

[illegible]

Name	DNS: DNSSEC Enabled
URL	https://www.attackdefense.com/challengedetails?cid=236
Type	Network Recon : DNS

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. What is the key ID of key signing key of witrap.com ?

Answer: 47466

Command: dig DNSKEY witrap.com +multiline @192.204.191.3

;; ANSWER SECTION:

witrap.com.

```
86400 IN DNSKEY 257 3 7 (  
  AwEAAbtM3NZHtVK+rrzBY0OVTf50V6WogTSPEhzVeNdv  
  qQnjDzawTJSUgzzmkNSII1BkMuuI4QwLXGy0ZZgg9/lf  
  zGWHzCpC6uEV8BrNKT2+04TgJ48/LAGiNi/qRRc2jUQp  
  EMo5tSnXWMDoc56C2n2g0Wq521pdiPskTWe4lwNbE4cG  
  GSwWvnnY+0QFJInYDv7vR5MSnQUyG1FfTTW6WX16fvyN  
  QMPJAiTbnqyNP2+GkjWX+5xm+rtp91hTEvKQONTsYryL  
  Yh1FdzkSMFbBD8Rz+6Eu7Cxc3BJknBysxRA2AKmWaGD8  
  0HLSM3d1p920p4iC6YwhZ02HmjMxzcZzGZzm9BTyNfcfy  
  HDxa7Qp4L2oF7h8aNCPgNB4Y70vM8UH6huejOHgR6Wkk  
  aOGwX8Ds3oKYWRhuyTael99EmsAfCiCyb0c2a0I4nwoh  
  t6XE9XEJHx5gxCXnH6MSQYrJmOzU1jefnoDcEOhiX07n  
  Ss1TiUun482Ch3rHK9vCYPfGwhrLsYzGRRGtWZA87GST  
  CMFKCGvPzRPaB8Nj1o9TASJ9pQ2UGk8enAbYg6RSUtDb  
  zMv8t10faGt1dkZgrFeWkuA5I+Q0uSmBFceMgEsRdJgJf  
  TQ8WwkJ9wS1bemPRJYK7yhne0bt/x7LLkyzWmcWoYnxL  
  BbR0ExESGKVurMzfHlCYtwFivhP3  
  ) ; KSK; alg = NSEC3RSASHA1 ; key id = 47466
```

witrap.com.

```
86400 IN DNSKEY 256 3 7 (  
  AwEAAc/J2KXA4dkUSBce20Mm+hbWUfZpWJ7lAyDDafC0  
  VovbYE/ROEIiOURFcN1yZfjWE550tupRHx6rqq8eNEov  
  sb8ELB8BXVqNhr/b/ilgq6cKzuTFC+vCMbdfHKj/swdp  
  2DNEFtr+30jPz5jGa4JrN15j5/L02vrcRbb3VUDVyu8m  
  mSMUq1AozTkqHiFb490Qk5tPrHvd9Hu19NTAxlcfy4UY  
  63Zj4I7+KfuTPkt4ENdLyIqy4jXhp7cQ2uZCzOp2tJge  
  dC6Vmd9vP1sdUwuv3wRy4PBaVtM0VhMtacISfWxG4qyJ  
  VqcOVwl6Pa4pfIeRtYp7J9EV4/29M7yWS2POL3E=  
  ) ; ZSK; alg = NSEC3RSASHA1 ; key id = 47204
```

Q2. What is the algorithm used for to create KSK and ZSK for witrap.com ?

Answer: NSEC3RSASHA1

Command: dig DNSKEY witrap.com +multiline @192.204.191.3

;; ANSWER SECTION:

