2. GYAKORLAT határidő:2017. márc. 6. NÉV: NEPTUN KÓD:

1. feladat

Építs fel egy telnet (TCP) kapcsolatot kézzel, Scapy segítségével, és küldj át egy üzenetet! Elemezd a csomagokat tcpdump segítségével!

TIPP:

1. Ismeretlen fogalmakhoz használd a google-t és wikipediat :)
2. Felveszel két gépet az GNS3-ban és összekötöd
3. Adsz nekik IP címet
4. Megnézed, hogy a fogadó gépen melyik TCP pont van nyitva (*netstat*) vagy megnyitsz egy újat (*nc*)
5. Elküldöd az egyikről Scapyvel a TCP protokoll szerinti csomagokat

+1. Mikor kiküldesz egy gépről TCP SYN-t, és arra a másik SYN ACK-al visszaválaszol, akkor a küldő gép saját IP stackje meglepődik, hogy ő nem küldött SYN-t ezért RST-vel válaszol. Így viszont a fogadó fél mindig becsukja a portot és a kapcsolat nem marad nyitva. Ezért tehát az RST üzenetet ki kell szűrni a küldő gépen egy tűzfal paranccsal. Ehhez a javasolt parancs:

iptables -t raw -A OUTPUT -p tcp --tcp-flags RST RST -j DROP

**Minta topológia** (természetesen a routert és a hostot is openwrt routerrel célszerű megvalósítani; Hogy az routerként vagy egyszerű hostként működik, az abból derül ki, hogy a routing táblájában van-e valami):



Host2

Host1

2. GYAKORLAT határidő:2017. márc. 6. NÉV: NEPTUN KÓD:

2. feladat

Hajts végre egy TCP SYN támadást egy másik gép ellen, elemezd a csomagokat tcpdump ill. netstat segítségével!

TIPP:

1. Ismeretlen fogalmakhoz használd a google-t és wikipediat :)
2. Felveszel két gépet az GNS3-ban és összekötöd
3. Adsz nekik IP címet
4. Megnézed, hogy a fogadó gépen melyik TCP pont van nyitva (*netstat*) vagy megnyitsz egy újat (*nc*)
5. Elküldöd az egyikről Scapyvel a TCP protokoll szerinti csomagokat
6. Figyelj rá, hogy az „R.” flaggek (azaz RST+ACK) a válaszban azt jelzik, hogy a port nem volt nyitva és ezért a támadás nem jött létre! A helyes válasz a SYN-re az S. (tehát az SYN+ACK).

+1. Két lehetőséged van, VAGY eleve hamis forrás IP címet adsz és akkor nincs további teendőd, VAGY meghagyod a sajátodat, de ha meghagyod a sajátodat, akkor mikor kiküldesz TCP SYN-t, és arra a másik SYN ACK-al visszaválaszol, akkor a küldő gép saját IP stackje meglepődik, hogy ő nem küldött SYN-t ezért RST-vel válaszol. Így viszont a fogadó fél mindig becsukja a portot és a kapcsolat nem marad nyitva, így a SYN támadás sem jön létre. Ezért tehát az RST üzenetet ki kell szűrni a küldő gépen egy tűzfal paranccsal. Ehhez a javasolt parancs:

iptables -t raw -A OUTPUT -p tcp --tcp-flags RST RST -j DROP

**Minta topológia** (természetesen a routert és a hostot is openwrt routerrel célszerű megvalósítani; Hogy az routerként vagy egyszerű hostként működik, az abból derül ki, hogy a routing táblájában van-e valami):



Host2

Host1

2. GYAKORLAT határidő:2017. márc. 6. NÉV: NEPTUN KÓD:

3. feladat

Hozz létre három hálózatot egy routerrel összekötve, és demonstráld egy Scapyvel generált PING üzenettel, ill. a többi gépen elindított tcpdump-al, hogy tényleg a legspecifikusabb útvonalon történik az útvonalválasztás!

