Liên kết khác k3751070033@gmail.com Bảng điều khiển Đăng xuất

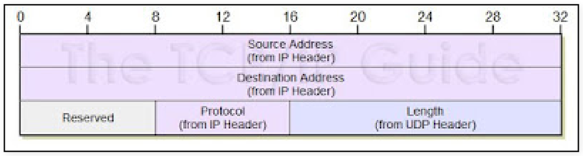
Learning by practicing

Learning is an ongoing activity ... practicing makes it fun

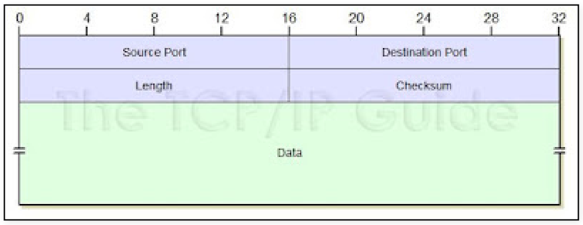
Monday, August 3, 2015

Calculating the UDP Checksum, with a taste of scapy + Wireshark

In this post we will calculate the UDP checksum. To calculate the UDP checksum we first must understand, in addition to its own header, UDP checksum uses a pseudo header. This pseudo header consists of the original source IP, destination IP, reserved (identified as 0000 0000), protocol (x11) and the length from the UDP header.

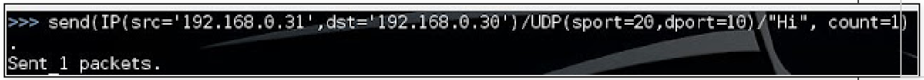

0
4
8
12
16
20
24
28
32
Source Address (from IP Header)
Destination Address (from IP Header)
Reserved
Protocol (from IP Header)
Length (from UDP Header)
The TCP/IP Guide

UDP pseudo header. Reprinted with permission from tcpipguide.com



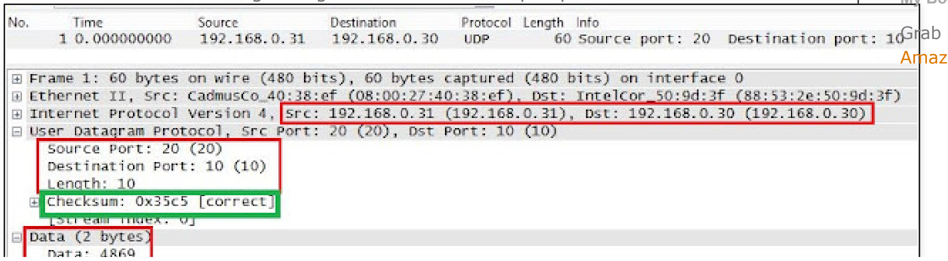
UDP header: Reprinted with permission from tcpipguide.com

Considering the above, let us craft a UDP Packet in scapy. We have the following
Source IP = 192.168.0.31
Destination = 192.168.0.30
UDP source port = 20
UDP destination port = 10
Data (2 bytes) = "Hi"



```
>>> send(IP(src='192.168.0.31',dst='192.168.0.30')/UDP(sport=20,dport=10)/"Hi", count=1)
.
Sent 1 packets.
```

Let's see what the receiving host got from a Wireshark perspective



```
No.   Time          Source         Destination    Protocol Length Info
    1 0.000000000   192.168.0.31   192.168.0.30   UDP         60 Source port: 20  Destination port: 10

⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: CadmusCo_40:38:ef (08:00:27:40:38:ef), Dst: IntelCor_50:9d:3f (88:53:2e:50:9d:3f)
⊞ Internet Protocol Version 4, Src: 192.168.0.31 (192.168.0.31), Dst: 192.168.0.30 (192.168.0.30)
⊟ User Datagram Protocol, Src Port: 20 (20), Dst Port: 10 (10)
    Source Port: 20 (20)
    Destination Port: 10 (10)
    Length: 10
  ⊞ Checksum: 0x35c5 [correct]
    [Stream index: 0]
⊟ Data (2 bytes)
    Data: 4869
```

Contributors

- Abdul
- Nik Alleyne, MSc | CISSP | GC|IA|IH|REM|PEN

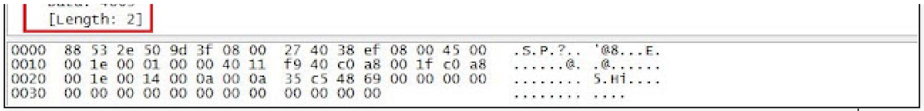
Keep up-to-date with the latest posts
Enter your email address:

