Network Security

Assignment 5, Wednesday 20 May 2020, version 1.0

Handing in your answers: Submission via Brightspace (https://brightspace.ru.nl)

Deadline: Wednesday 27 May, 23:59:59 (midnight)

Teachers. Please email *all* of us if there is a problem.

- Pol Van Aubel <pol.vanaubel@cs.ru.nl>
- Daan Sprenkels <d.sprenkels@cs.ru.nl>

In this assignment you will be using the following tools:

- netcat: https://nc110.sourceforge.io/[1]
- openvpn: https://openvpn.net/index.php/open-source/documentation.html

Again, do not compile these programs from source, but install them using your distribution's package manager.

Please turn in all your work in plain text files (program source files are also plain text), unless specified otherwise. If you prefer a document with formatting for whatever reason, like including images, use the PDF format to turn in your work (most editors allow you to export to PDF). Note that it's okay to include images separately and then refer to them from within the text files.

[1] You will not find any useful information here. Use the man page instead.

DNS amplification precautions

1. Create a file called `exercise1` and write your answers to that file.

   Suppose you are the administrator of a network. Imagine the gateway from the LAN to the internet is *non-NAT'ing*. You want to prevent hosts, from inside the LAN, from being able to execute DNS amplification attacks. The LAN network is `203.0.113.0/24`, the gateway's internal IP address is `203.0.113.1`, and its external IP address is `198.51.100.78`.

   (a) What firewall measure should prevent DNS amplification attacks from originating from your network, *without* impeding normal operation of the network?

   (b) Write an iptables configuration that implements this measure.

DNS query randomization

2. Create a file called `exercise2` and write your answers to that file.

   Assume you're an attacker who wants to trick a DNS cache into believing your server is actually hosting proctorio.com. You try to race a legitimate DNS server to provide the answer faster, but you are *not* a MITM between the DNS cache and the DNS server.

   (a) How would you ensure that you can predict the queries that the cache is going to produce, and how would you ensure that your answers will be accepted (i.e. pass the bailiwick check)? Describe the setup and/or process.

   QID randomization and port randomization are (somewhat) effective countermeasures against cache poisoning.

   (b) If you craft a single blind response, to a single DNS query, what is the probability that you guess right if the DNS cache is only using QID randomization in its queries?

   (c) What is the probability if the cache is also using source port randomization?

   Imagine that on top of that, these DNS servers also deploy 0x20 randomization (see slides, the random capital letters in the query).

   (d) What is the probability now that you will guess right on a query for the proctorio.com host?

   (e) Describe an attack that would allow you to get a good success rate, even though your odds of guessing a single response correctly are low. Explain the idea behind the attack, and the way it would be performed. Exact calculations of probability are not required.

   Until now, we assumed the attacker cannot see the DNS queries. The countermeasures we mentioned are designed with that assumption as well.

   (f) Explain, in your own words, why all these countermeasures are less effective against a DNS attack performed by a passive MitM attacker.

   (g) Explain, in your own words, why all these countermeasures do not work against a DNS attack performed by an active MitM attacker.

Firewalls and UDP “connections”

3. Create a file called exercise3 and write your answers to that file.

   (a) The firewall configuration you made in assignment 4, exercise 1a, should still allow DNS conversations initiated by an outgoing DNS query, but block unsolicited incoming traffic. However, DNS usually runs over UDP and UDP is a connectionless protocol. Try to explain how the firewall still knows that it should allow this DNS traffic. Feel free to consult iptables documentation for this.

sandor.cs.ru.nl and ygritte.cs.ru.nl want to set up a UDP peer-to-peer connection. However, they are both behind a (different) firewall that does not allow incoming connections. (Just as in exercise 1, there is no NAT involved.) They are smart, however, so they look up what UDP hole punching is.

   (b) How can you set up a peer-to-peer UDP session between two different hosts, both behind a firewall that blocks incoming connections? For each peer, list the netcat command(s) that should achieve this goal.

OpenVPN

4. Create a folder called exercise4 to hold your answers and configuration files.

   CNCZ provides an OpenVPN-based Science VPN, which you may find useful at some point. Instructions for this are at http://wiki.science.ru.nl/cncz/index.php?title=Vpn&setlang=en#OpenVPN_.5Bvoor.5D.5Bfor.5D_Linux_.26_MacOS.

   (a) See if you can get this to work with your Science account. If you are unable to do this within 30 minutes, skip to the next exercise and come back if you have time left over.

   (b) Look up in the OpenVPN man page (man openvpn) what each line of the configuration file means. For easy searching, append “--” to the first word on the line. So searching for “dev” becomes “--dev”.

   (c) Perform traceroutes (traceroute) to brightspace.ru.nl, www.google.com, www.cs.ru.nl, and to the VPN server itself, with and without the VPN running. Paste the commands you used and their output to a file. Look at the routing table (ip route show), and paste it as well.

   (d) Explain the differences between the traceroutes, paying special attention to the one to the VPN server itself.

   (e) Explain why it is not straightforward to run other services on the OpenVPN server and contact them via the VPN tunnel. Can you think of a solution for this problem?

5. Place the directory exercise1, exercise2, exercise3, exercise4. and all its contents in a folder called netsec-assignment5-SNR1-SNR2. Replace SNR1 and SNR2 by your respective student numbers, and accomodate for extra / fewer student numbers.

   Make a tar.gz archive of the whole directory netsec-assignment5-SNR1-SNR2 and submit this archive in Brightspace.