Computer Networks - part 2

Lab: Extra exercises

P. Geens – R. Swennen

- Create a oneliner which shows the amount of currently revoked certificates in the Terena SSL CA revocation list. Do not create temporary files. The CRL can be found at http://crl.tcs.terena.org/TERENASSLCA.crl.

  Tip: '-' (no quotes) specified as a filename means STDOUT. The answer should be more or less 4960

- Your very curious it-enabled grandmother likes to see how you solved some of the lab exercises on debbie. She gave you her public key id_rsa.pub. Which command allows her to login to your ssh account without entering credentials?

- Create a onliner which sends one icmp echo packet to 127.0.0.1 for every pdf downloaded from the following folder: /documenten/echo/08-09/. The required info can be found in the apache logfile: apache_google.log. The output from your command should look like this (nothing else):

```
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.035 ms
...
64 bytes from 127.0.0.1: icmp_seq=29 ttl=64 time=0.057 ms
```

- Create a oneliner which lists the top 3 most used passwords in the ftp brute force attack captured in ftp_bruteforce.pcap. Use a suitable sniffer filter which only displays whats really needed to get the output below.

```
maggie
harley
donald
```

- Perform a network capture while surfing to http://debbie.vlan77.be/nw2/test.html . Write a wireshark filter that will show only HTTP POST requests to the server debbie. Filter out any other traffic, also from other servers or clients.

- Try to find out which TCP ports are open on debbie without being logged in to the server itself. Use your virtual machine. Try to determine which services are running on these ports, but don't scan too fast because the allmighty KHLeuven firewall might detect that you are up to something evil and block your IP or even kick you off the network.

- On server debbie, use the list of logged in users to print only the username that has been logged in to the server for the longest time. (Hint: use “perl -ne”)

- It is always a good idea to make (secure) backups of your data and store them on a different location. Use 'tar' to compress the contents of your entire home directory on debbie, encrypt the result with openssl and send the output file to your windows computer. Choose a strong encryption algorithm. (Use 2 one-liners, one on debbie and one on windows)

- On server debbie, list all TCP ports on which a daemon is currently listening for connections. Only show the ports you can connect to using IPv4. Also hide all port numbers that have one or more repeating digits.

- An ftp brute force attack was captured using wireshark in the following file: ftp_bruteforce.pcap. You want to know if the attack was successful, i.e. if the attacker found a working username and password combination. Use a suitable tshark oneliner to display all possible successful login attempts in the following format:

  USER bob
  PASS verysecure

  Tip: step 1: use tshark to display the tcp destination port used by the server to inform the client the login was successful.
  step 2: substitute the above oneliner as a variable in a new tshark oneliner which displays the relevant client session.

  If you're familiar with tshark/wireshark mate scripts, this may also be used.

- Companies like Google and Microsoft make heavily use of the X.509 subjectAltName extension. KHLeuven also uses this extension to add an alternative name *.khleuven.be to the common name (khleuven.be) of the cerificate. Create a oneliner which calculates the amount of DNS Subject Alternate Names used in the SSL certificate of gmail.be.

- Create a oneliner which lists all palindromes with exactly 4 letters in a dictionary.

- Show the permissions of only your homedirectory, without using any pipes. The solution must be generic: It should work from any location and without specifying your exact username.

- Bob needs to send a text file through an encrypted tunnel to Alice. Both already agreed on a shared secret 'mysecret' using the Diffie Hellman algorithm. Alice wants to display the contents of the file directly on her screen in stead of storing it locally and then opening it. Use a suitable encryption algorithm. The data is sent over a medium which only allows ASCII text.

  Alice is logged in on debbie and Bob on the virtual machine.

