DDOS Sandbox

Vitajte! V tejto hre sa zahráte na bezpečnostného analytika, ktorého úlohou je vylepšiť bezpečnostnú konfiguráciu siete. Cieľom výslednej konfigurácie je zabránenie zamietnutia služby vyvolanej z DDOS útoku. Počas prebiehajúceho útoku musí byť stránka ddos.com dostupná pre klienta. K dispozícii máte administrátorove zariadenie, z ktorého sa môžete pripojiť na apache2 server alebo dns server, kde budete meniť bezpečnostné nastavenia. V tejto hre sa naučíte detekovať typ prebiehajúceho ddos útoku, filtrovať pakety pomocou nastavení firewallu a konfigurovať moduly apache2 serveru.

Inštalácia hry:

Pred spustením hry si nainštalujte Cyber Sanbox Creator podľa nasledujúceho návodu: Installation · Wiki · MUNI-KYPO-CSC / cyber-sandbox-creator · GitLab. Nasledujúce príkazy spúšťajte z príkazového riadku otvorenom v priečinku tohto projektu „sandbox“.

Hru zapnite pomocou:

manage-sandbox build

Hru ukončíte pomocou:

manage-sandbox destroy

Prístup na zariadenia:

Po spustení hry by sa vám malo otvoriť okno s administrátorovým zariadením. Do tohto zariadenia sa musíte prihlásiť dvakrát po sebe s nasledujúcimi prihlasovacími údajmi:

Meno: admin Heslo: admin

V tejto hre budete pracovať len na administrátorovom zariadení. Na to aby ste mohli zmeniť bezpečnostnú konfiguráciu apache2 servera a DNS servera budete sa musieť pripojiť pomocou protokolu ssh na tieto zariadenia. Prihlásenie máte umožnené z administrátorovho počítača bez zadania hesla.

Na pripojenie na apache2 server použite tento príkaz:

ssh remote-admin@server

Na pripojenie na DNS server použite tento príkaz:

ssh remote-admin@dns

Na pripojenie na serverový router použite tento príkaz:

ssh remote-admin@server-router

Ovládanie DDOS útokov:

Na spustenie alebo zastavenie DDOS útokov použite skript „ddos-master.sh“, ktorý sa nachádza na administrátorovom zariadení na ceste /home/admin. Pomocou tohto skriptu môžete otestovať prístup klienta na server pomocou pingov na overenie spomalenia pripojenia a pomocou w3m na overenie odmietnutia služby.

DDOS útoky:

Spustenie TCP SYN flood DDOS útoku: *„. /ddos-master.sh tcp-syn-flood“*

Spustenie TCP ACK flood DDOS útoku: *„. /ddos-master.sh tcp-ack-flood“*

Spustenie UDP flood DDOS útoku: *„. /ddos-master.sh udp-flood“*

Spustenie ICMP flood DDOS útoku: *„. /ddos-master.sh icmp-flood“*

Spustenie DNS flood DDOS útoku: *“. /ddos-master.sh dns-flood“*

Spustenie DNS reflekčno-amplifikačného DDOS útoku: *„. /ddos-master.sh dns-reflection“*