Subscribe

Delivered by FeedBurner

My Book Resume, SANS GCIA Gold Paper, etc

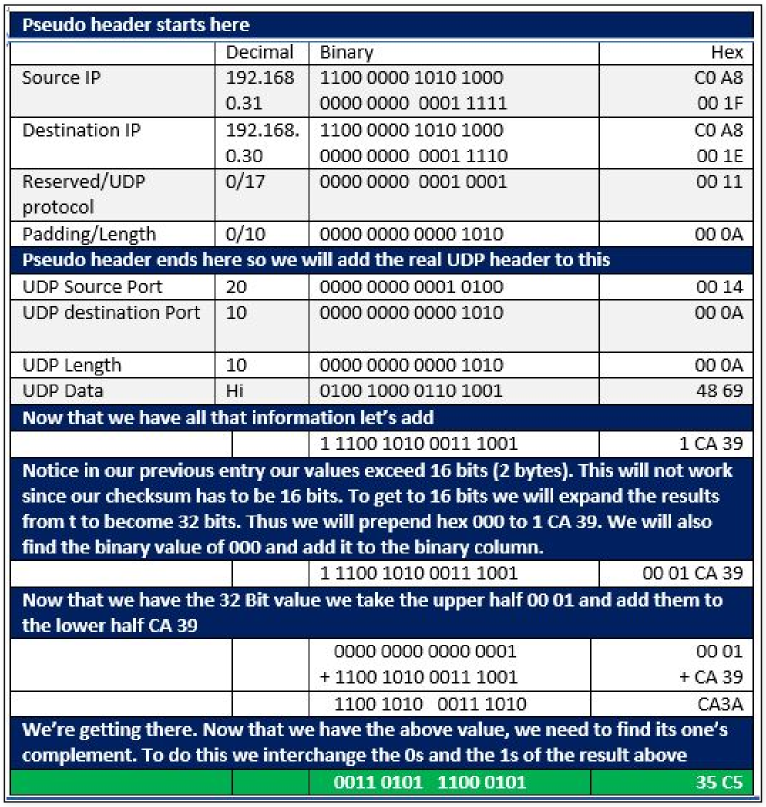
Grab a copy of Hack and Detect from Amazon. Read the sample chapters.



```
[Length: 2]

0000  88 53 2e 50 9d 3f 08 00  27 40 38 ef 08 00 45 00   .S.P.?.. '@8...E.
0010  00 1e 00 01 00 00 40 11  f9 40 c0 a8 00 1f c0 a8   ......@. .@......
0020  00 1e 00 14 00 0a 00 0a  35 c5 48 69 00 00 00 00   ........ 5.Hi....
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

when adding, these values needs to be added 16 bits or 2 bytes at a time.



Pseudo header starts here			
	Decimal	Binary	Hex
Source IP	192.168 0.31	1100 0000 1010 1000 0000 0000 0001 1111	C0 A8 00 1F
Destination IP	192.168. 0.30	1100 0000 1010 1000 0000 0000 0001 1110	C0 A8 00 1E
Reserved/UDP protocol	0/17	0000 0000 0001 0001	00 11
Padding/Length	0/10	0000 0000 0000 1010	00 0A
Pseudo header ends here so we will add the real UDP header to this			
UDP Source Port	20	0000 0000 0001 0100	00 14
UDP destination Port	10	0000 0000 0000 1010	00 0A
UDP Length	10	0000 0000 0000 1010	00 0A
UDP Data	Hi	0100 1000 0110 1001	48 69
Now that we have all that information let's add			
		1 1100 1010 0011 1001	1 CA 39
Notice in our previous entry our values exceed 16 bits (2 bytes). This will not work since our checksum has to be 16 bits. To get to 16 bits we will expand the results from t to become 32 bits. Thus we will prepend hex 000 to 1 CA 39. We will also find the binary value of 000 and add it to the binary column.			
		1 1100 1010 0011 1001	00 01 CA 39
Now that we have the 32 Bit value we take the upper half 00 01 and add them to the lower half CA 39			
		0000 0000 0000 0001 + 1100 1010 0011 1001	00 01 + CA 39
		1100 1010 0011 1010	CA3A
We're getting there. Now that we have the above value, we need to find its one's complement. To do this we interchange the 0s and the 1s of the result above			
		0011 0101 1100 0101	35 C5

That's it our UDP Checksum is 0x35C5 which matches what Wireshark provided us above.
Hope this helps someone who wanted to know how to calculate the UDP Checksum

References:

http://www4.ncsu.edu/~mlsichit/Teaching/407/Resources/udpChecksum.html
http://www.tcpipguide.com/free/t_UDPMessageFormat-2.htm
http://www.secdev.org/projects/scapy/
https://www.wireshark.org/
https://www.ietf.org/rfc/rfc768.txt

Posted by Nik Alleyne, MSc | CISSP | GC|IA|IH|REM|PEN at 8:16 PM

9 comments:

Unknown October 28, 2017 at 1:32 AM

This comment has been removed by the author.

Reply

Replies

Unknown May 30, 2019 at 11:05 AM

Really ???? so sad :p

Reply

Unknown July 4, 2018 at 9:29 PM

Thank you for this tutorial.

Reply

View a PDF version of my resume
Presentation to the Ottawa Chapter of the High Technology Crimes Investigation (HTCIA) Association & ISC2 Toronto Chapter, SANS @night, etc
Building a Forensically Capable Network Infrastructure

SANS Webcast
The Importance of Intrusion Detection in a compromise prone world

Presentation at Canada International Cyber Security Conference:
Threat Analysis and Investigative Techniques in the Modern world

SANS GCIA Gold Paper
Building a Forensically Capable Network Infrastructure

Github Project QRadar ThreatIntel
Qradar Threat Intel on the Cheap

Python/Scapy DNS Spoofing Tool/Tutorial

Masters Capstone Paper
FROM PAPERLESS TO PLASTICLESS, EMV CARD SECURITY AND THE FUTURE OF PAYMENTS IN THE USA

asecure.cloud - Build a Secure Cloud
A free repository of customizable AWS security configurations and best practices

Generate custom CloudFormation and CLI deployment scripts by adding multiple configuration items to stacks
go get it **here**

My GITHub

