Radius Packet Generator ToolKit

Introduction:

The Radius Packet Generator tool allows you to craft or build a Radius Authentication, Accounting, COA and Authorization packet.

#Developed by Sumit Thapa

Emai Address : thapa.sumit6@gmail.com

Follow linkedin: https://www.linkedin.com/in/sumit-thapa-99a75996/

#Follow Github : https://github.com/sumitthapa/RadiusPacketGeneratorToolKit

Packet Flow:

[Web Browser] ==== HTTP_POST ====➜ [Code Server X extracts post data and initiate radius traffic] ===== Radius Protocol==➜ [Radius Server]

Installation:

i.   Download XAMP server.
URL : https://www.apachefriends.org/download.html

ii.   1 Download Perl Radius module.

URL: https://pecl.php.net/package/radius/1.4.0b1/windows

iii.   Include Perl radius extension path

Path: C:/xampp/php/ext/

iv.   Then add **php_radius.dll** extension.

v.   Edit "php.ini" file in module settings.

```
extension=php_radius.dll
zend_extension=another_extension
```

vi.   In the xamp htdocs folder add "radius.php" and "processradius.php" file.

Source code : https://github.com/sumitthapa/RadiusPacketGeneratorToolKit

vii.   Access page http://localhost/radius.php

Console:

1. Radius_IP_Address : <Radius Server IP>

2. Radius_Secret_Key : <Radius Secret Key>

3. Radius_Port : <Customizable port>

4. Radius Handle Type

i. RADIUS_ACCESS_REQUEST: An Access-Request, used to authenticate a user against a RADIUS server.

ii. RADIUS_ACCOUNTING_REQUEST : An Accounting-Request, used to convey accounting information for a service to the RADIUS server.

iii. RADIUS_DISCONNECT_REQUEST : Disconnect-Request, sent from the RADIUS server to indicate that the user session must be terminated.

iv . RADIUS _COA_REQUEST : A CoA-Request, sent from the RADIUS server to indicate that the authorisations within the user session have changed. A response must be sent in the form of a CoA-ACK or a CoA-NAK.

5. Radius attributes to pass attribute pair and value.

Example :

a. How to send Access-Request used to authenticate RADIUS user.

| Radius IP_Address : 10.40.19.235 | Radius Secret_Key : admin@123 | Radius_Port : 1812 |

Radius Handle Type : ● RADIUS_ACCESS_REQUEST ○ RADIUS_ACCOUNTING_REQUEST ○ RADIUS_DISCONNECT_REQUEST ○ RADIUS_COA_REQUEST

[Radius Attributes] Supported Attributes [Click Here]

1. Radius Handle Type : radius_put_attr Attribute_type RADIUS_USER_NAME Address_Value sumit
2. Radius Handle Type : radius_put_attr Attribute_type RADIUS_USER_PASSWORD Address_Value admin@123 ⊕ ⊗

Available Attribute_Type Option : RADIUS_USER_NAME   RADIUS_USER_PASSWORD

Generate Packet

[Radius Server Configuration]

Radius_Server_IP : 10.40.19.235, Port : 1812, Shared_Key : admin@123, Radius Handle Type: **RADIUS_ACCESS_REQUEST**

Total Group Attributes : 2
Resource > radius_put_attr, [Attributes Value Pair : t=RADIUS_USER_NAME length=5 val= sumit]
Resource > radius_put_attr, [Attributes Value Pair : t=RADIUS_USER_PASSWORD length=9 val= admin@123]

Radius Result :
Authentication successful⌐X
[85 4 Bytes 00000258]

Output:

| 📘 radius |
No.	Time	Source	Destination	Protocol	Length	Info
17	-7.964054	172.31.137.100	10.40.19.235	RADIUS	87	Access-Request id=175
19	-7.696016	10.40.19.235	172.31.137.100	RADIUS	68	Access-Accept id=175

▷ Frame 17: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0
▷ Ethernet II, Src: 00:66:65:72:26:01 (00:66:65:72:26:01), Dst: 00:62:6f:73:41:03 (00:62:6f:73:41:03)
▷ Internet Protocol Version 4, Src: 172.31.137.100, Dst: 10.40.19.235
▷ User Datagram Protocol, Src Port: 63119, Dst Port: 1812
⊿ RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0xaf (175)
    Length: 45
    Authenticator: e06f3daa4b389f7a15e131a57ca5fb52
    [The response to this request is in frame 19]
  ⊿ Attribute Value Pairs
    ▷ AVP: t=User-Name(1) l=7 val=sumit
    ▷ AVP: t=User-Password(2) l=18 val=Encrypted

