VYSOKÉ UČENIE TECHNICKÉ V BRNE
FAKULTA INFORMAČNÝCH TECHNOLOGIÍ

Přenos dat, počítačové sítě a protokoly (PDS)

2017/2018

DHCP Útoky

Ľubomír Gallovič (xgallo03)

Marec 2018

Obsah

1 Úvod

Cieľom projektu bolo si naštudovať problematiku útokov na DHCP, implementovať útoky DHCP starvation a Rogue DHCP server, otestovať ich na reálnej alebo virtuálnej sieti a demonštrovať ich činnosť.

2 Útoky na DHCP

DHCP, alebo Dynamic Host Configuration Protocol je sieťový protokol, ktorý definuje akým spôsobom DHCP server dynamicky prideľuje IP adresy jednotlivým klientom. Zmyslom protokolu je zrušiť nutnosť admonistrátora siete klientom manuálne prideľovať IP adresy. Táto služba býva častokrát v reálnych sieťach nedostatočne zabezpečená a útokmi na ňu je možné docieliť Denaial of service, podvrhovanie ilegitímnych informácií klientovi (napríklad vlastnú adresu DNS servera), alebo sledovanie internetovej prevádzky klientov. Útoky, ktoré sa u DHCP najčastejšie vyskytujú sú DHCP starvation a Rogue DHCP server.

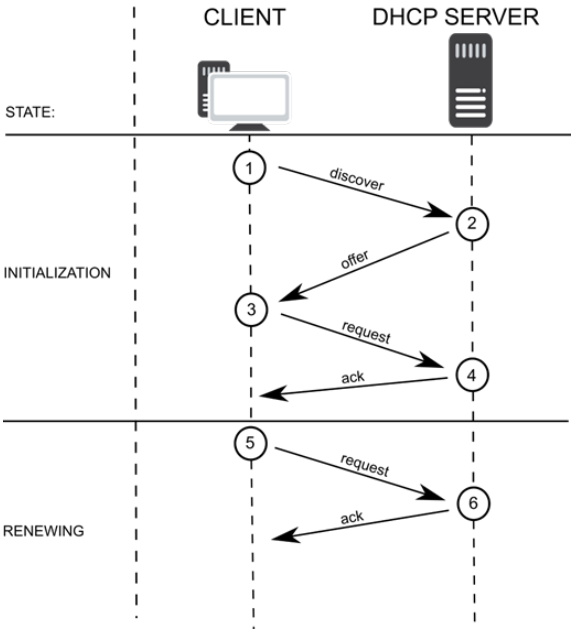

Figure 1: Princíp DHCP komunikácie

2.1 DHCP komunikácia

Na vykonávanie úspešných útokov na DHCP je najprv nutné byť oboznámený s presným protokolom DHCP komunikácie. Komunikácia definovaná v DHCP je nasledovná: Nový klient po pripojení do siete odošle na broadcast správu DISCOVER, ktorou žiadá dostupné servery na danej sieti o pridelenie IP adresy. Klient takisto môže žiadať o doplňujúce informácie pre prístup na internet, ako je napríklad maska siete, adresa DNS servera a predvolená brána siete. Každý DHCP server, ktorý správu dostane a má k dispozícii voľnú IP adresu odpovie správou OFFER, ktorá obsahuje ponúkanú IP adresu. Klient spätne odošle správu REQUEST, ktorou žiadá server o ponúkanú adresu. Server má možnosť odpovedať správou ACK, ktorou tento požiadavok povoľuje, alebo NAK, ktorou ho zamietne. Správa ACK okrem pridelenej IP adresy obsahuje tiež dodatočné informácie žiadané klientom, ktoré mohol server poskytnúť. Ak server odpovedal správou ACK, môže klient danú adresu používať pre prístup na internet.

