Post-Lab 1 Report
Secure Systems and Networks
dr inż. Tomasz Surmacz

Piotr Giedziun 184731
Lab Date: 21/10/14

Abstract

This report presents the analysis of the packages gathered by Wireshark. I did observe several protocols vulnerabilities. They are related to unsafe handling of data. Unsecure protocols such as FTP and HTTP uses plain-text transmission of passwords over the network. Report also covers tools to diagnose network like ping and traceroute. Ping is used to test reachability, on the other hand traceroute is used to obtain messages path.

Introduction

Our task was to investigate network traffic while given tasks were performed. The virtual machine, on which all tasks were executed runs Ubuntu with root privileges. I used Wireshark in order to monitor and sniff local network traffic. Everything else was already preinstalled.

Ping

Ping is a administration utility used to test host reachability. In my cases I pinged to google.com host. In order to obtain IP address of given host DNS query was executed.

No.	Source	Destination	Protocol	Length	Info
1	10.0.2.	192.168.1.1	DNS	70	Standard query 0x4aa9 A google.com
2	192.168	10.0.2.15	DNS	326	Standard query response 0x4aa9 A 89.228.4.222 A 89.228.4.251 A 89.228.4.247 A

Figure 1: Sniffed DNS packages

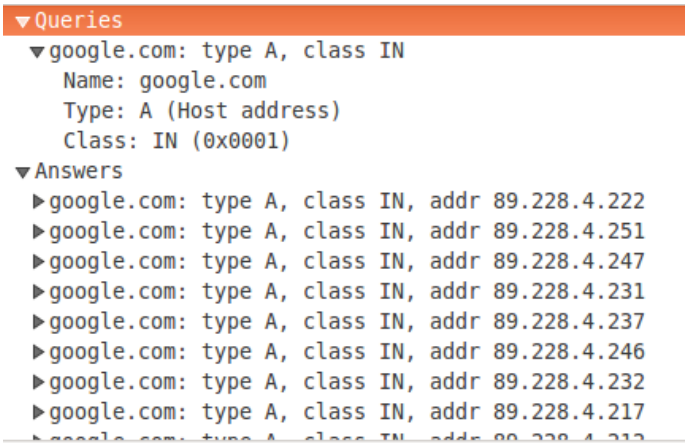

Figure 2: DNS query response

Ping uses ICMP protocol's 'echo' request and reply message types. ICMP is categorized as a layer 3 protocol in the OSI model (Network layer). ICMP packet is an IP packet with ICMP data in it. Ping is limited as a diagnostic tool, information received declares if we can reach the

```
 7 10.0.2.89.228.4.222 ICMP      98 Echo (ping) request  id=0x0d85, seq=2/512, ttl=64 (reply in 8)
 8 89.228.10.0.2.15    ICMP      98 Echo (ping) reply    id=0x0d85, seq=2/512, ttl=58 (request in 7)
 9 10.0.2.89.228.4.222 ICMP      98 Echo (ping) request  id=0x0d85, seq=3/768, ttl=64 (reply in 10)
10 89.228.10.0.2.15    ICMP      98 Echo (ping) reply    id=0x0d85, seq=3/768, ttl=58 (request in 9)
11 10.0.2.89.228.4.222 ICMP      98 Echo (ping) request  id=0x0d85, seq=4/1024, ttl=64 (reply in 12)
12 89.228.10.0.2.15    ICMP      98 Echo (ping) reply    id=0x0d85, seq=4/1024, ttl=58 (request in 11)
13 10.0.2.89.228.4.222 ICMP      98 Echo (ping) request  id=0x0d85, seq=5/1280, ttl=64 (reply in 14)
14 89.228.10.0.2.15    ICMP      98 Echo (ping) reply    id=0x0d85, seq=5/1280, ttl=58 (request in 13)
15 10.0.2.89.228.4.222 ICMP      98 Echo (ping) request  id=0x0d85, seq=6/1536, ttl=64 (reply in 16)
16 89.228.10.0.2.15    ICMP      98 Echo (ping) reply    id=0x0d85, seq=6/1536, ttl=58 (request in 15)
17 10.0.2.89.228.4.222 ICMP      98 Echo (ping) request  id=0x0d85, seq=7/1792, ttl=64 (reply in 18)
18 89.228.10.0.2.15    ICMP      98 Echo (ping) reply    id=0x0d85, seq=7/1792, ttl=58 (request in 17)
19 10.0.2.89.228.4.222 ICMP      98 Echo (ping) request  id=0x0d85, seq=8/2048, ttl=64 (reply in 20)
20 89.228.10.0.2.15    ICMP      98 Echo (ping) reply    id=0x0d85, seq=8/2048, ttl=58 (request in 19)
```