witrap.com.

```
86400 IN DNSKEY 257 3 7 (  
  AwEAAbtM3NZHtVK+rrzBY00VTf50V6WogTSPEhzVeNdv  
  qQnjDzawTJSUgzzmkNSII1BkMuuI4QwLXGy0ZZgg9/lf  
  zGWHzCpC6uEV8BrNKT2+04TgJ48/LAGiNi/qRRc2jUQp  
  EMo5tSnXWMD0c56C2n2g0Wq521pdiPskTwe4lwNbE4cG  
  GSwWvnnY+0QFJInYDv7vR5MSnQUyGlfTTW6WX16fvyN  
  QMPJAiTbnqyNP2+GkjWX+5xm+rtp91hTEvKQONTsYryL  
  Yh1FdzkSMFbBD8Rz+6Eu7Cxc3BJknBysxRA2AKmWaGD8  
  0HLSM3d1p920p4iC6YwhZ02HmjMxzcZzGZzm9BTyNfCfy  
  HDxa7Qp4L2oF7h8aNCpGNB4Y70vM8UH6huejOHGr6Wkk  
  aOGwX8Ds3oKYWRhuyTae199EmsAfCiCyb0c2a0I4nwoh  
  t6XE9XEJHx5gxCXnH6MSQYrJmOzU1jefnoDcEOhiX07n  
  Ss1TiUun482Ch3rHK9vCYPfGwhrLsYzGRRGtWZA87GST  
  CMFKCGvPzRPaB8Nj1o9TASJ9pQ2UGk8enAbYg6RSUtdb  
  zMv8t10faGt1dkZgrFwkuA5I+Q0uSmBFceMgEsrdJgjf  
  TQ8WwkJ9wS1bemPRJYK7yhne0bt/x7LLkyzWmcWoYnxL  
  BbR0ExESGKVurMzfHlCYtwFivhP3  
  ) ; KSK; alg = NSEC3RSASHA1 ; key id = 47466
```

witrap.com.

```
86400 IN DNSKEY 256 3 7 (  
  AwEAAC/J2KXA4dkUSBce20Mm+hbWUfZpWJ71AyDDafc0  
  VovbYE/ROEIiOURFcn1yZfjWE550tupRHx6rqq8eNEov  
  sb8ELB8BXVqNhr/b/ilgq6cKzuTFC+vCMbdFHKj/swdp  
  2DNEFtr+30jPz5jGa4JrN15j5/L02vrcRbb3VUDVyu8m  
  mSMUqlAozTkqHiFb490Qk5tPrHvd9Hu19NTAx1cfy4UY  
  63Zj4I7+KfuTPkt4ENDLyIqy4jXhp7cQ2uZC0p2tJge  
  dC6Vmd9vP1sdUwuv3wRy4PBaVtM0VhMtacISfWxG4qyJ  
  VqcOVw16Pa4pfIeRtYp7J9EV4/29M7yWS2P013E=  
  ) ; ZSK; alg = NSEC3RSASHA1 ; key id = 47204
```

Q3. What is the RRSIG A Record of witrap.com ?

Answer:

oheCda/JJITjPDYoskGh/YW+o8Tixx0hAHs0UtMPy91o6vZttrL0SA/5LLmYgmTwMioBq2fhPm19
tX4NBdBec/HRHNad/yKmZYp/kC/qQMeSthg1kKPOKrvKvtbMvW7tmMXRjaVTFIQADg2/gCnPf
p8PkwwSmcJMWTS0h0ivbnoUXARddTPMY5Gnaxy2CxQK3cBHsjVnBosmChHqabNUdPPqP+
X53fdQ4z2GxYkO9Y4KmVLbljYnb45TI+J1IL4nLxChglXXL7Fzs7bziwR8bsWD0IXaJWha1MF8
R9u9USS+CQzGhtOIWcZikY3RxXrBu+PmrJcHx7TaObsLgXw==

Command: dig A witrap.com +multiline @192.204.191.3 +noadditional +dnssec +multiline


```

root@attackdefense:~# dig A witrap.com +multiline @192.204.191.3 +noadditional +dnssec +multiline

; <<>> DiG 9.11.4-4-Debian <<>> A witrap.com +multiline @192.204.191.3 +noadditional +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35383
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;witrap.com.                IN A

;; ANSWER SECTION:
witrap.com.                86400 IN A 192.168.60.2
witrap.com.                86400 IN RRSIG A 7 2 86400 (
                             20181120150154 20181021150154 47204 witrap.com.
                             oheCda/JJlTjPDYoskGh/YW+o8Tixx0hAHs0UtMPy91o
                             6vZttrL0SA/5LLmYgmTwMioBq2fhPm19tX4NBdBec/HR
                             HNad/yKmZYp/kC/qqMesthhg1kKPOKrVKvtbMvW7tmMX
                             RjaVTFIQADg2/gCnPfp8PkwwSmcJMwTS0h0ivbnoUXAR
                             ddTPMY5Gnaxy2CxQK3cBHsjVnBosmChHqabNUdPPqP+X
                             53fdQ4z2GxYk09Y4KmVLbljIYnb45Tl+J1lL4nLxCHgI
                             XXL7Fzs7bziwR8bsWD0lXaJWha1MF8R9u9USS+CQzGht
                             OIWcZikY3RxXrBu+PmrJcHx7Ta0bssLgXw== )

```

Q4. What is the Salt used for hash Calculation for NSEC3?