IP adresa však klientovi väčšinou nie je pridelená na neurčitú dobu, ale server mu ju rezervoval len na konečný čas nazývaný Lease time, ktorý je obsiahnutý v ACK správe. Po vypršaní 50% rezervovaného času prejde klient do stavu RENEWING a znovu pošle serveru správu REQUEST, ktorou ho žiadá o predĺženie rezervovaného času. Čas je predĺžený, ak server odpovie správou ACK. Ak nedošlo k predĺženiu času prejde klient po vypršaní 87,5% rezervovaného času do stavu REBINDING, v ktorom žiadá o predĺženie od všetkých dostupných serverov. Ak sa mu predĺženie nepodarilo ani druhý krát, stráca po vypršaní času svoju pridelenú IP adresu a musí znova začať DHCP komunikáciu ako nový klient. V prípade, že klient má pridelenú IP adresu a sám sa rozhodol odísť zo siete, odošle serveru správu RELEASE, ktorou sa vzdáva pridelenej IP adresy.

2.2 DHCP starvation

Prvý druh útoku sa nazýva DHCP starvation, a jeho cieľom je zarezervovanie si všetkých dostupných IP adries od DHCP servera. Pri pripojení nového klienta do siete mu nebude možné poskytnúť žiadnu IP adresu, čo má za následok Denial of Service. Útok začína odosielaním veľkého množstva DISCOVER správ, pričom cieľom je zaistiť, aby každá z týchto správ sa javila byť od iného klienta. Súčasťou identifikácie klienta v správe je jeho MAC adresa, ktorú musí útočník pre jednotlivé komunikácie spoofovať. Po odpovedi servera pokračuje každá individuálna komunikácia protokolom popísaným vyššie, až kým server falošnému klientovi nezarezervuje IP adresu. Zahlcovanie servera správami pokračuje, dokiaľ nie sú vyčerpané všetky adresy ponúkané serverom. Následkom tohto útoku je, že novému klientovi pripojenému do siete nebude server schopný prideliť IP adresu, a tým mu je zamedzený prístup na internet.

Pre útočníka je tiež vhodné naimplementovať protokoly pre stavy RENEWING a REBINDING, pretože jeho cieľom môže byť dlhodobé udržiavanie rezervovaných adries. Je potrebné poznamenať, že tento útok nefunguje na klientov, ktorí sa už v sieti nachádzajú a server im pridelil IP adresu skôr ako k útoku došlo. Avšak zahlcovanie DHCP servera packetmi od útočníka môže spôsobiť jeho paralýzu, čo má za dôsledok nemožnosť komunikácie s legitímnym klientom a neschopnosť klienta si predĺžit rezervovaný čas IP adresy. Po určitom čase nebude mať žiaden z legitímnych klientov možnosť získať IP adresu, a nebude môcť využívať služby internetu.

2.3 Rogue DHCP server

Druhý útok je Rogue DHCP server, teda falošný server, ktorý poskytuje klientom ktorí s ním komunikujú falošné informácie. Klienti okrem IP adresy od servera spravidla žiadajú aj ďalšie informácie o sieti, ktoré môže útočník využiť. Najjdenoduchšou formou útoku je, že Rogue server klientovi odošle nesprávnu IP adresu alebo masku siete, čím mu zamedzí prístup na internet a spôsobí DoS útok. Ďalšiu formu útoku je Man in the middle attack, ktorý je dosiahnutý tak, že brána siete, ktorú Rogue server klientovi odoslal je IP adresa útočníka. Útočník prichádzajúce dáta preposiela na reálnu bránu siete a získava schopnosť sledovať sieťovú prevádzku klienta bez jeho vedomosti. Útočník takisto môže vykonať Phishing attack tak, že podvrhne adresu nelegitímneho DNS servera. Tento server presmeruje klienta na falošné verzie navštívených webových stránok, a umožňuje útočníkovi získať citlivé údaje.