- Some subdirectory of /tmp contains a bunch of movies. However their extension is wrong. The extension should be .avi in stead of .jpg. Copy these files to your homedirectory and correct their extensions in one line. (tip: basename)

- Create a onliner which relies on the command ping to do a fully automatic icmp traceroute. Limit the amount of hops to 10. The output should look like this:

```
193.191.187.62
khleuven-vrrp.access.leuven.belnet.net
...
209.85.250.163
wi-in-f94.1e100.net
```

- The VoIP lab, one of the cnw2 labs amazed you so much you immediately bought some cheap VoIP phones off Ebay for further experimenting. When the phones arrived it seemed they had a pin code set by their previous owner, making it impossible to configure them. A quick nmap scan revealed that the phone was listening on tcp port 80. By pointing your browser to the phones ip address you were prompted for a username and password (pincode). The accompanying docs said the default username was admin.

  A simulated phone is runnning at http://debbie.vlan77.be/nw2/phonie. Create a oneliner to bruteforce the pincode. Tips: pincode range: 8000-9000

- You just received your pem encoded certificate from you CA. Now you have 2 files: cert.pem en cert.key. Use the command `chmod` to set the appropriate permissions.

- Create a linux CLI oneliner to extract the DNS servers and their destination ports of the DNS replies in the sip_dump.pcap file.

- Create a linux CLI oneliner to decode the following string “TGludXggUlVMRVM=“. (the l is a minor L)

- What linux command with options should be used to perform a scan to the server debbie.vlan77.be with the following requirements:

  Use only the IP address of the server
  Don’t randomize the scanned ports
  List only open TCP ports

- Create a CLI oneliner using openssl to retrieve the certificate of the server facebook.com and to display only it’s fingerprint and public key.

- As a web server administrator you have been asked to give your manager a linux CLI oneliner to extract the 5 IP adresses that contacted the web server the most. The apache log is located in /home/log. Create a correct oneliner. The output should look something like this: (count IPs)

  8000 10.10.10.10
  ...
  82 81.30.45.89

- Create a linux CLI oneliner to extract the source ports of the DNS requests in the sip_dump.pcap file.

- Create a linux CLI oneliner to download and decode the encoded file “encoded.text” on http://debbie.vlan77.be/nw2/encoded.

- What linux command with options should be used to perform a scan to the server debbie.vlan77.be with the following requirements:

  TCP connect scan
  Service scan (banner grabbing)

- Create a oneliner to find a match between different rsa private key files and their csr files. The output should look like: alfa.key matches to beta.csr. To test your oneliner you can create some openssl rsa private key files and their csr.

- Create a linux CLI oneliner to extract an overview of the different FTP usernames in the file ftp_bruteforce.pcap.

- Create a oneliner to show ‘Time = 15:44:25 (11/10/1901)’ with the current time and date.

- Create a CLI oneliner to match all words with 14, 15 and 16 unique letters. The output shoud look like:
  Words with 14 letters:
  bedrijfsomvang
  ...
  Words with 15 letters:
  ...

- What linux command with options should be used to perform a scan with the following requirements:

  Scan all systems in 193.191.187.12/25
  Exclude 192.191.187.1 and 192.191.187.2

- Create a CLI oneliner using openssl to retrieve the certificate of the server www.facebook.be and to encrypt the text “CNW2 RULES” with it’s public key.

- Create a CLI oneliner to find a match between different rsa private key files and their companion crt files. The output should look something like:

  alfa.key matches to beta.crt

- Create a linux CLI oneliner to extract the top 3 SIP methods in sip_dump.pcap.

- Which linux command with options should be used to perform a scan with the following requirements:

  Scan the first 20 systems in 193.191.187.129/25.
  Use the system debbie.vlan77.be as ftp proxy server.

- Create a CLI oneliner to retrieve the file public.gpg from the site encoded.rudi.vlan77.be and encode the (own created) file clear.txt into secret.txt.

- What Linux ssh command do you use to bind your local port 3000 to a web server on port 4444 on the network of the ssh server.

- Create a regular expression to match all words in a dictionary with 5 unique letters.

- Use tshark to create an overview and an amount of the different response codes of FTP in the file ftp_bruteforece.pcap.