VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

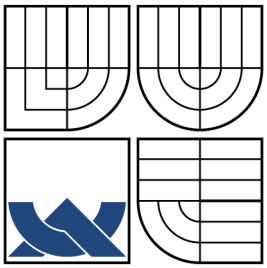
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

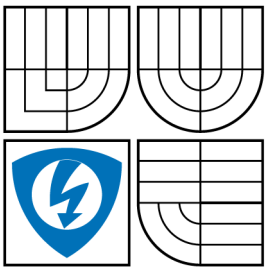
LABORATORNÍ ÚLOHA - IPv6 ÚTOKY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE Bc. LUKÁŠ GEYER
AUTHOR



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND
COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

LABORATORNÍ ÚLOHA - IPv6 ÚTOKY

LABORATORY EXERCISE - IPV6 ATTACKS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. LUKÁŠ GEYER
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. KAREL BURDA, CSc.
SUPERVISOR

BRNO 2012

OBSAH

1 LABORATORNÍ ÚLOHA

Pro laboratorní ulohu byly vybrány útoky, zneužívající hlavní mechanismy na kterých je IPv6 založen.

parasite6
dos-new-ip6
flood_router6
flood_dhcp6

Útok pomocí **parasite6** zneužívá mechanismus objevování sousedů (neighbor discovery), který je ekvivalentem protokolu ARP, kdy komunikující stanice zjišťuje linkovou adresu (MAC) stanice se kterou chce komunikovat.

Útok pomocí **dos-new-ip6** zneužívá mechanismus detekce duplicitních adres, kdy útočník zabraňuje cílové stanici přiřazení IPv6 adresy síťovému rozhraní.

Útok pomoci **flood_router6** zneužívá mechanismus autokonfigurace, zasíláním obrovského množství router advertisement (síťové parametry) ze kterých si cílová stanice vytváří IPv6 adresy z uvedených útoků je nejnebezpečnější.

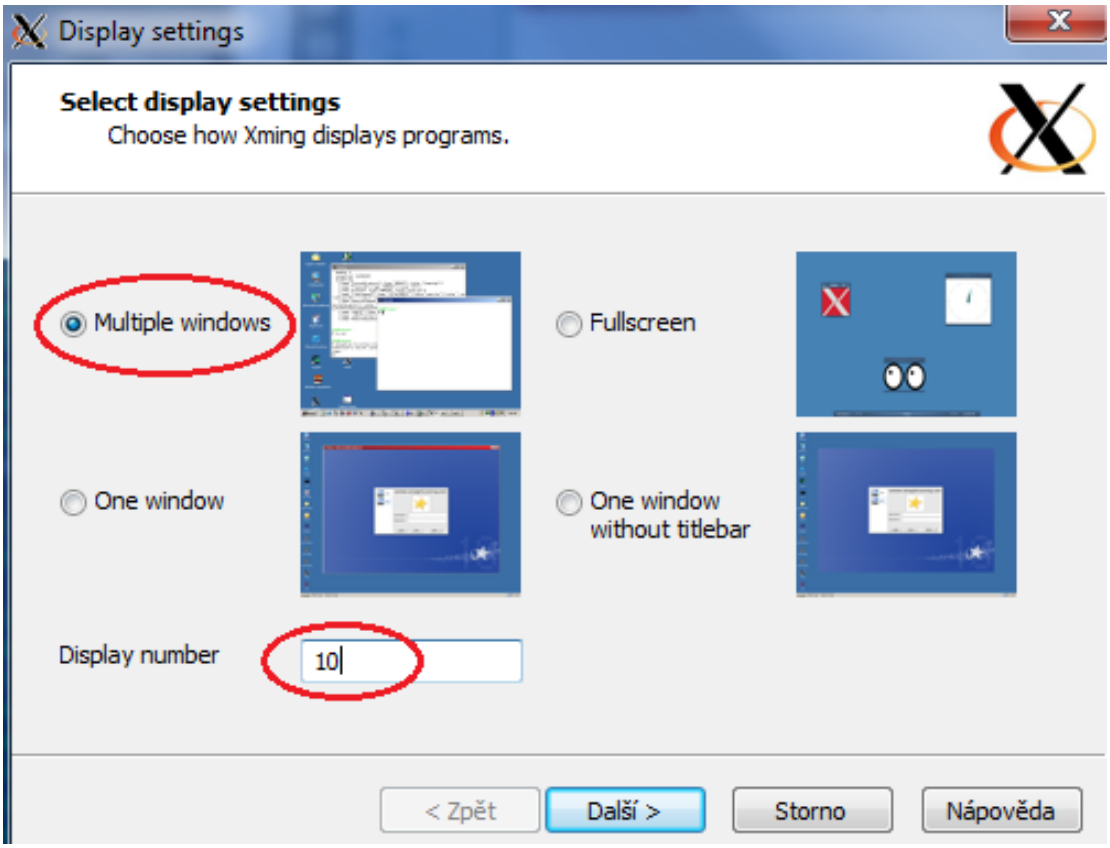
Útok na DHCPv6 poukazuje na alternativní mechanismus adresace koncových stanic. Přiložené DVD obsahuje dva obrazy s nainstalovanými operačními systémemy Debian 6, každý se dvěma systemovými účty