Existujú dve varianty Rogue serveru: prvá varianta pracuje popri reálnom DHCP serveri a snaží sa ho predbehnúť pri komunikácii s klientom, a druhá varianta najprv odstaví legitímny server a až potom sa stane falošným serverom. V prvej variante falošný server čaká na DISCOVER packet od klienta, ktorý po príchode prepošle legitímnemu serveru. Reálny server mu odpovie správou OFFER, ktorú Rogue server prepošle klientovi. Komunikácia prebieha podobne pri REQUEST a ACK

packetoch, avšak do ACK packetu má útočník možnosť podvrhnúť falošné informácie, skôr ako tento packet prepošle klietovi. Výhoda tejto varianty je, že je ťažšie detekovateľná, pretože nerobí útok na reálny DHCP server. Nevýhodou je, že útočník môže byť pri preposielané pakcetov príliš pomalý, čo spôsobí, že klient nadviaže komunikáciu s legitímnym serverom.

Druhá varianta Rogue DHCP servera je, že útočník najprv získa všetky IP adresy od legitímneho servera a tieto adresy sám začne prideľovať pripojujúcim sa klientom. Získanie všetkých adries od reálneho serveru je dosiahnuté útokom DHCP starvation popísaným vyššie. Reálny server nemôže novým klientom ponúknuť IP adresy, a teda klienti nemajú inú možnosť, iba komunikovať s falošným DHCP serverom. Rogue server môže následne všetkým novým klientom podvrhnúť požadované informácie.

3 Implementácia

Boli vyvinuté dve programy pre útok na DHCP: pds-dhcpstarve pre DHCP starvation a pds-dhcprogue pre Rogue DHCP server. Programy boli vyvíjané v jazyku C++ a pracujú s knižnicou pcap.h pomocou ktorej zachytávajú DHCP packety na sieti a odosielajú vlastné packety. Zdrojový kód je rozdelený do troch súborov: pds-dhcpstarve.cpp implementujúci funkcie potrebné pre prvý program, pds-dhcprogue.cpp implementujúci funkcie pre druhý program a common.cpp implementujúci funkcie využívané oboma útokmi.

3.1 DHCP starvation

Prvý program vykonáva útok DHCP starvation popísaný vyššie. Súčasťou implementácie je vytváranie vlastných DHCP packetov vrátane spoofovnia MAC adries. Program si udržiava informácie o individuálnych komunikáciách s DHCP serverom vrátane štádia daného požiadavku (SELECTING, RENEWING, REBINDING). Ak mu je pridelená IP adresa, prejde po uplynutí dostatku času do stavov RENEWING a REBINDING a snaží sa predĺžiť si lease time. Ak server neodpovedá na niektorý jeho požiadavok, prepošle packet znovu. Po viacerých neúspešných pokusoch preruší komunikáciu a danú transakciu vymaže z pamäte. V programe je možné definovať ako často posiela DISCOVER packety a ako dlho má čakať pri neodpovedajúcom serveri pred ukončením komunikácie.

3.2 Rogue DHCP server

Bola implementovaná druhá verzia DHCP servera, teda najprv dôjde k útoku DHCP starvation, a následne začne falošný server ponúkať získané IP adresy jednotlivým klientom. Rogue server sa teda neustále snaží získavať IP adresy od legitímneho servera a predĺžovať rezervovaný čas, pričom zároveň komunikuje s klientami a manažuje prideľovanie získaných adries. Okrem prideľovania adries je implementované aj predĺžovanie lease time v stavoch RENEWING a REBINDING a takisto správa RELEASE po ktorej je IP adresa uvoľnená. Server konštruuje vlastné packety, do ktorých podvrhuje informácie špecifikované v argumentoch programu.

4 Demonštrácia činnosti

Programy boli testované a sú demonštrované na virtuálnej sieti načrtnutej nižšie. Na vytvorenie siete bol použitý program VMware, a každý z virtuálnych počítačov beží na operačnom systéme Ubuntu 17.10.