Figure 3: Echo request/replay packages

target network element. Moreover it doesn't tell if we can reach target service. It can only tell determine if we can reach the IP layer of the target.

Traceroute

Traceroute is a diagnostic tools used to diagnosis latency in the transit path. This time around I decided to ping google DNS server.

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  1.313 ms  1.270 ms  1.220 ms
 2  10.146.0.1 (10.146.0.1)  9.006 ms  12.808 ms  11.910 ms
 3  host-89-228-14-57.dynamic.mm.pl (89.228.14.57)  27.778 ms  27.749 ms  27.708
 ms
 4  gdy-lub-1.gdynia.mm.pl (217.172.225.145)  28.853 ms  28.816 ms  28.781 ms
 5  89.228.2.33 (89.228.2.33)  27.543 ms host-176-221-97-1.dynamic.mm.pl (176.22
1.97.1)  27.718 ms host-176-221-97-233.dynamic.mm.pl (176.221.97.233)  27.670 ms
 6  89.228.6.38 (89.228.6.38)  27.414 ms  22.469 ms  25.769 ms
 7  de-cix20.net.google.com (80.81.193.108)  48.859 ms  44.108 ms  48.327 ms
 8  209.85.253.244 (209.85.253.244)  49.245 ms  51.416 ms  51.369 ms
 9  209.85.251.248 (209.85.251.248)  48.959 ms 209.85.251.178 (209.85.251.178)
48.000 ms 72.14.234.231 (72.14.234.231)  48.951 ms
10  209.85.240.142 (209.85.240.142)  57.813 ms  57.764 ms  57.704 ms