Note: The username and password must be pass through "Attribute_Type" as "Radius_put_att" . Example: RADIUS_USER_NAME   RADIUS_USER_PASSWORD

B. How to send radius Disconnect-Request to the authenticator server.

[Radius Packet Generator Tool] by @SumitThapa

Radius IP_Address : 10.40.19.235   Radius Secret_Key : admin@123   Radius_Port : 3799

Radius Handle Type : ○ RADIUS_ACCESS_REQUEST ○ RADIUS_ACCOUNTING_REQUEST ◉ RADIUS_DISCONNECT_REQUEST ○ RADIUS_COA_REQUEST

[Radius Attributes] Supported Attributes [Click Here]

1. Radius Handle Type : radius_put_addr Attribute_type RADIUS_Framed_IP_Address   Address_Value 10.212.134.200

2. Radius Handle Type : radius_put_string Attribute_type RADIUS_USER_NAME   Address_Value sumit ⊕⊗

Available Attribute_Type Option : RADIUS_Framed_IP_Address

Generate Packet

[Radius Server Configuration]

Radius_Server_IP : 10.40.19.235, Port : 3799, Shared_Key : admin@123, Radius Handle Type: RADIUS_DISCONNECT_REQUEST

Total Group Attributes : 2
Resource > radius_put_addr, [Attributes Value Pair : t=RADIUS_Framed_IP_Address length=14 val= 10.212.134.200]
Resource > radius_put_string, [Attributes Value Pair : t=RADIUS_USER_NAME length=5 val= sumit]

No.	Time	Source	Destination	Protocol	Length	Info
1598	27.294686	172.31.128.30	172.31.128.16	RADIUS	75	Disconnect-Request id=65
1604	29.396371	172.31.128.16	172.31.128.30	RADIUS	86	Disconnect-ACK id=65

```
> Frame 1604: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Ethernet II, Src: 00:61:65:67:10:03 (00:61:65:67:10:03), Dst: 00:61:65:67:1e:01 (00:61:65:67:1e:01)
> Internet Protocol Version 4, Src: 172.31.128.16, Dst: 172.31.128.30
> User Datagram Protocol, Src Port: 3799, Dst Port: 52943
∨ RADIUS Protocol
    Code: Disconnect-ACK (41)
    Packet identifier: 0x41 (65)
    Length: 44
    Authenticator: 0dccd45a77c59f001111c2f5e13e8c13
    [This is a response to a request in frame 1598]
    [Time from request: 2.101685000 seconds]
  ∨ Attribute Value Pairs
    > AVP: t=Event-Timestamp(55) l=6 val=Dec 10, 2020 22:25:23.000000000 India Standard Time
    > AVP: t=Message-Authenticator(80) l=18 val=e17b9f3ebf922ae86d7c3cccd14c3862
```

FGT debug :

diagnose debug application radius-das -1

diagnose debug application fnbamd -1

Sample FGT Output :

7080.758 RADIUS message: code=40 (Disconnect-Request) identifier=65 length=33

  Attribute 1 (User-Name) length=7 pos 0xdd48f86

    Value: 'sumit'

  Attribute 8 (Framed-IP-Address) length=6 pos 0xdd48f8d

    Value: 172.31.128.30

77080.771 DAS: received msg with hdr_code 40

77080.774 DAS: No Message-Authenticator attribute found

77080.777 DAS: select framed_ip 172.31.128.30

77080.780 DAS: select user_name sumit

[2450] handle_req-Rcvd 8 req

[306] fnbamd_create_radius_socket-Opened radius socket 15

[306] fnbamd_create_radius_socket-Opened radius socket 16

[2300] fnbamd_radius_acct_send-

[2277] fnbamd_rad_acct_dns_cb-10.40.51.235->10.40.51.235

[2495] __fnbamd_acct_send_pkt-Sent radius req to 10.40.51.235: code=4 id=124 len=166 action=2

77080.836 DAS: 1 auth session(s) deleted.

77080.838 DAS: Received DAS_STA_DEL_RESULT (276 bytes)

77080.841 Received data - hexdump(len=276):

[1515] create_acct_session-Acct type 8 session created

    03 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ....

[528] fnbamd_acct_handle_result-Received valid ack for id 124 from 10.40.51.235

[3111] handle_acct_rsp-Acct session completed

   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ....