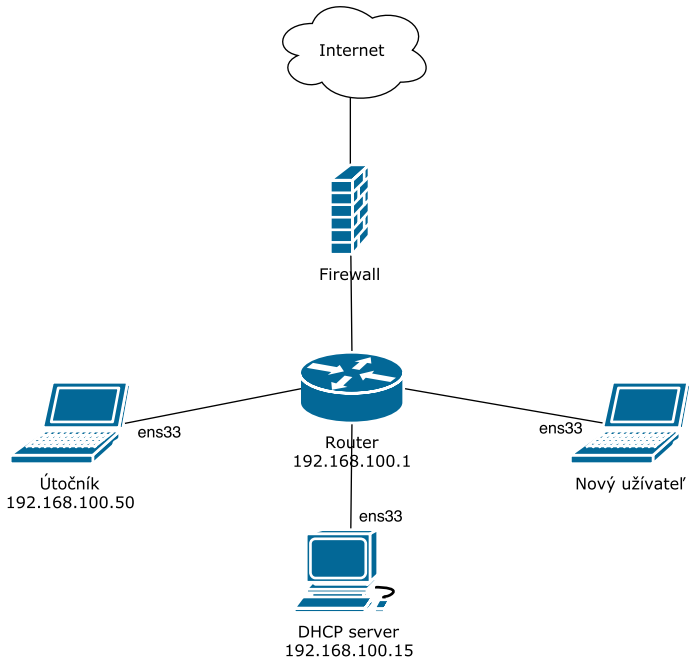

Figure 2: Topológia virtuálnej siete

Na jednom s počítačov beží DHCP server, ktorí prideľuje IP adresy v rozmedzí 192.168.100.50 - 192.168.100.70, teda 20 adries. Útočníkovi server po pripojení do siete pridelí adresu 192.168.100.50. Demonštrácia útokov bude prebiehať programom pds-dhcprogue, pretože vykonáva obidva útoky.Program je spustený s nasledujúcimi parametrami:

```
sudo ./pds-dhcprogue -i ens33 -p 192.168.100.60-192.168.100.70
    -g 192.168.100.1 -n 209.244.0.3 -d google.com -l 300
```

Po spustení programu je legitímny DHCP server zahltený DISCOVER packetmi:

```
 73 60.483893670  0.0.0.0          255.255.255.255    DHCP     286 DHCP Discover - Transaction ID 0x110bdb94
 75 60.584750919  0.0.0.0          255.255.255.255    DHCP     286 DHCP Discover - Transaction ID 0x681b3c22
 77 60.685673721  0.0.0.0          255.255.255.255    DHCP     286 DHCP Discover - Transaction ID 0x187ab7c4
 79 60.786621514  0.0.0.0          255.255.255.255    DHCP     286 DHCP Discover - Transaction ID 0x27a14502
 81 60.922832689  0.0.0.0          255.255.255.255    DHCP     286 DHCP Discover - Transaction ID 0x1c693758
 83 61.023414311  0.0.0.0          255.255.255.255    DHCP     286 DHCP Discover - Transaction ID 0xc8022180
```

Server následne ponúka adresy správami OFFER, na ktoré útočník odpovedá správami REQUEST.

```
107 61.587270291  192.168.100.15   255.255.255.255    DHCP     342 DHCP Offer    - Transaction ID 0x681b3c22
111 61.688885467  192.168.100.15   255.255.255.255    DHCP     342 DHCP Offer    - Transaction ID 0x187ab7c4
115 61.789337507  192.168.100.15   255.255.255.255    DHCP     342 DHCP Offer    - Transaction ID 0x27a14502
121 61.924930622  192.168.100.15   255.255.255.255    DHCP     342 DHCP Offer    - Transaction ID 0x1c693758
125 62.025856115  192.168.100.15   255.255.255.255    DHCP     342 DHCP Offer    - Transaction ID 0xc8022180
129 62.124783968  0.0.0.0          255.255.255.255    DHCP     298 DHCP Request  - Transaction ID 0x8be18258
130 62.125199999  0.0.0.0          255.255.255.255    DHCP     298 DHCP Request  - Transaction ID 0xf3c3bab8
131 62.125577703  0.0.0.0          255.255.255.255    DHCP     298 DHCP Request  - Transaction ID 0x953cacb2
132 62.125952118  0.0.0.0          255.255.255.255    DHCP     298 DHCP Request  - Transaction ID 0x110bdb94
```

