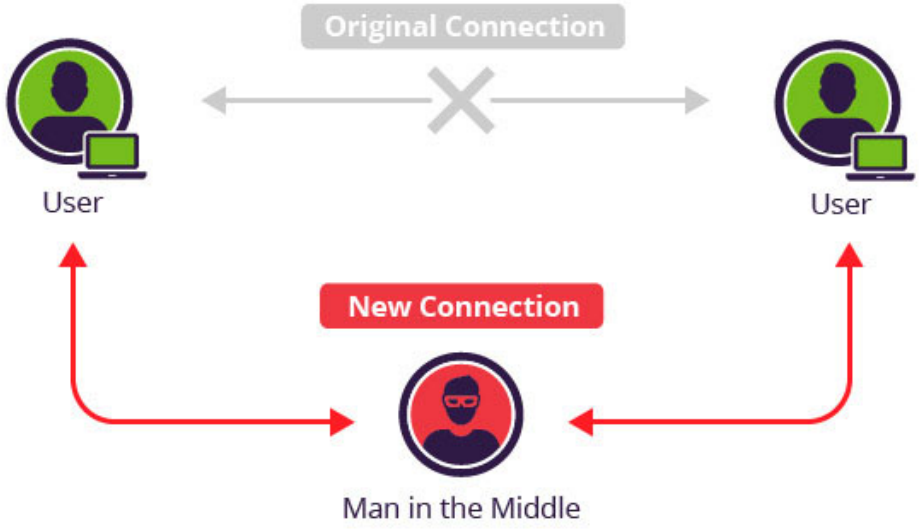
Втора лабораториска вежба по предметот “Мрежна безбедност”

Компјутерски и мрежни ранливости

“Men in the middle” напад

Овој напад се изведува така што напаѓачот (men in the middle), се поставува како посредник во комуникацискатa врска помеѓу две машини кои не знаат дека не се директно поврзани помеѓу себе.
Во оваа ситуација напаѓачот има прилика да го преслушува сообраќајот, да вметнува или изменува податоци.
Комуникацијата помеѓу уредите знаеме дека на физичко ниво се одвива преку испраќање на секвенци од броеви во одреден временски такт. Кога се шпионира сообраќајот, хакерот може да ги следи тие секвенци и да ги предвиди наредните секвенци кои следуваат и во оваа прилика тој фактички ја презема конекцијата и може да ја менува.
Најдобра заштита од ваков тип на напади е енкриптирање на сообраќајот.

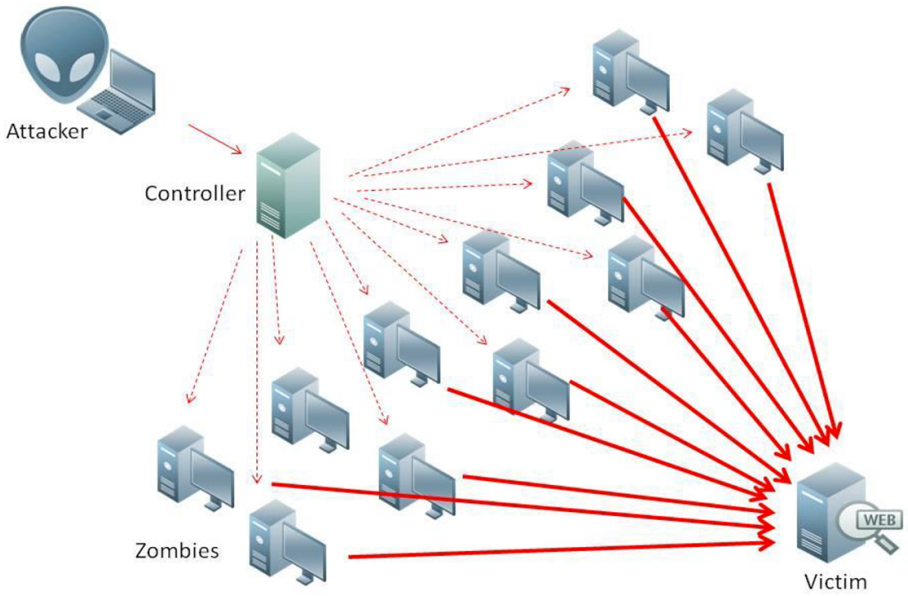


DoS – Denial of Service

Denial of Service е една од најпознатите техники за хакирање. Оваа техника како концепт има многу варијанти и има за цел да уништи сајт или сервер така што тој сајт или сервер ќе го бомбардира со огромно количество на сообраќај така што серверот нема да биде способен да ги обработи сите побарувања во реално време и ќе колабира т.е. нема повеќе да функционира.

