How could somebody on the defense side (i.e., in charge of the network security) make the most of whois against attackers?

- that you are exposing too much information about yourself in your own domain info (owners name, address, phone number, etc.)
- how long domains have been registered so that you can use automated tools to block domains that are very young (and likely to be malicious if suddenly appearing in emails)
- who to contact in the event that a legitimate domain is sending spam or hosting malicious content
- To complying with ICANN's policies, there must be *some* contact information in the WHOIS record for your domain, but it doesn't have to be your personal data.

1.2 - Netcraft - go to resources -> Site report

1.2 Host command

host tieto.com
tieto.com has address 217.114.85.70
tieto.com mail is handled by 10 ebb07.tieto.com.
tieto.com mail is handled by 10 ebb09.tieto.com.
tieto.com mail is handled by 10 ebb08.tieto.com.
tieto.com mail is handled by 10 ebb10.tieto.com.

Alternative:

- dig:
    - dig tito.com MX

```
; <<>> DiG 9.16.37-Debian <<>> tieto.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41838
;; flags: qr rd ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;tieto.com.                     IN      MX

;; ANSWER SECTION:
tieto.com.              0       IN      MX      10 ebb07.tieto.com.
tieto.com.              0       IN      MX      10 ebb09.tieto.com.
tieto.com.              0       IN      MX      10 ebb08.tieto.com.
tieto.com.              0       IN      MX      10 ebb10.tieto.com.

;; Query time: 0 msec
;; SERVER: 172.31.96.1#53(172.31.96.1)
```

;; WHEN: Sat May 13 11:39:39 CEST 2023
;; MSG SIZE rcvd: 160

- dig tieto.com MX +short
  - 10 ebb07.tieto.com.
  - 10 ebb09.tieto.com.
  - 10 ebb08.tieto.com.
  - 10 ebb10.tieto.com.

- nslookup
  nslookup
  > set type=mx
  > tieto.com
  Server: 10.0.0.138
  Address: 10.0.0.138#53

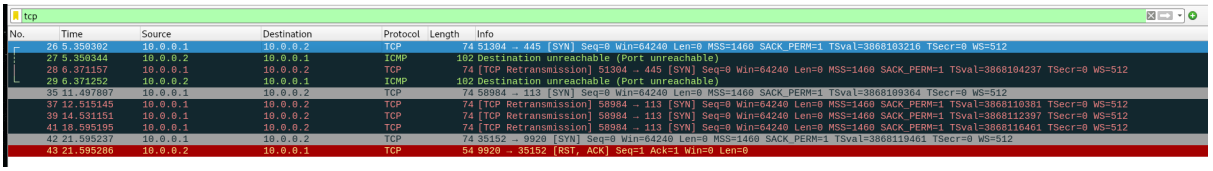
  Non-authoritative answer:
  tieto.com mail exchanger = 10 ebb07.tieto.com.
  tieto.com mail exchanger = 10 ebb09.tieto.com.
  tieto.com mail exchanger = 10 ebb08.tieto.com.
  tieto.com mail exchanger = 10 ebb10.tieto.com.

Are mail servers hosted by the same company? Depending on the company, the answer to this question can be "yes" or "no". Considering each of these possibilities, does it make sense targeting mail servers as potential vectors for penetration attacks?
In case that the mail server is hosted by the same company the answer is clearly yes as this might give access to other servers as well if the different company servers are not properly separated / isolated from each other. While additionally giving additional information via email.

If the mail server is hosted by a different company the answer is still yes as this can open up the possibility for supply chain attacks or give more information about the company. However, in this case it is really important to get a permit to attack for this part as well because otherwise this is not legal.

Why email: password resets via email, sensitive data, company secrets, address books, …

2.2 Port probing



10.0.0.1 -> 10.0.0.2 445 - Destination unreachable ICMP
10.0.0.1 -> 10.0.0.2 113 - Paket dropped no response = retransmission
10.0.0.1 -> 10.0.0.2 9920 - RST (destination port is closed)