Spustenie low and slow DDOS útoku: *„. /ddos-master.sh slowloris“*

Spustenie náhodného DDOS útoku: *„. /ddos-master.sh random“*

Zastavenie všetkých DDOS útokov: *„./ddos-master.sh kill“*

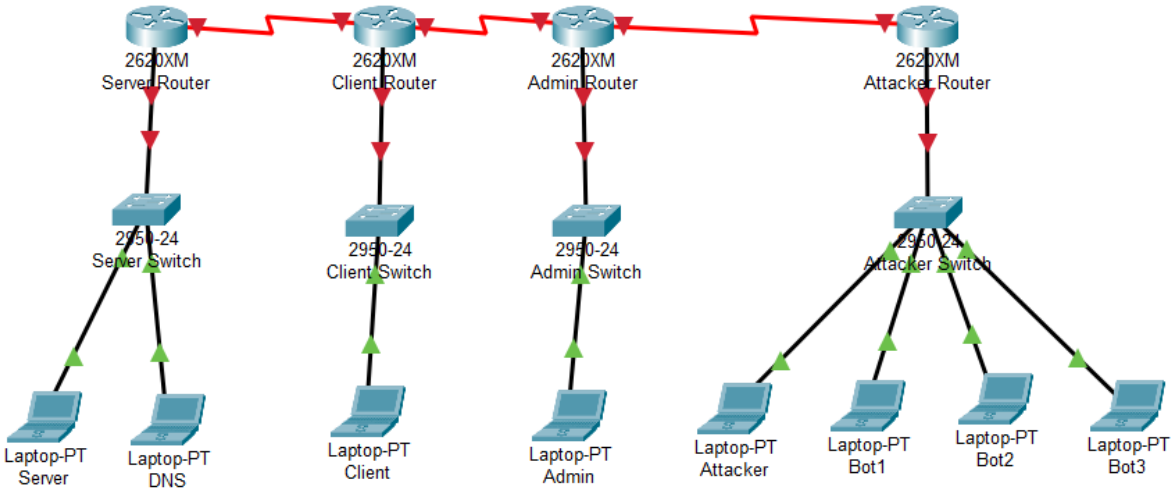
Pridaním prípony „-unspoofed“ spustíte DDOS útok bez použitia IP spoofingu. Napr.: *„./ddos-master.sh tcp-syn-flood-unspoofed“. Útok slowloris funguje len bez IP spoofingu a reflekčno-amplifikačný DDOS útok bez IP spoofingu nemôže fungovať.*

Testy pripojenia klienta:

Overenie odmietnutia služby servera pre klienta: *„./ddos-master.sh w3m-test“*

Overenie rýchlosti spojenia klienta ku serveru: *„./ddos-master.sh ping-test“*

Opis siete:



Dôležité zariadenia:

admin: Z tohto zariadenia môžete hrať hru pod účtom „admin“. Nachádza sa tu skript „ddos-master.sh“ pomocou ktorého môžeme oznámiť útočníkovi aby spustil alebo zastavil DDOS útok. Tiež môžeme pomocou tohto skriptu otestovať prístup klienta ku serveru. Admin ma vzdialený prístup na zariadenia „server“ a „DNS“.

server: Na toto zariadenie sa môže hráč vzdialene pripojiť pomocou účtu „remote-admin“. Na tomto zariadení sa nachádza apache2 server „ddos.com“.

DNS: Na toto zariadenie sa môže hráč vzdialene pripojiť pomocou účtu „remote-admin“. Na tomto zariadení sa nachádza DNS, zabezpečený pomocou služby bind9.

server-router: Na toto zariadenie sa môže hráč vzdialene pripojiť pomocou účtu „remote-admin“. Slúži ako router pre zariadenia „Server“ a „DNS“. Je tu nainštalovaný nástroj tshark, pomocou ktorého môžeme sledovať pakety v sieti.

client: Toto zariadenie slúži na testovanie prístupu ku serveru. Je tu nainštalovaný nástroj w3m na otvorenie stránky v príkazovom riadku.

Študijné materiály:

Na vypracovanie úloh budete potrebovať používať určité príkazy. Ich používanie si môžete naštudovať v nasledujúcich manuálov:

tshark

iptables

reverse path forwarding

Na vypracovanie úloh budete potrebovať nakonfigurovať určité moduly pre apache2. Ich konfiguráciu si môžete naštudovať v nasledujúcich manuálov:

apache2 mod security

apache2 mod qos

apache2 mod evasive

apache2 mod reqtimeout

Dotazník:

Tento dotazník slúži na porovnanie vašich vedomostí pred a po vyplnení nasledujúcich úloh. Ak neviete odpoveď na niektorú z nasledujúcich otázok, tak napíšte čo si myslíte alebo napíšte, že odpoveď neviete. Odpovede na tieto otázky napíšte do súboru „alias_dotaznik1.txt“ („alias“ nahraďte za svoje priezvisko/alias) ak ho vypĺňate prvýkrát pred vypracovaním úloh. Ak dotazník robíte druhýkrát po vypracovaní úloh, tak svoje odpovede zapíšte do súboru „alias_dotazník2.txt“.

1. Čo je DDOS útok?
2. Vymenujte konkrétne typy DDOS útokov, ktoré poznáte.
3. Čo je IP spoofing a ako sa využíva pri DDOS útokoch?
4. Čo je reflekcia a ako sa využíva pri DDOS útokoch?
5. Čo je amplifikácia a ako sa využíva pri DDOS útokoch?
6. Ako sa dá zabrániť IP spoofingu?
7. Akými metódami sa môže server chrániť pred DDOS útokmi?
8. Opíšte DDOS flood útoky.
9. Opíšte low and slow DDOS útoky.