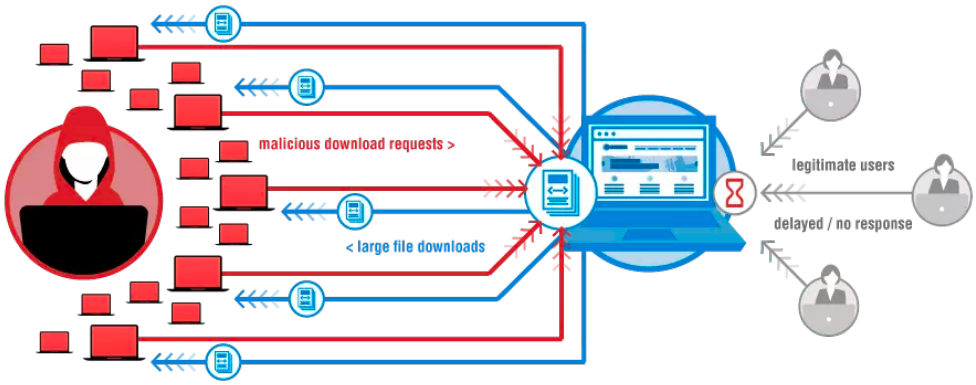
DDoS (Distributed Denial of Service)

Оваа изведба на DoS напад е наречена дистрибуирана (distributed) поради тоа што нападите се извршуваат од многу различни уреди кои може да бидат од било каде во светот.



HTTP Flood

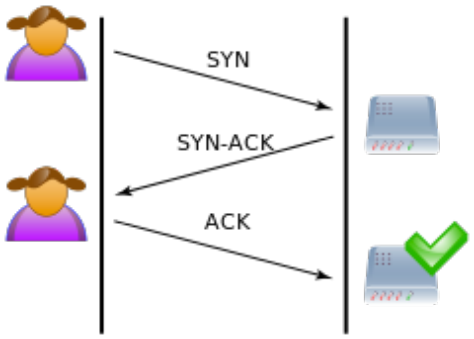
HTTP Flood е уште една варијанта на DoS напад која е многу тешко за откривање. Кога се комуницира со веб апликација или сервер, најчесто комуникацијата се одвива преку http протоколот. Со GET методот се испраќа барање до серверот за да ни испрати некаква содржина (веб страна, слика, документ ...) со што се одземаат дел од ресурсите со кои располага серверот. Идејата е да се испратат огромен број на вакви побарувања до серверот кои навидум се коректни како и од сите останати корисници, и таргетираат побарувања на големи фајлови за даунлоад кои одземаат максимум ресурси.



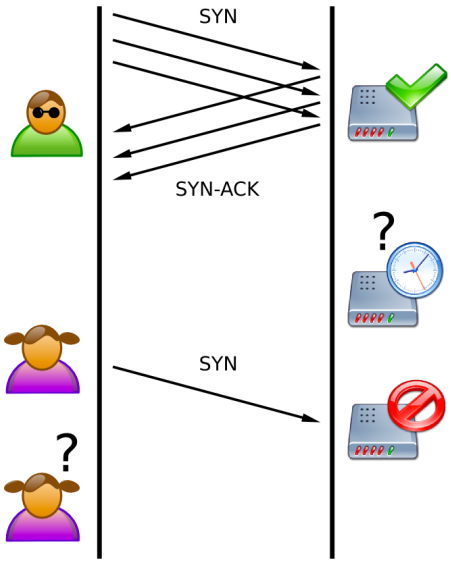
SYN food

Концептот three-way-handshake на TCP протоколот во нормални услови се одвива во 3 чекори:

1. Клиентот испраќа барање до серверот со кој сака да оствари комуникација со SYN порака
2. Серверот одговара со SYN-ACK (acknowledge) порака назад до клиентот
3. Клиентот повторно му враќа ACK порака на серверот и врската е воспоставена