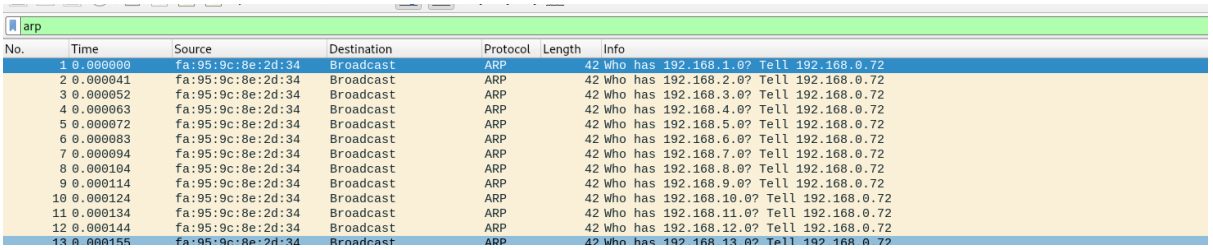
Imagine using Wireshark for checking all the traffic passing through an intermediate routing device. Do you think that you could detect hosts performing horizontal scanning? And vertical scanning? Do you consider Wireshark as a suitable tool for analyzing large amounts of network traffic data? Why?

The problem with wireshark is that it is really good for static analysis but not so much for dynamic analysis. For dynamic analysis the new packets are constantly coming in which makes analysing the data really hard. For this purpose tools like suricata or snort are better suited especially because they also have alerting functionalities that make it easier to focus only on the important packets.

However, for static data wireshark it is possible to detected horizontal and vertical scanning as one can filter accoring to some tcp port or soucre ip and also specify ip ranges. But this comes with a lot of effort (think about legitimate connections). The problem is you cannot specify complex rules like: if from one source ip there are requests to greater x ips alert me.

3.1 - Horizontal scan

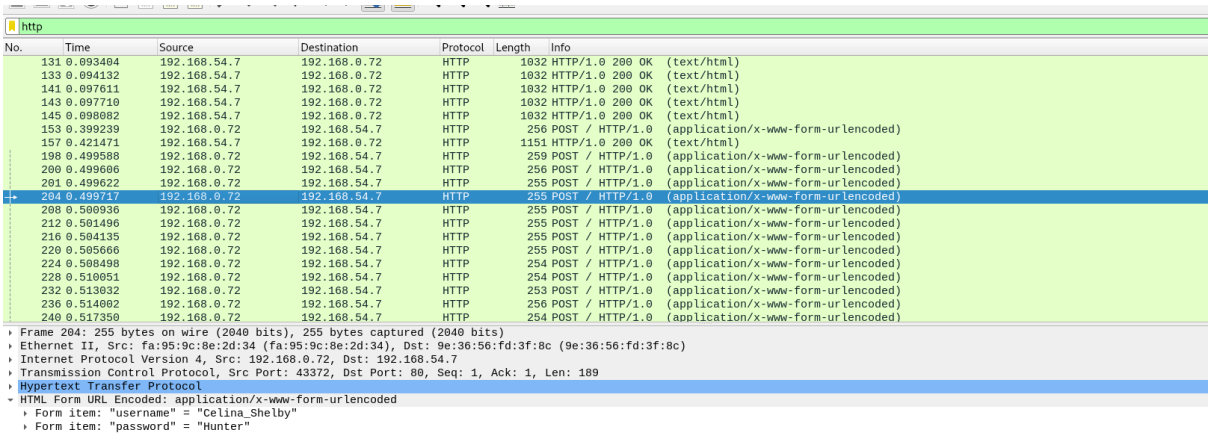
addresses are varied



The size of an ARP request or reply packet is 28 bytes **and more importantly not really a calculation is needed when receiving the response**. (DOS attack)