luke : mnsb2012
root : mnsb2012

Jednotlivé síťové utoky lze spouštět pouze s právy roota. Ostatní pomocný software zahrnující xming, putty, thc-ipv6 a VMware player jsou součástí doprovodného DVD.

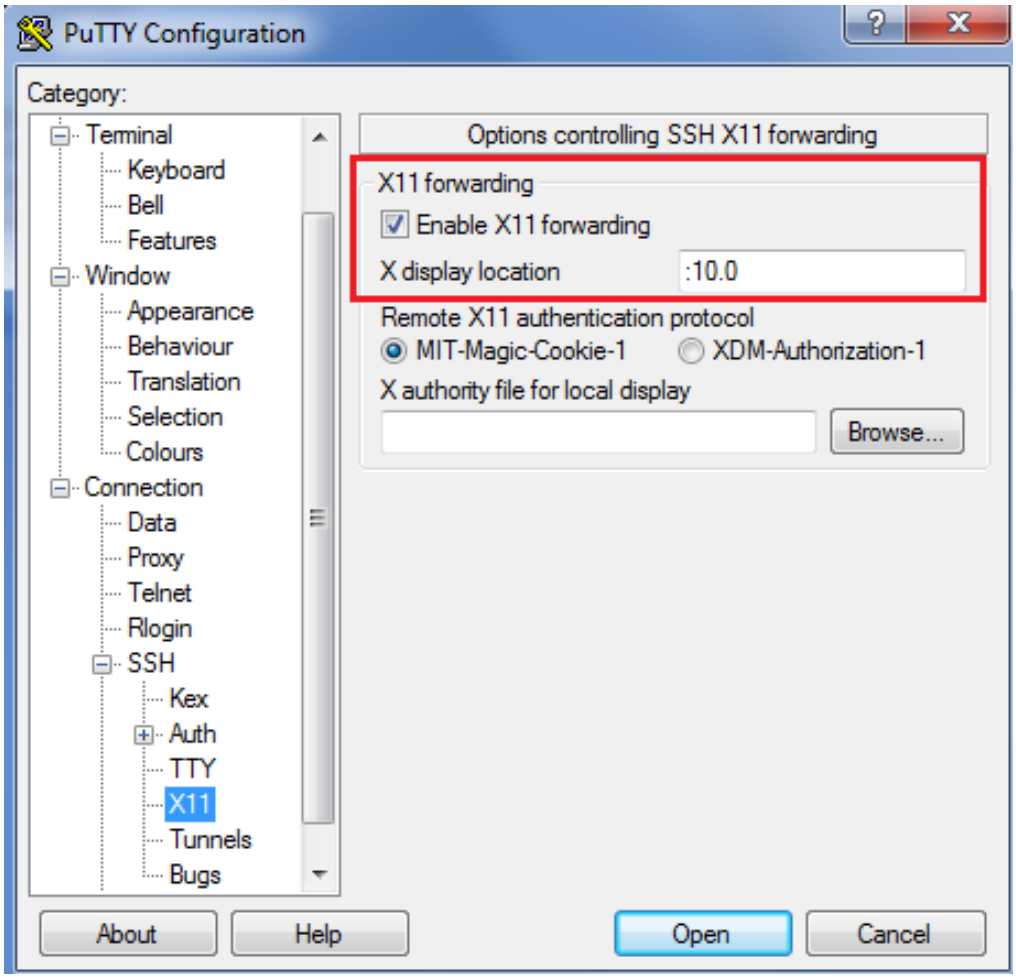
1.1 Konfigurace Xming a Putty

Součastí přiloženého DVD je Xming a Putty instalátor. Xming je opensource X Server pro Windows. Z důvodu serverové instalace jednotlivých distribucí linuxu, které neobsahují grafické rozhraní je nutné nainstalovat Xming abychom byli schopni spustit síťový analyzátor Wireshark.



Obr. 1.1: Konfigurace Xming.