Server potvrdí žiadané adresy packetom ACK, až kým nazarezervuje všetky adresy.

```
142 62.135844778  192.168.100.15   255.255.255.255    DHCP     342 DHCP ACK      - Transaction ID 0x953cacb2
143 62.137016477  192.168.100.15   255.255.255.255    DHCP     342 DHCP ACK      - Transaction ID 0x110bdb94
144 62.137624246  192.168.100.15   255.255.255.255    DHCP     342 DHCP ACK      - Transaction ID 0x681b3c22
145 62.138169290  192.168.100.15   255.255.255.255    DHCP     342 DHCP ACK      - Transaction ID 0x187ab7c4
146 62.138767723  192.168.100.15   255.255.255.255    DHCP     342 DHCP ACK      - Transaction ID 0x27a14502
147 62.139366711  192.168.100.15   255.255.255.255    DHCP     342 DHCP ACK      - Transaction ID 0x1c693758
```

Súčasťou funkcionality útoku DHCP starvation je aj predĺžovanie času, na ktorý rezervoval server útočnikovi IP adresy. Pred tým ako server útočníkovi odoberie získané IP adresy pošle útočník REQUEST packety, vďaka ktorým mu server predĺži rezervovaný čas.

```
627 558.154941846 192.168.100.56   255.255.255.255   DHCP    286 DHCP Request  - Transaction ID 0x681b3c22
628 558.155429652 192.168.100.55   255.255.255.255   DHCP    286 DHCP Request  - Transaction ID 0x110bdb94
629 558.155852035 192.168.100.54   255.255.255.255   DHCP    286 DHCP Request  - Transaction ID 0x953cacb2
630 558.156232573 192.168.100.53   255.255.255.255   DHCP    286 DHCP Request  - Transaction ID 0xf3c3bab8
631 558.156675604 192.168.100.52   255.255.255.255   DHCP    286 DHCP Request  - Transaction ID 0x8be18258
632 558.157550603 192.168.100.15   255.255.255.255   DHCP    342 DHCP ACK      - Transaction ID 0x27a14502
633 558.160114803 192.168.100.15   255.255.255.255   DHCP    342 DHCP ACK      - Transaction ID 0x1c693758
634 558.162156581 192.168.100.15   255.255.255.255   DHCP    342 DHCP ACK      - Transaction ID 0xc8022180
635 558.164016228 192.168.100.15   255.255.255.255   DHCP    342 DHCP ACK      - Transaction ID 0x187ab7c4
```

Týmto mechanizmom má útočník adresy rezervované na neurčitú dobu.

Druhým útokom je Rogue DHCP server, ktorý pracuje v spolupráci s DHCP starvation. Útočník má rezervované všetky IP adresy DHCP servera, a po pripojení nového klienta mu ponúkne adresu z povoleného rozmedzia.