Answer: DBF4725BEF433A41

Command: dig NSEC3PARAM witrap.com @192.204.191.3

```

root@attackdefense:~# dig NSEC3PARAM witrap.com @192.204.191.3

; <>> DiG 9.11.4-4-Debian <>> NSEC3PARAM witrap.com @192.204.191.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39532
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;witrap.com.                IN      NSEC3PARAM

;; ANSWER SECTION:
witrap.com.                 0       IN      NSEC3PARAM 1 0 10 DBF4725BEF433A41

;; AUTHORITY SECTION:
witrap.com.                 86400   IN      NS       ns.witrap.com.
witrap.com.                 86400   IN      NS       ns2.witrap.com.

;; ADDITIONAL SECTION:
ns.witrap.com.              86400   IN      A        192.168.63.4
ns2.witrap.com.             86400   IN      A        192.168.67.14

```

Q5. How many RRSIG records exists for witrap.com ?

Answer: 11

Command: dig RRSIG witrap.com +short @192.204.191.3


```

root@attackdefense:~# dig RRSIG witrap.com +short @192.204.191.3
SOA 7 2 86400 20181120150154 20181021150154 47204 witrap.com. Je4u3kbWJrLNH3AMiKAYZDG5qb81UJGRx2Fp7JFRJib5rUxxXNaIaNZE pB7bXG/UdJIEiJjTrVttJ8Mg
sWH3V9wpmw1ZxZGq91G14jJrVx4nuG/S H4EZ865GA9rh78KOWZ8MA3DKThJ1/3FFZ0BhJufJBeppRev0g5QKhip PJ51eA3/a+F010JUGNk1kHCBgJ7P197BzppMHNNe28UFEloB6SgoG
whO rSUV5GxUA6keBGnaFh+CICQSKJ8AKUbbvanrI9pkNvduQntz0TrE9XW S/SifdgnJc7ssiHtnLr/1ZQv1vfGbE5oJkLX18DJ+e3r2wvWosAn0hmQ pZMRVw==
NS 7 2 86400 20181120150154 20181021150154 47204 witrap.com. vH0aJMa1lHeMcffIP6VvBoHkQUjRtsnRwFxeQaoqesyKAgSMOXGDPjGD kt0Dqk3LGtystMqC/ZMWgZJGy
im2jPJjN9/vry47AUfUQe5maXn3vA5U Urj+VJEaX3Q1C6Cot188GXHHAJxFetHcA8U7Tii8Ic91isuuUuLcat N9Yax/BAVJ65xRE4MV2LkqzngffocVjo2QOPBB9TLvitpf9sklspY
Ix m7XCRJ9ZPRAOLu1Wd6U/q0xkE7MG28mw1e1b088+XPCJYB4eEnji7aDe0 PwwRK5zTFX6iVwyqVt14VpilaUX/8aeByfLKCONZEDwmstrtAcWa4UpX 910g7w==
A 7 2 86400 20181120150154 20181021150154 47204 witrap.com. oheCda/JJlTjPDYoskGh/Yw+o8Tixx0hAhs0UtMPy91o6vZttrL0SA/5 LLmYgmTmMioBq2fhPm19tX4Nbd
Bec/HRHNad/yKmZyp/kc/qQmesthgh 1kKPOkrVKvtbMvW7tmMXRjAvTFIQADg2/gCnPfp8PkwwSmcJMTWS0h0i vbnoUXARddTPMY5Gnaxy2CxCQK3cBhsjVnBosmChHqabNudPPqP+X53f
d Q4z2GxYk09Y4KmVlBljIYnb45Tl+J11L4nLxCHgIXXL7Fzs7bziwR8Bs WD0lXaJWha1MF8R9u9USS+CQzGhtOIWcZikY3RxxRBU+PmrJcHx7TaOb sSLgXw==