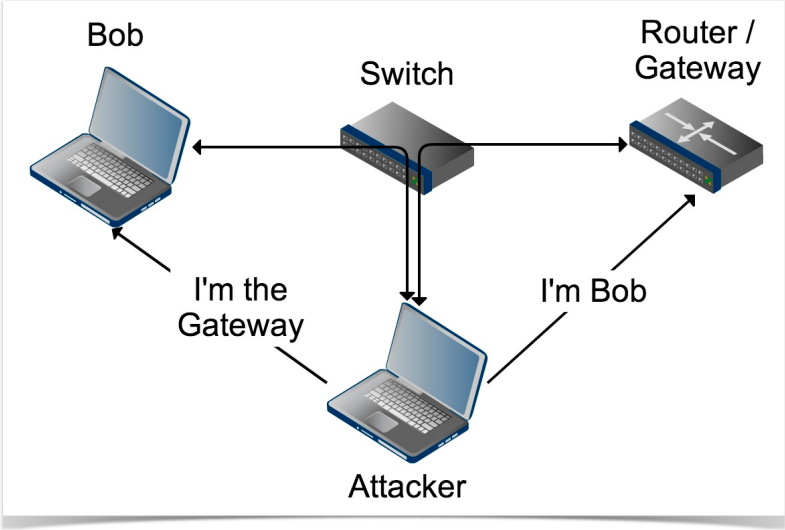


Идејата на SYN food нападот е напаѓачот да испрати огромен број на SYN пораки до серверот за воспоставување на врска и никогаш да не му одговори со ACK порака или пак, изворната адреса во пакетот ќе ја постави на друга случајна IP адреса од која никогаш нема да се врати ACK . Така серверот ќе чека извесно време за ACK а во меѓувреме се трупаат нови SYN пораки и доаѓа до колабирање на системот и не овозможување вистинските корисници да бидат опслужени.



ARP Poisoning

ARP (Address Resolution Protocol) се користи во мрежата за да се дознае MAC адресата на корисникот со одредена IP адреса.
Најпрво напаѓачот се приклучува на истата/локална мрежа на која се наоѓа и жртвата. Следно, напаѓачот испраќа ARP порака до си сите уреди на мрежата дека има промени во ARP табелата и во неа ги има променето податоците така да кој и да сака да оствари комуникација со жртвата, сообраќајот ќе се препрати до напаѓачот. По авотоматизам, ARP табелата ќе биде споделена помеѓу уредите во мрежата и нападот технички е започнат. Со овој напад, напаѓачот всушност станува “man in the middle”



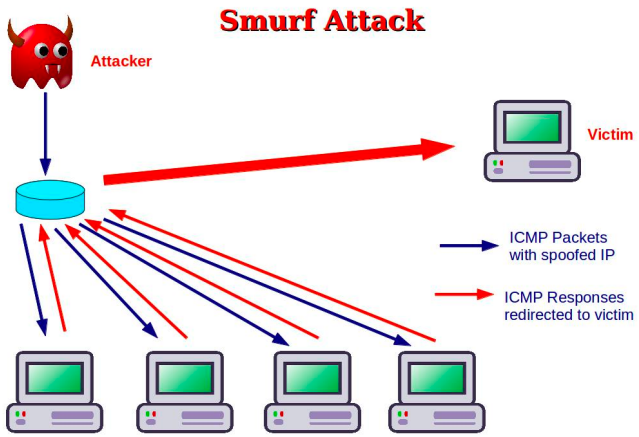
Brute force напад

Brute force нападите (напади со груба сила), е техника за напад која има за цел да погоди пасворд или пин преку обиди за внесување на сите можни комбинации (нумерички, алфанумерички или знаковни) се додека не ја погоди вистинската комбинација. Постојат огромен број на софтвери кои го автоматизираат овој процес преку внесување на бројот на карактери на пасвордот/пинот, постоење на одредени карактери во него, дали е составен од броеви, знаци, букви или нивна комбинација, го намалуваат потребното време да се најде точната комбинација.

Smurf attack

Ping пораката за проверка дали има конекција до одредена IP адреса се врши преку Internet Control Message Protocol (ICMP). Напаѓачот испраќа лажна ping порака со изворна IP адреса на жртвата и дестинациска IP адреса на default gateway за да ја преплави

мрежата и сите уреди да одговорат на барањето и да испратат порака назад до нападнатиот уред. Доколку бројот на уреди во мрежата е доволно голем и одзивот на барањето е голем, нападнатиот уред ќе биде преплавен со сообраќај што ќе дојде до забавување или целосно оневозможување за користење.



Trojan horse

Многу често хакерите подметнуваат злонамерен софтвер во системите. Тројанците се софтвер кој откако ќе се инсталира на машината може да краде и снима податоци или да ја преземе контролата над машината. Најчесто се испраќаат по e-mail, лажен линк за даунлоад и сл., преку кој се мами корисникот несвесно да ги инсталира на компјутерот.

Изработи:
Никола Танев 141140