Výpis získavania IP adresy nového klienta od Rogue DHCP servera:

```
Listening on LPF/ens33/00:0c:29:c3:91:75
Sending on   LPF/ens33/00:0c:29:c3:91:75
Sending on   Socket/fallback
DHCPDISCOVER on ens33 to 255.255.255.255 port 67 interval 3
DHCPREQUEST of 192.168.100.60 on ens33 to 255.255.255.255 port 67
DHCPOFFER of 192.168.100.60 from 192.168.100.50
DHCPNAK from 192.168.100.15 (xid=0xef7f7d58)
DHCPACK of 192.168.100.60 from 192.168.100.50
bound to 192.168.100.60 -- renewal in 141 seconds.
```

Klientovi odpovedal Rogue DHCP server z adresy 192.168.100.50, a ponúkol mu prvú adresu z intervalu 192.168.100.60 - 192.168.100.70. Legitímny server mu adresu neponúkol, pretože žiadnu nemal k dispozícii. Komunikácia zachytená programom Wireshark:

```
199 28.033923633  0.0.0.0           255.255.255.255   DHCP    342 DHCP Discover - Transaction ID 0xef7f7d58
201 28.218242180  192.168.100.50    255.255.255.255   DHCP    316 DHCP Offer    - Transaction ID 0xef7f7d58
202 28.219824130  0.0.0.0           255.255.255.255   DHCP    342 DHCP Request  - Transaction ID 0xef7f7d58
203 28.220454893  192.168.100.15    255.255.255.255   DHCP    342 DHCP NAK      - Transaction ID 0xef7f7d58
204 29.242254867  192.168.100.50    255.255.255.255   DHCP    316 DHCP ACK      - Transaction ID 0xef7f7d58
```

Vo výpise súboru `/var/lib/dhcp/dhclient.leases` sa môžeme presvedčiť, že klient získal informácie podvrhnuté falošným serverom:

```
lease {
  interface "ens33";
  fixed-address 192.168.100.60;
  option subnet-mask 255.255.255.0;
  option routers 192.168.100.1;
  option dhcp-lease-time 300;
  option dhcp-message-type 5;
  option domain-name-servers 209.244.0.3;
  option dhcp-server-identifier 192.168.100.50;
  renew 3 2018/03/07 10:14:40;
  rebind 3 2018/03/07 10:17:02;
  expire 3 2018/03/07 10:17:40;
}
```

Klient po uplynutí 50% rezervovaného času prejde do stavu RENEWING, a pošle serveru REQUEST packet. Server mu odpovie ACK packetom a predĺži rezervovaný čas.

```
340 171.468739210 192.168.100.60   192.168.100.50   DHCP    342 DHCP Request  - Transaction ID 0xef7f7d58
341 171.578038022 192.168.100.50   192.168.100.60   DHCP    316 DHCP ACK      - Transaction ID 0xef7f7d58
```

5 Záver

V jazyku C++ boli vytvorené programy realizujúce útoky DHCP starvation a Rogue DHCP server. Testovanie prebiehalo na vituálnej sieti vytvorenej programom VMware na platforme Ubuntu 17.10, pričom neboli zistené žiadne výrazné nedostatky. Vytvorené aplikácie by mali dosahovať plnú funkcionalitu definovanú v zadaní projektu.

References

[1] R. Droms, *RFC 2131: Dynamic Host Configuration Protocol*. 1997, [Online]
https://tools.ietf.org/html/rfc2131

[2] S. Alexander, R. Droms, *RFC 2132: DHCP Options and BOOTP Vendor Extensions*. 1997, [Online]
https://tools.ietf.org/html/rfc2132

[3] P. Straatsma, *Network Takedown Part 2: Rogue DHCP Server with DHCP Starvation and Rogue Routing*. 2013, [Online]
http://www.hackandtinker.net/2013/11/27/going-rogue/

[4] Ch. Kozierok, *DHCP Message Format*. [Online]
http://www.tcpipguide.com/free/t_DHCPMessageFormat.htm

[5] *DHCP Attacks*. [Online]
https://amandeepsingh05.wordpress.com/2012/04/11/dhcp-attacks/

[6] J. Thomas, *DHCP Starvation attacks and DHCP spoofing attacks*. [Online]
http://www.omnisecu.com/ccna-security/dhcp-starvation-attacks-and-dhcp-spoofing-attacks.php