[1551] destroy_acct_session-Acct session poll deleted

[1556] destroy_acct_session-Acct session poll deleted

   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ....

[1561] destroy_acct_session-Acct session destroyed

   ...... (20 bytes truncated)

77080.906 DAS: Get coa event result 2 with req_num 21

77082.840 DAS: Reply ACK to 172.31.128.30:52943

C. How to send radius accounting packet using ToolKit.

```
      The Value field is four octets in Integer

   1       Start
   2       Stop
   3       Interim-Update
   7       Accounting-On
   8       Accounting-Off
   9-14    Reserved for Tunnel Accounting
   15      Reserved for Failed
```

RFC : https://tools.ietf.org/html/rfc2866

[Radius Packet Generator Tool BLR]by @SumitThapa

Radius IP_Address : 172.31.128.16   Radius Secret_Key : admin@123   Radius_Port : 1813

Radius Handle Type : ○ RADIUS_ACCESS_REQUEST ● RADIUS_ACCOUNTING_REQUEST ○ RADIUS_DISCONNECT_REQUEST ○ RADIUS_COA_REQUEST

[Radius Attributes]   Supported Attributes [Click Here]

1. Radius Handle Type : radius_put_string   Attribute_type RADIUS_USER_NAME   Address_Value sumit

2. Radius Handle Type : radius_put_addr   Attribute_type RADIUS_Framed_IP_Address   Address_Value 172.31.128.16

3. Radius Handle Type : radius_put_int   Attribute_type RADIUS_ACCT_STATUS_TYPE   Address_Value 1   ⊕ ⊗

Available Attribute_Type Option : RADIUS_USER_NAME   RADIUS_ACCT_SESSION_ID   RADIUS_Framed_IPv6_Prefix RADIUS_ACCT_SESSION_ID   RADIUS_MESSAGE_AUTHENTICATOR RADIUS_ACCT_STATUS_TYPE

Integer

Generate Packet

[Radius Server Configuration]

Radius_Server_IP : 172.31.128.16, Port : 1813, Shared_Key : admin@123, Radius Handle Type: RADIUS_ACCOUNTING_REQUEST

Total Group Attributes : 3
Resource > radius_put_string, [Attributes Value Pair : t=RADIUS_USER_NAME length=5 val= sumit]
Resource > radius_put_addr, [Attributes Value Pair : t=RADIUS_Framed_IP_Address length=13 val= 172.31.128.16]
Resource > radius_put_int, [Attributes Value Pair : t=RADIUS_ACCT_STATUS_TYPE length=1 val= 1]

Wireshark Capture

1739	895.475461	172.31.128.30	172.31.128.16	RADIUS	81 Accounting-Request id=124
1740	895.476097	172.31.128.16	172.31.128.30	RADIUS	62 Accounting-Response id=124

> Frame 1739: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
> Ethernet II, Src: 00:61:65:67:1e:01 (00:61:65:67:1e:01), Dst: 00:61:65:67:10:03 (00:61:65:67:10:03)
> Internet Protocol Version 4, Src: 172.31.128.30, Dst: 172.31.128.16
> User Datagram Protocol, Src Port: 51156, Dst Port: 1813
∨ RADIUS Protocol
      Code: Accounting-Request (4)
      Packet identifier: 0x7c (124)
      Length: 39
      Authenticator: 1c21d2b702002ba00e5791a66152f0f9
      [The response to this request is in frame 1740]
   ∨ Attribute Value Pairs
      > AVP: t=User-Name(1) l=7 val=sumit
      > AVP: t=Framed-IP-Address(8) l=6 val=172.31.128.16
      > AVP: t=Acct-Status-Type(40) l=6 val=Start(1)

aegon-kvm16 # diagnose firewall auth list

aegon-kvm16 # diagnose firewall auth list

172.31.128.16

    type: rsso, id: 0, duration: 455, idled: 455

    flag(10): radius

    server: root

    packets: in 0 out 0, bytes: in 0 out 0

----- 1 listed, 0 filtered ------

aegon-kvm16 # diagnose debug application fnbamd -1

aegon-kvm16 # diagnose debug application radiusd -1

aegon-kvm16 # diagnose debug en

aegon-kvm16 # Received radius accounting eventMissing profile name.DB 0 insert [ep='n/a' pg='n/a' ip='172.31.128.16/32'] success

aegon-kvm16 #

D. How to send radius accounting packet with Group details using ToolKit.

The default FGT value for `rsso-endpoint-attribute` might work in common remote access scenarios where users are identified by their unique `Calling-Station-Id`, but in other scenarios the user name might be in a different attribute.