Úlohy:

Odpovede na tieto otázky napíšte do súboru „alias_ulohy.txt“. Ak neviete aký príkaz použiť, pomôžte si vyhľadávaním na internete. Ak niektorú úlohu neviete vyriešiť, tak aspoň napíšte čo ste sa snažili spraviť.

Pre urýchlenie inštalácie aplikácií na DNS serveri alebo apache serveru použite nasledujúci príkaz:
sudo wondershaper clear enp0s8
Po dokončení inštalácie musíte obnoviť reštrikciu siete týmto príkazom:
Sudo wondershaper enp0s8 1000 1000

1. Spustite DDOS útok z administrátorovho zariadenia pomocou príkazu – „./ddos-master.sh uknown-ddos“. Počas prebiehajúceho DDOS útoku sa skúste pripojiť na stránku „ddos.com“. Zistite aký typ flood DDOS útoku sa spustil a zistite IP adresy útočiacich zariadení. (*nápoveda: pripojte sa na server-router a sledujte trafiku na rozhraní enp0s8*)
2. Upravte nastavenia firewallu na serverovom routeri tak, aby sa zablokovali všetky pakety, ktoré prichádzajú od útočiacich zariadení. Po upravení firewallu (*nápoveda:* n*a serverovom routeri musíte použiť reťaz pravidiel FORWARD*)zapnite znova DDOS útok pomocou príkazu - „./ddos-master.sh unknown-ddos“. Môžete sa teraz pripojiť na stránku „ddos.com“? Ak áno, úlohu ste úspešne splnili.
3. Spustite iný DDOS útok pomocou príkazu - „./ddos-master.sh unknown-ddos-2“. Skúste sa znova dostať na stránku „ddos.com“. Zistite aký DDOS útok sa spustil. Ak ste sa nemohli dostať na stránku vysvetlite prečo.
4. Nastavte serverový router tak, aby sa na sieťovom rozhraní striktne kontrolovala zdrojová adresa (*nápoveda: rp_filter*). Funkčnosť pravidlo overte spustením „./ddos-master.sh unknown-ddos-2“.
5. Zrušte bezpečnostnú konfiguráciu z úlohy 2. Nastavte na firewalle serverového routera pravidlo, ktoré limituje počet spojení od jedného zariadenia na TCP port 80 pre trafiku smerujúcu na server. Funkčnosť tohto pravidla overte pomocou príkazu „./ddos-master.sh tcp-syn-flood-unspoofed“
6. Spustite DDOS útok pomocou príkazu – „./ddos-master.sh unknown-ddos-3“. Skúste sa dostať na stránku „ddos.com“. Môžete sa na stránku dostať? Skúste sa na stránku dostať znova zadaním IP adresy „10.10.10.10“. Aký DDOS útok prebieha? Opíšte ako tento útok funguje.
7. Zrušte bezpečnostnú konfiguráciu z úlohy 4. Spustite DDOS útok pomocou príkazu – „./ddos-master.sh dns-reflection“ a otestujte dostupnosť stránky „ddos.com“. Pozrite si aká sieťová trafika prebieha na serverovom routeri. Upravte nastavenia firewallu na serverovom routeri tak, aby sa DNS query nemohli reflektovať na apache2 server. Vysvetlite ako funguje tento útok a ako dosiahol amplifikáciu.
8. Zrušte bezpečnostnú konfiguráciu z úlohy 5. Spustite low nad slow DDOS útok na server pomocou príkazu - „./ddos-master.sh slowloris“ a otestujte dostupnosť stránky „ddos.com“. Nájdite a nainštalujte vhodný modul pre apache2 server a nakonfigurujte ho tak, aby ste zabránili DDOS útoku. Úspešnosť tejto konfigurácie si môžete overiť navštívením stránky „ddos.com“. (nápoveda: napr. mod_qos, mod_reqtimeout, mod_security a mod_evasive) Vysvetlite ako tento útok funguje.

Po vypracovaní týchto úloh vyplňte znova dotazník na predošlej strane.