TIPP:

1. Ismeretlen fogalmakhoz használd a google-t és wikipediat :)
2. Felveszel négy gépet az GNS3-ban és összekötöd
3. Adsz nekik IP címet
4. Felkonfigurálod a routert, hogy külböző specifikusságú (de az elejében teljesen megegyező) címekre más és más hostra menjen az üzenet
5. Elküldöd az egyikről (mondjuk H1) Scapyvel a PING csomagot egy IP címre
6. Megnézed, hogy végül H2 vagy H3 kapta meg a csomagot

**Minta topológia** (természetesen a routert és a hostot is openwrt routerrel célszerű megvalósítani; Hogy az routerként vagy egyszerű hostként működik, az abból derül ki, hogy a routing táblájában van-e valami):



Host2

Router

Host1

Host3

2. GYAKORLAT határidő:2017. márc. 6. NÉV: NEPTUN KÓD:

4. feladat

Forwardol-e helyi forgalmat az Openwrt router? Oldd meg egyszerű netmask segítségével (router+2 host, switchel összekötve) (ehhez tehát Scapy sem kell elvileg), és Scapyvel is (itt akár elég egy host és egy router is ha ügyes vagy)!

TIPP (egy lehetséges megoldás):

1. Ismeretlen fogalmakhoz használd a google-t és wikipediat :)
2. Felveszel két vagy három gépet az GNS3-ban és összekötöd
3. Adsz nekik IP címet (mindkét host ugyanazon az alhálón kell legyen)
4. Elküldesz az egyik hostról Scapyvel egy olyan PING-et, ami a ROUTER MAC címét használja, de a host2 IP címére megy. Vajon hajlandó a router továbbküldeni, vagy visszautasítja és jelzi, hogy ezt a host1-nek közvetlenül a host2 MAC címére kellett volna elküldeni?

**Minta topológia** (természetesen a routert és a hostot is openwrt routerrel célszerű megvalósítani; Hogy az routerként vagy egyszerű hostként működik, az abból derül ki, hogy a routing táblájában van-e valami):

http://www.takistmr.com/wp-content/uploads/2011/07/cisco-switch-icon.png

Switch

Host1

Host2

Router

2. GYAKORLAT határidő:2017. márc. 6. NÉV: NEPTUN KÓD:

5. feladat

Állíts össze egy TCP portscannert 1-től 2000-ig, és mutatsd meg, mely portok voltak nyitva. Ezt netstat-al is ellenőrizd!

TIPP:

1. Ismeretlen fogalmakhoz használd a google-t és wikipediat :)
2. Felveszel két gépet az GNS3-ban és összekötöd
3. Adsz nekik IP címet
4. Elküldesz az egyikről Scapyvel, pl. egy for ciklussal, egy csomó portnyitást a TCP protokoll szerint. A válaszból kiderül majd, hogy TCP SYN+ACK (S.) vagy TCP RST+ACK (R.))., azaz, hogy nyitott vagy nem. Az „R.” flaggek (azaz RST+ACK) a válaszban azt jelzik, hogy a port nem volt nyitva! Ha a port nyitva van a helyes válasz a SYN-re az S. (tehát az SYN+ACK). Egyébként a 3-way handshake-et a küldő ACK válasza zárná le, de persze ez most nem fog megtörténni!

+1. A Scapy “sr” parancsával, esetleg annak a dport paraméterénél tartomány megadásával egyszerűsíthető a feladat...

**Minta topológia** (természetesen a routert és a hostot is openwrt routerrel célszerű megvalósítani; Hogy az routerként vagy egyszerű hostként működik, az abból derül ki, hogy a routing táblájában van-e valami):



Host2

Host1

2. GYAKORLAT határidő:2017. márc. 6. NÉV: NEPTUN KÓD:

6. feladat

Szimulálj véletlenszerű intervallumokban generált ARP-ket Scapy-vel állítsd le és ez alapján generálj egy tetszőleges üzenetet Scapy-vel, amelyben már tudod a MAC címet!

TIPP:

1. Ismeretlen fogalmakhoz használd a google-t és wikipediat :)
2. Felveszel két gépet az GNS3-ban és összekötöd
3. Adsz nekik IP címet
4. Elküldöd az egyikről Scapyvel az ARP protokoll szerinti csomagokat, leállítod
5. A választ felhasználva küldesz pl. egy PING üzenetet

+1. A Scapy “sr1” parancsával, ill. annak inter és loop paraméterével egyszerűsíthető a feladat...

**Minta topológia** (természetesen a routert és a hostot is openwrt routerrel célszerű megvalósítani; Hogy az routerként vagy egyszerű hostként működik, az abból derül ki, hogy a routing táblájában van-e valami):



Host2

Host1