In our case, we are sending user information in USER_Name attributes.

```
config user radius
    edit "Local RSSO Agent"
        set rsso-endpoint-attribute User-Name
        set sso-attribute User-Name
    next
end
```

[Radius Packet Generator Tool BLR] *by @SumitThapa*

Radius IP_Address : `172.31.128.16`   Radius Secret_Key : `admin@123`   Radius_Port : `1813`

Radius Handle Type : ○ RADIUS_ACCESS_REQUEST ● RADIUS_ACCOUNTING_REQUEST ○ RADIUS_DISCONNECT_REQUEST ○ RADIUS_COA_REQUEST

[Radius Attributes]   Supported Attributes [Click Here]

1. Radius Handle Type : `radius_put_string`	Attribute_type `RADIUS_USER_NAME`	Address_Value `sumit`	
2. Radius Handle Type : `radius_put_addr`	Attribute_type `RADIUS_Framed_IP_Address`	Address_Value `172.31.128.30`	
3. Radius Handle Type : `radius_put_string`	Attribute_type `RADIUS_CLASS`	Address_Value `group1`	
4. Radius Handle Type : `radius_put_int`	Attribute_type `RADIUS_ACCT_STATUS_TYPE`	Address_Value `1`	⊕⊗

Available Attribute_Type Option : RADIUS_USER_NAME   RADIUS_ACCT_SESSION_ID   RADIUS_Framed_IPv6_Prefix RADIUS_ACCT_SESSION_ID   RADIUS_MESSAGE_AUTHENTICATOR

[Generate Packet]

[Radius Server Configuration]

Radius_Server_IP : 172.31.128.16, Port : 1813, Shared_Key : admin@123, Radius Handle Type: RADIUS_ACCOUNTING_REQUEST

Total Group Attributes : 4
Resource > radius_put_string, [Attributes Value Pair : t=RADIUS_USER_NAME length=5 val= sumit]
Resource > radius_put_addr, [Attributes Value Pair : t=RADIUS_Framed_IP_Address length=13 val= 172.31.128.30]
Resource > radius_put_string, [Attributes Value Pair : t=RADIUS_CLASS length=6 val= group1]
Resource > radius_put_int, [Attributes Value Pair : t=RADIUS_ACCT_STATUS_TYPE length=1 val= 1]

No.	Time	Source	Destination	Protocol	Length	Info
8	8.757971	172.31.128.30	172.31.128.16	RADIUS	89	Accounting-Request id=236
9	8.772008	172.31.128.16	172.31.128.30	RADIUS	62	Accounting-Response id=236
259	246.309698	172.31.128.30	172.31.128.16	RADIUS	89	Accounting-Request id=173
260	246.319973	172.31.128.16	172.31.128.30	RADIUS	62	Accounting-Response id=173

```
> Frame 259: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
> Ethernet II, Src: 00:61:65:67:1e:01 (00:61:65:67:1e:01), Dst: 00:61:65:67:10:03 (00:61:65:67:10:03)
> Internet Protocol Version 4, Src: 172.31.128.30, Dst: 172.31.128.16
> User Datagram Protocol, Src Port: 50213, Dst Port: 1813
v RADIUS Protocol
    Code: Accounting-Request (4)
    Packet identifier: 0xad (173)
    Length: 47
    Authenticator: 391a8b9e7fc6e41e62b759c3f3906065
    [The response to this request is in frame 260]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=7 val=sumit
    > AVP: t=Framed-IP-Address(8) l=6 val=172.31.128.30
    > AVP: t=Class(25) l=8 val=67726f757031
    > AVP: t=Acct-Status-Type(40) l=6 val=Start(1)
```

Radius debug

Received radius accounting eventvd 0:root Add/Update auth logon for IP 172.31.128.30 for user sumit DB 0 insert [ep='sumit' pg='group1' ip='172.31.128.30/32'] success

aegon-kvm16 # diagnose firewall auth list

172.31.128.30, sumit type: rsso, id: 0, duration: 13, idled: 13

    flag(10): radius server: root

    packets: in 0 out 0, bytes: in 0 out 0

    group_id: 3

    group_name: RS

----- 1 listed, 0 filtered ------

#Developed by Sumit Thapa

Emai Address : thapa.sumit6@gmail.com

Follow linkedin: https://www.linkedin.com/in/sumit-thapa-99a75996/

#Follow Github : https://github.com/sumitthapa/RadiusPacketGeneratorToolKit