https://blog.radware.com/security/2012/02/ddos-attacks-myths/

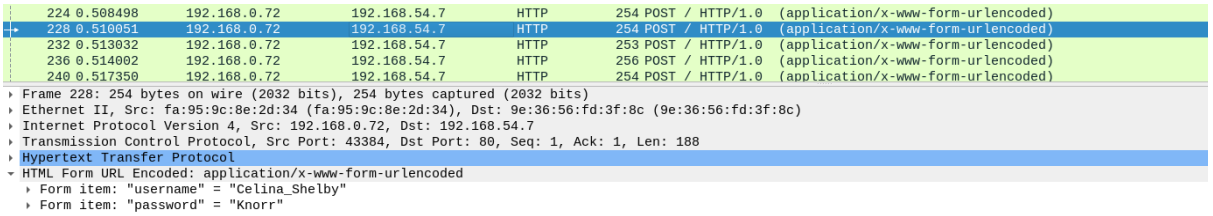
3.1 - Bruteforce

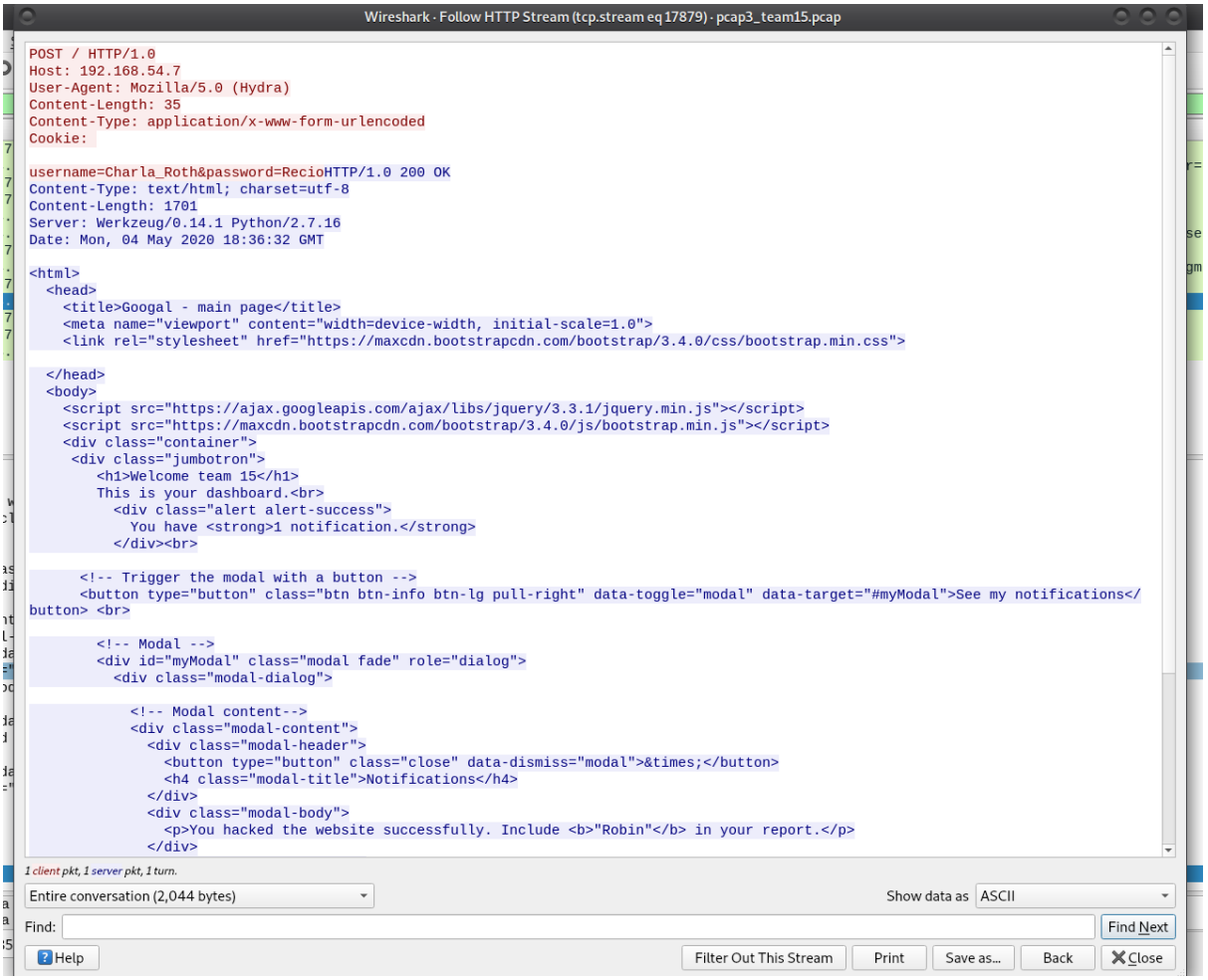


Find butofocre creds:

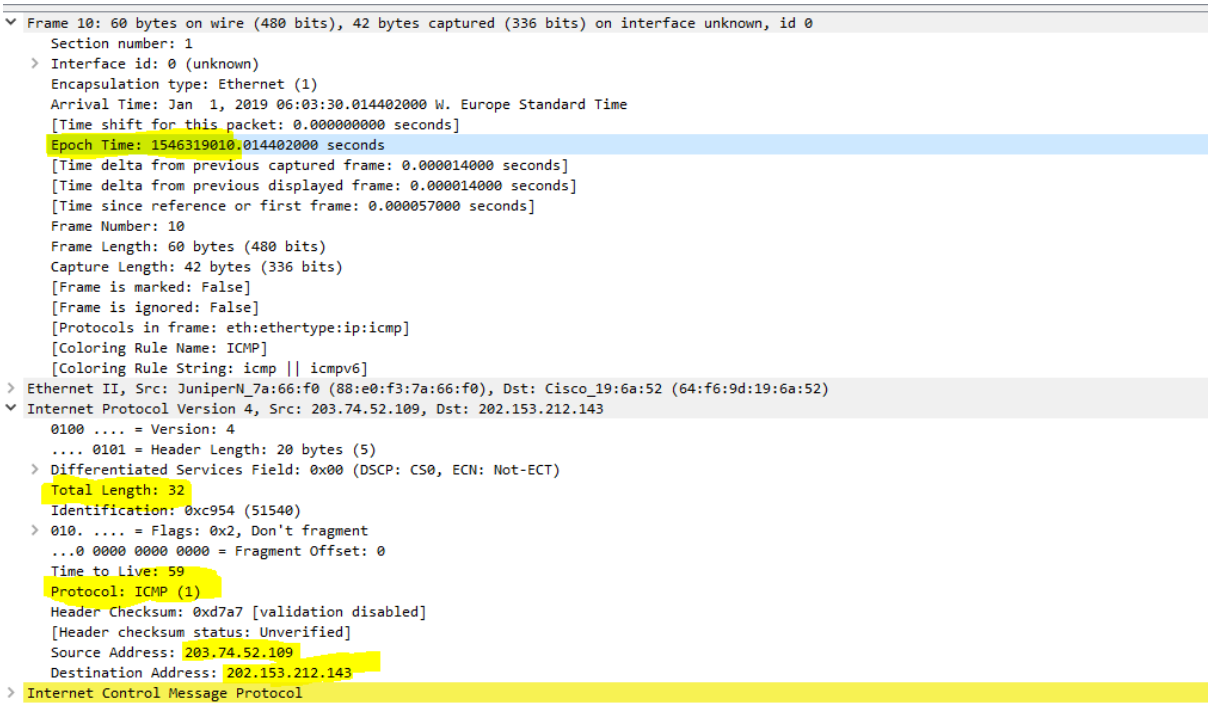
http && (http.content_length > 1000 || http.content_length < 800)

!data-text-lines contains "Invalid Credentials" && http.response.code == 200 && !data-text-lines contains "Login"





2 -
wireshark packet 10
PING nutzt das Protokoll ICMP, welches auf der Ebene 3 im OSI-Schichtenmodell angesiedelt ist, wie IP. Es ist also etwas "tiefer" als TCP und UDP, die auf Ebene 4 sind. ICMP kennt daher auch keine "Ports".



Install Go-Flows

1) Clone repo
2) go build
3) go install
4) locate go-flows binary (was in ~/go/bin)
5) execute command: ./go-flows run features /mnt/c/Users/alexh/Downloads/pcap2pkts.json export csv Ex2_team15.csv source libpcap /mnt/c/Users/alexh/Desktop/Ex2_team15.pcap

Remember that here we have extracted flows within a time-frame of 10 seconds. Can you think about legitimate and ilegitimate situations for case (c), i.e., a source sending traffic to many different destinations in a short time?

- Legitimate
  - Server (sends to many clients)
- Illegitimate
  - Horizontal Scan
  - Botnet control traffic

You can additionally count the number of flows that show TCP, UDP, ICMP, and other IP protocols as "mode" protocol. Do you think that you will get a similar proportion as in [rep-11]? Beyond answering "yes" or "no", think about reasons that might make such proportions similar or different (there are some that are worth considering).

mode: value that appears the most
mode count: how often is the mode value present

rep23: diagram does not tell us anything…. the number in the diagram works however (even though it is off by approx. 10 or so) 176977 works with 176964

rep23:
solution - use filter

part 2:
srcip address: 93.91.224.215
total # of sent packets: 35397