11  209.85.255.75 (209.85.255.75)  57.650 ms 209.85.254.213 (209.85.254.213)  61
.058 ms 209.85.255.75 (209.85.255.75)  56.404 ms
12  216.239.49.28 (216.239.49.28)  61.369 ms 209.85.255.51 (209.85.255.51)  61.3
48 ms 209.85.254.189 (209.85.254.189)  54.075 ms
13  * * *
14  google-public-dns-a.google.com (8.8.8.8)  57.513 ms  61.344 ms  58.564 ms
```

Figure 4: Traceroute response

Traceroute sends ICMP Echo Request packages with TTL (Time-to-live) value starting with 1. Each receiver decrement packet' TTL value by one, when TTL value is equal to zero packet is dropped. As a response router sends an ICMP Time Exceeded message to the source. Thus gives us an ability to reproduce transmit path.

The path (following IP addresses) alongside with round-trip times of packets was displayed in terminal (Figure 4).

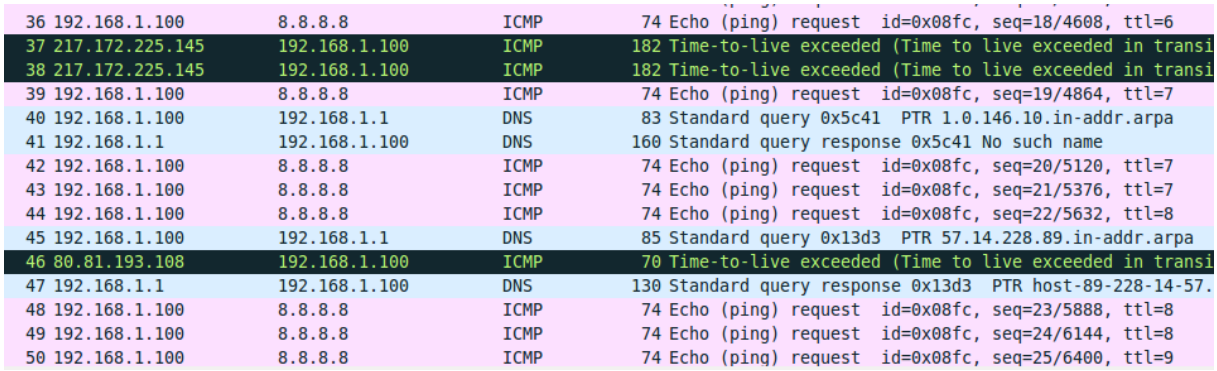

Figure 5: ICMP Echo Request TTL values

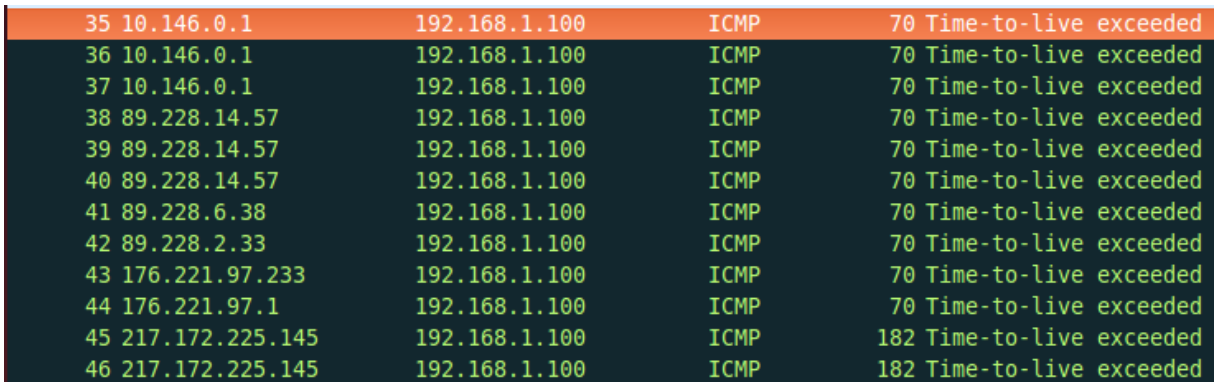

Figure 6: ICMP with TTL Expired filter

FTP auth

FTP (File Transfer Protocol) is used to transfer files in network. There is multiple methods to secure FTP transfers like FTPS or SFTP. For our task we used standard FTP protocol, without any encryption.

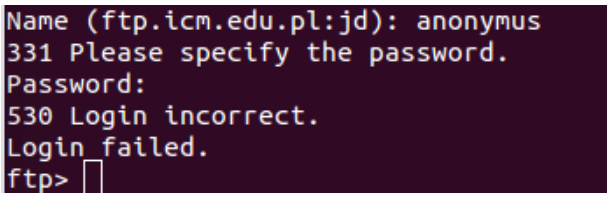

