového kódu.[3]
6. Spusťte instalační skript pi-hole pomocí příkazu `sudo bash basic-install.sh`.
7. Instalací pi-hole vás bude provázet dialogové okno, ve kterém bude nutné vybrat následující možnosti:
   (a) V dialogovém okně budete dotázáni na instalaci PHP. V tomto případě vyberte možnost `no`.
   (b) Potvrďte, že souhlasíte, aby se Vaše zařízení stalo blokátorem reklam.
   (c) Potvrďte informaci, že se jedná o software zdarma.
   (d) Potvrďte, že rozumíte nutnosti přidělení statické IP adresy v lokální síti.
   (e) Při výběru síťového rozhraní nechte zaškrtnuté ethernetové (`enp0s3`).

[2] Pihole je populární open-source DNS sink-hole, jehož zdrojové kódy můžete nalézt na adrese `https://github.com/pi-hole/pi-hole/`, ostatně taktéž tento instalační skript se stahuje z tohoto oficiálního GitHub repozitáře

[3] Tento krok jsme již provedli a proto ho můžete v tomto případě přeskočit.

(f) U výběru "Upstream DNS Provider"sescrollujte dolů, kde zvolte možnost `Custom` a následně pro adresu serveru zadejte `127.0.0.1#5335` a potvrďte klávesou `Enter`. Také v dalším okně potvrďte adresu serveru.

(g) Dále při výběrů blocking listů ponechte zaškrtnuté oba dva listy.

(h) Zbytek nastavení ponecháme ve výchozím stavu a jenom vždy odsouhlasíme buď `yes` nebo `ok`.

8. Jakmile je instalace pi-hole dokončena, restartujte systém pomocí příkazu `reboot`.

9. Přihlašte se do systému a zkontrolujte zdali pi-hole běží v pořádku:

   (a) Spusťte příkaz `pihole status`.

   (b) Zkontrolujte obsah souboru `/etc/resolv.conf`, měl by obsahovat záznam pro nameserver ukazující na `127.0.0.1#5335`.

10. Spusťte prohlížeč Firefox a přistupte znovu na stránku `idnes.cz`. Jaký rozdíl jste vypozorovali? Zapište do odpovědního archu.

11. Pořiďte snímek obrazovky s načtenou webovou stránkou `idnes.cz` tak, aby vypozorovaný rozdíl byl na snímku obrazovky viditelný, a uložte snímek obrazovky jako obrázek s názvem `cv3-idnes.{png|jpg|jpeg|...}` v dostatečně nízkém rozlišením, aby ho bylo možné odevzdat do WIS-u.

Poznámka ke cvičení

Použití nasazení nástroje pi-hole lokálně na zařízení není úplně standardní a je v této konfiguraci pouze z demonstračních důvodů. Standardně je tato aplikace určena pro nasazení na samostatném serveru (například Raspberry Pi) běžícím v lokální síti a použití tohoto serveru všemi zařízeními v síti jednotně. Je možné jej pak zkombinovat i s tunelováním DNS přes TLS jako v tomto cvičení (viz úloha 3). Pro případné nasazení na serveru v lokální síti bude potřeba pár drobných změn v tomto cvičení.

Odevzdávané soubory

Zkontrolujte, zda máte všechny soubory které se budou odevzdávat:

- `protokol.md`
- `cv3-dns.pcap`
- `cv3-DoH.pcap`
- `cv3-DoT.pcap`
- `cv3-idnes.{png|jpg|jpeg|...}`

Ukončení práce v laboratoři

- Do WIS-u odevzdejte vyplněný `protokol.md`, všechny zachycené `pcap` soubory a snímek obrazovky.
- Vypňete virtuální stroj a obnovte jeho snapshot vytvořený na začátku této laboratoře.