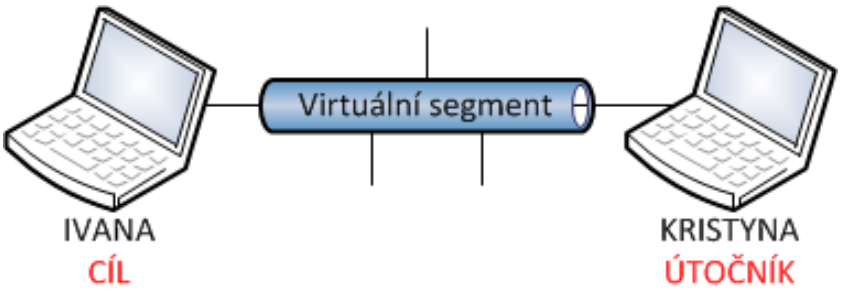
Xming se spouští přes nabídku Start na hostitelském operačním systému Windows: Start > Všechny programy > Xming > XLaunch. Abychom byli schopni spouštět aplikace jako Wireshark s grafickým rozhraní je nutné nakonfigurovat klienta Putty tak, aby vykresloval grafické rozhraní dané aplikace přes Xming.



Obr. 1.2: Konfigurace Putty.

1.2 Útoky na IPv6

Útoky demonstrované v laboratorní úloze jsou uskutečňovány pomocí balíku nástrojů thc-ipv6. Balík thc-ipv6 je součastí přiloženého DVD, ale je už nainstalovaný na obou linuxových distribucích. Jednotlivé obrazy jsou nazvány IVANA a KRISTYNA. Stroj IVANA je cíl útoků, zatímco stroj KRISTYNA funguje jako zdroj útoků.



Obr. 1.3: Laboratorní topologie.

1.2.1 Útok pomocí flood_router6

Útok pomocí **flood_router6** efektivně vyřazuje z činnosti koncové stanice 100% využitím procesoru, zasíláním obrovského množství zpráv

Název =
ICMPv6 typ =

Tyto zprávy tvoří základ autokonfigurace IPv6. Standardně je distribuce těchto zpráv obsluhováná síťovým démonem Quagga (Linux). Konfigurace tohoto démona je uložena v souboru /etc/quagga/zebra.conf a /etc/quagga/daemons. V souboru daemons je nutné povolit démona zebra a nakonfigurováním distribuovaných síťových parametrů v souboru zebra.conf . Samotné spuštění přes /etc/init.d/quagga start

1. Na stroji KRISTYNA spusťte pod uživatelem luke síťový analyzátor wireshark pomocí příkazu **wireshark &**
2. Na stroji IVANA spusťte pod uživatelem luke nástroj **top**
3. **(ROOT)** Podle syntaxe příkazu spusťte útok pomocí příkazu **flood_router6** pouze po dobu maximálně 5-10 vteřin. Pokud útok necháte běžet déle, způsobíté kompletní zamrznutí virtualizačního software i hostitelského počítače.
4. Analyzujte datový provoz generovaný tímto útokem a zatížení procesoru stroje IVANA.
   Zatížení procesoru =
   Doba trvání útoku =
   Množství vygenerovaných ICMPv6 zpráv =
   Síťové parametry
4. **(ROOT)** Na stroji IVANA pomocí přikazu **ip -6 address show dev eth0** kontrolujte množství přiřazených IPv6 adres
   Počet přiřazených IPv6 adres? =
5. **(ROOT)** Pomocí **ip6tables** nakonfigurujte správné firewallové pravidlo na stroji IVANA blokující správný typ ICMPv6 zprávy ve správném směru.

Firewallové pravidlo =

1.2.2 Útok pomocí parasite6

Útok pomocí parasite6 zneužívá tabulku sousedů v IPv6 a mechanismus objevování sousedů (ekvivalentní mechanismus protokolu ARP v IPv4). Tabulka sousedů obsahuje dvojici MAC adresa a IPv6 adresa pro všechny koncové stanice na lokálním segmentu sítě.