Figure 7: FTP login - terminal

Our job was simply sniff the password sent through FTP protocol.

Here is the sniffed data in a raw form.

The password and username were sent as a ASCII characters. AN attacker has access to all three things required to lo on to FTP account (destination IP address, username and password).

Same rule applies to file transfer. Files transferred via FTP were also sent as a plain-text. We are able to reconstruct entire file using Follow TCP Stream option.

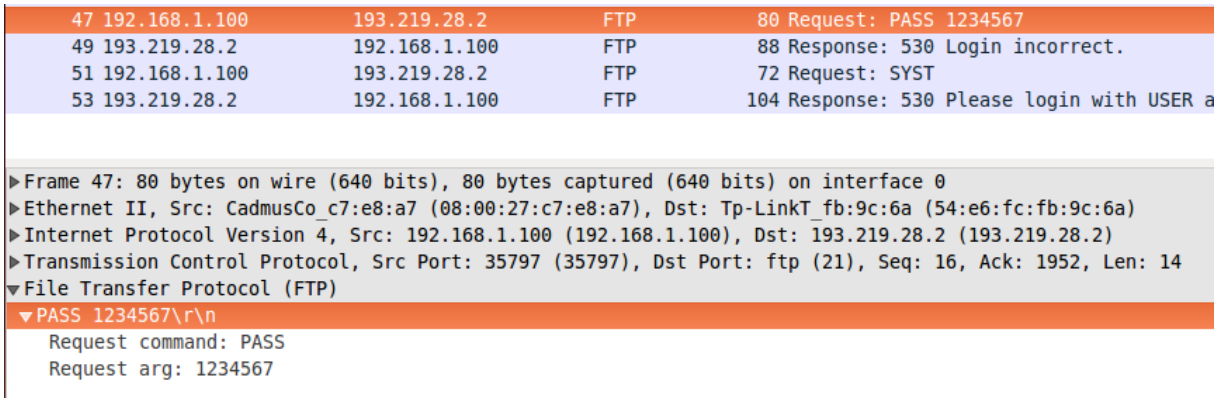

Figure 8: sniffed packages

HTTP auth

HTTP auth uses a combination of a username and password to authenticate the user. Server as a response sends a message with "Authorization Required" header. User is prompted to enter username and password, entered data is sent in 'Authorization' header. Username and password is encoded using the Base 64. In our case Wireshark (as shown in Figure 9) decrypted it for us (username: test, password: test).

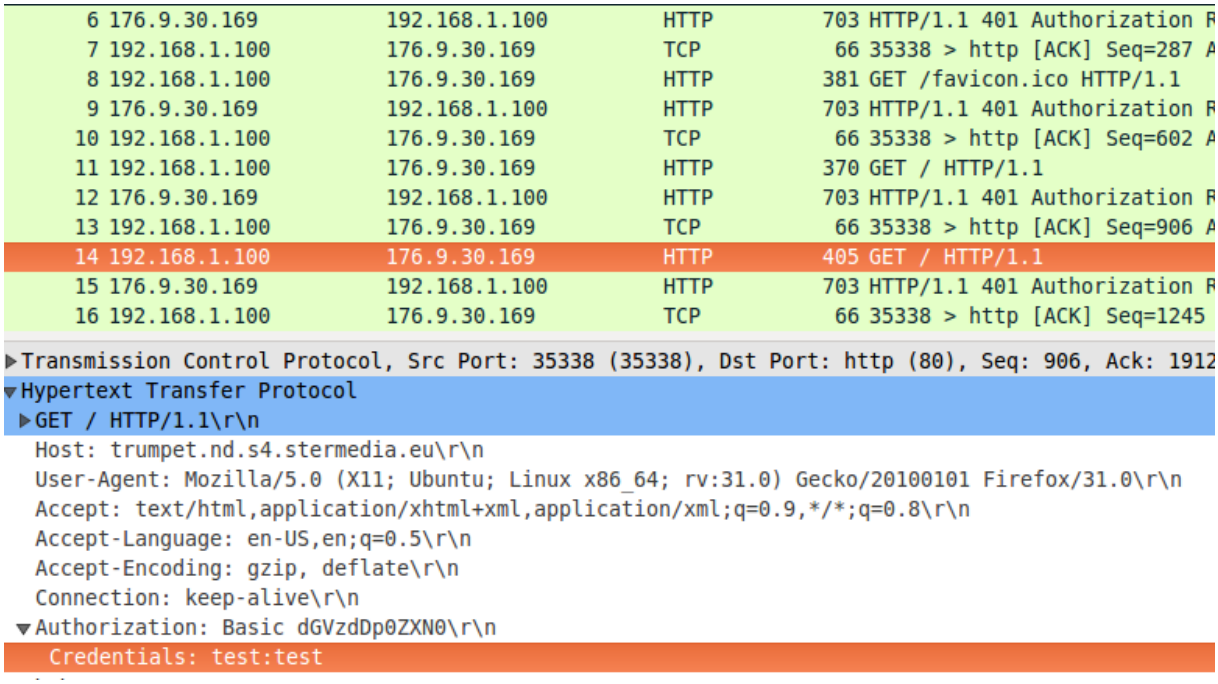

Figure 9: sniffed HTTP-Base Auth

References

[1] http://www.networksorcery.com/enp/protocol/icmp.htm

[2] http://linux.die.net/man/8/traceroute

[3] http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html