Blog Archive

- ► 2023 (3)
- ► 2022 (16)
- ► 2021 (32)
- ► 2020 (39)
- ► 2019 (27)
- ► 2018 (24)

Replies

Nik Alleyne, MSc | CISSP | GC|IA|IH|REM|PEN January 29, 2019 at 7:50 PM

Sonu,
You are welcome!

Reply

Anonymous October 27, 2020 at 2:56 PM

the tutorial helped loads! Thank you!

Reply

Replies

Nik Alleyne, MSc | CISSP | GC|IA|IH|REM|PEN October 27, 2020 at 2:58 PM

Really happy you found it beneficial.

Reply

lechercheur123 November 24, 2020 at 3:47 AM

This tutorial helped me to check that my checksum calculator program worked. It was very helpful :)

Reply

Replies

Nik Alleyne, MSc | CISSP | GC|IA|IH|REM|PEN November 24, 2020 at 6:10 AM

I'm glad you found it helpful lechercheur123!

Reply

hasnain July 9, 2021 at 11:31 PM

To calculate the UDP checksum we first must understand, in addition to its own header, UDP checksum uses a pseudo header. matrix calculator can be of great use here to make it easy.

Reply

Enter Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

- ► 2017 (64)
- ► 2016 (42)
- ▼ 2015 (86)
  - ► December (5)
  - ► November (11)
  - ► October (4)
  - ► September (3)
  - ▼ August (7)
    - Windows 10 Recycle Bin Analys - RIFIUTI2
    - Calculating the TCP Checksum, with a taste of scap...
    - Calculating the UDP Checksum, with a taste of scap...
    - Calculating the IP Checksum, with a taste of scapy...
    - Stimulus and response revisited
    - Integrating RSA 8.1 (SNMPv3 traps) with Splunk on ...
    - Metadata - Telling the story
  - ► July (6)
  - ► June (9)
  - ► May (7)
  - ► April (8)
  - ► March (9)
  - ► February (8)
  - ► January (9)
- ► 2014 (70)

Learning Sites:
http://www.securitytube.net
http://www.cybrary.it/
ENISA
Seed Labs
Open Security Training
Fuzzy Security
Honeynet Project
Corelan Exploiting Writing Tutorial
Mitre

Additional Readings
SANS Reading Room
https://www.us-cert.gov/
http://taosecurity.blogspot.ca/
http://krebsonsecurity.com/
http://securityweekly.com/
http://www.csoonline.com/blogs
https://securosis.com/blog/
http://threatpost.com/
http://nakedsecurity.sophos.com/
http://blog.zeltser.com/
https://www.schneier.com/
Morning Star Security
Infosec Industry

Intelligence Feeds - IPs/Domains/URLs

[MALICIOUS IPs]
Emerging Threats - Compromised IPs
My IPs
Spamhause drop
Spamhause edrop
Emerging Threats Block IP
DShield
SANS ISC
Zonefiles.io
SSL IP Blokclist
SSL IP Blokclist - Aggressive
Feedotracker - recommended ip blocklist
Feedotracker - IP Blocklist

Block IP

[MALICIOUS DOMAINS]
Malware Domains Delisted
OpenPhish
Hostnames
Domains
Domains

[MALICIOUS URLS]
vxvault.net URL_List

[PHISHING URLS]
openphish

Below is a list of threat intelligence websites that you can use. Cymon.io is an excellent one as it searches around 200 different sources. If you’re looking for a more exhaustive list of threat intel sites, check out https://github.com/rshipp/awesome-malware-analysis

IP and Domain Reputation / Malicious Activity Reports
http://cymon.io
https://www.recordedfuture.com/live/
http://urlquery.net/ (URL Scanner)
https://virustotal.com/
https://otx.alienvault.com/
https://exchange.xforce.ibmcloud.com/

IP Information (open ports, details, WHOIS, etc)
https://www.censys.io
https://www.shodan.io/
https://centralops.net/co/
http://viewdns.info/
https://www.threatcrowd.org

Malware Analysis
https://malwr.com/
https://www.hybrid-analysis.com/

Misc
https://isc.sans.edu/services.html (Port information)

Malware / Malicious Site Samples:
https://malwr.com/
http://vxvault.net/ViriList.php
http://cybercrime-tracker.net/
https://ransomwaretracker.abuse.ch/tracker/
http://malc0de.com/database/

OSINT Framework