1. **(ROOT)** Na stroji KRISTYNA spusťte program **alive6** a podle syntaxe zjistěte aktivní klientské stanice na síti.
2. **(ROOT)** Pomocí přikazu **ip -6 neighbor show** si zobrazte tabulku sousedů na stroji KRISTYNA.
   Lokální linková adresa cíle (IVANA) =
   MAC adresa cíle (IVANA) =
3. Na stroji IVANA spusťte pod uživatelem luke síťový analyzátor wireshark pomocí příkazu **wireshark &**
4. Ze stroje KRISTYNA spusťte příkaz **ping6 -I eth0 -c 5 adresa**, kde **adresa** je linková lokální adresa stroje IVANA získaná v bodě 2.
   Ping funguje? = ANO/NE
5. **(ROOT)** Na stroji IVANA spusťte program **parasite6 eth0 aa:aa:aa:aa:aa:aa** a nechte ho běžet.
6. **(ROOT)** Na stroji KRISTYNA vymažte tabulku sousedů pomocí přikazu **ip -6 neighbor flush dev eth0** a spusťte opět program **alive6 eth0**.
7. **(ROOT)** Na stroji KRISTYNA si zobrazte tabulku sousedů a spusťte ping na stroj IVANA.
   Liší se MAC adresa v tabulce sousedů z bodu 2? = ANO/NE
   MAC adresa cíle (IVANA) =
   Funguje ping? = ANO/NE
8. Na stroji IVANA nastavte ve wiresharku filtr tak, aby zobrazoval pouze ICMPv6 zprávy pomocí příkazu **icmpv6.type==135 || icmpv6.type==136**
   typ = 135
   název ICMPv6 zprávy =
   typ = 136
   název ICMPv6 zprávy =
9. Analyzujte daný provoz.
   V IPv4 se tento ekvivalentní mechanismus nazývá? =

1.2.3 Útok pomocí dos-new-ip6

Útok pomocí **dos-new-ip6** zneužívá unikátní mechanismus detekce duplicitních adres v architektuře IPv6. Mechanismus funguje následovně. Stanice před přiřazením dané IPv6 adresy síťovému rozhraní zjišťují zda-li adresa už není využívána jinou stanicí na lokálním segmentu sítě.

1. **(ROOT)** Na stroji KRISTYNA spusťte program **alive6 eth0**
2. Ze stroje KRISTYNA spusťte příkaz **ping6 -I eth0 -c 5 adresa**, kde **adresa** je linková lokální adresa stroje IVANA.
   Ping funguje? = ANO/NE
3. Na stroji KRISTYNA spusťte pod uživatelem luke síťový analyzátor wireshark pomocí příkazu **wireshark &**
4. Na stroji KRISTYNA spusťte útok pomocí přikazu **dos-new-ip6 eth0**
5. **(ROOT)** Na stroji IVANA shoďte síťové rozhraní eth0 pomocí přikazu **ifconfig eth0 down** a opětovně ho nahoďte pomocí příkazu **ifconfig eth0 up**
6. **(ROOT)** Identifikujte problém síťového rozhraní stroje IVANA přikazem **ip -6 address show dev eth0**
   Je rozhraní eth0 na stroji IVANA ve stavu tentative dadfailed? =
7. Ze stroje KRISTYNA spusťte příkaz **ping6 -I eth0 -c 5 adresa**, kde **adresa** je linková lokální adresa stroje IVANA.
   Ping funguje? = ANO/NE
8. Na stroji KRISTYNA nastavte ve wiresharku následující filtr pomocí příkazu **icmpv6.type==135 || ipv6.src==::**
9. Analyzujte datový provoz při shození a nahození síťového rozhraní na stroji IVANA za běhu programu **dos-new-ip6** na stroji KRISTYNA a bez.

1.2.4 Útok pomocí flood_dhcp6

DHCPv6 mechanismus se na současných sítích nepoužívá protože je nahrazen autokonfigurací. V laboratorní úloze je demonstrován útok, kdy útočník přetíží daný DHCPv6 server obrovským množstvím klientských DHCPv6 požadavků. V této uloze stroj IVANA pracuje jako DHCPv6 server, zatímco stroj KRISTYNA jako DHCPv6 klient = útočník. V laboratorní úloze jsou jako DHCPv6 použity debian balíčky

wide-dhcpv6-server
wide-dhcpv6-client

Konfigurace DHCPv6 serveru je uložena v souboru /etc/wide-dhcpv6/dhcp6s.conf ve kterém je specifikován DHCPv6 pool adres, které jsou přiřazovány jednotlivým žadatelům. Spuštění DHCPv6 serveru přikazem /etc/init.d/wide-dhcpv6-server start

1. **(ROOT)** Na stroji IVANA spusťte DHCPv6 server pomocí **/etc/init.d/wide-dhcpv6-server**
2. Na stroji KRISTYNA spusťte pod uživatelem luke síťový analyzátor wireshark pomocí příkazu **wireshark &**
3. **(ROOT)** Na stroji KRISTYNA spusťte DHCPv6 klient pomocí **/etc/init.d/wide-dhcpv6-client**
4. Analyzujte datový provoz DHCPv6 mechanismu
   Množství zpráv vyměněných během DHCPv6 mechanismu? =
   Zatížení procesoru stroje IVANA? =
5. Na stroji KRISTYNA spusťte program **flood_dhcpc6 -1 -N eth0**
6. Na stroji IVANA pomocí programu **top** zobrazte zatížení procesoru
   Zatížení procesoru stroje IVANA? =