MX 7 2 86400 20181120150154 20181021150154 47204 witrap.com. QX0T7yjc8VbalWM6Ucso+03Zoiu5ibmyryKxgXICT/Bz54buBtuf5Mf qWRaE2LEqwhvEecc7WENR6j7N
YN90S9dCMAutFpN6GjKJQ6oSR0/gsc1 NvThyu7gqEel/8PAMugIc//Vhb/wHT2J7umx4AmYl1vtznM5sJ6X1LzS G1VatliwB+LJRky0TjhnAGBLJccLP33DK2H/UAFKFNK/SJ0XBn4UTZ
0E xg5vyTTAnrPibV74kSwfm55ahi7eHvm/nMS7/zW+ARB3Fcwiq610q7N3 dfzQgFWPMZW/rGPNr3iMwZV3Jq4J6D3EZcV3iGZM7Rdd2XewUIRQpZ4m J/+R2Q==
TXT 7 2 86400 20181120150154 20181021150154 47204 witrap.com. UCuzhWRGvsLFD0S3mCBxKsVwMUTa6WbiKHL6B5dyMrPv3pzcbMRxji IurOswr70Pjfiu0uXm+nf0Q
npUZYQLH56Ks3y1AJjz5W0hPbjnNgcH9 Ehd2stojKlQkewXRdp2XjKGLGQ6KU3HA6/aDBruxVhh4z9z3rI8sMrbX jISK1huU8H8Igc8C/95mhlyOXBJzNARIyz7tiLfbLjAXZV+Bv36GwA
fEq /thU/DGQumNnq7J0brGNd4UARQss0shQ54vG9b4gOUKfujjsU6+4u+SM gYLGWJIEZKowRomvIPrJ06QE4KPD8JqpXjIPLKQEFteNS9EB6odxP+ cMYe0g==
AAAA 7 2 86400 20181120150154 20181021150154 47204 witrap.com. PXfPbMJXDz5PuLS7PBAR6SnYsd9LMGT2t0ra0Z4dxc8K0Imcga04QG JdIP2m+6jUJBtjgb4KIKYtu
iffkrmWjgr6B+33PWsQowI9yVwIitM4L dw1UKleJ18c35R6mJo9T64/bqZSUyhKT2uU+GsRtoL40phXyHs0IQvRK TJYINwto1iyX+E099c60a1C0FzjIFbvYUCCwphMn1ujlyCtd0UW
Wuy/ 3jd5K31VoYSw0t5hr3t5zLum0RfVvHYwTsg9I1WYi6PBLKTojgKnH/F UscQSWHl0cEaJeXetsS24TAd3ev2NZpaxgHI10ZNX5v3oK7QS2oVlk3y lw0PgW==
LOC 7 2 86400 20181120150154 20181021150154 47204 witrap.com. fPrC6pQBORHZV4SBUx+Pvh3wi1nc14zVJIMJUHqYdlnKk3/AoKnBj3Uk P1nH9PGeieim19QeyMLdei1q
ACOR2SP07A58u8Vv7qFsrBHC1QqNBHy 5Eht1f7qu1RWG70CnAgd18e3+kXwo56xjyhUm/pb46ccw692bihF9HDg QJ8pwIH7kYsYk8PbaMR6ADqhhd/j+c9xwLhtxRiITv51Q5Ioinc
x3X gSeZztbT46igTAZJ6tEsgrEnPvm+9CjaE+vfGtLp/d3mdMYRppSzwSR 3NXc9+2txrb715WrjTeAVTnTD+7rsBqDAZBSAHVgtmEh3ZB3+x6pqhCa Qtf4xg==

DNSKEY 7 2 86400 20181120150154 20181021150154 47204 witrap.com. quZLXwrOX7hxcPhhIY20VcNzE15xP7p7HLJHmH64D/rHPDw7jtzt/tc1K zgeyQdA+PgS0Pugi8v9u1
jZR66B9KCLZHxwGe+15u2wDvdU0iTF1QL4 tq1Sp2os0A/FVRGfjh51bFKsgCavnWytSZQFtdvSA/0UXntNqu8ihpXj KY3cvwgC0zb2x25irwY7VxZtNmWIoZetKvXtEgj+UagGJQisR
2iNvVv 8roBbAmGiwrJCl19ezmQAOmZQ+Bf/JyFbHFBGABpIyP0J/MSs2zawYRC iHMMvF20oSvGwY+AgaeZbPR4Pp1kYqnKBG4y1LIpH9LxXZVaoR9EiI2Y Z5/O4g==
DNSKEY 7 2 86400 20181120150154 20181021150154 47466 witrap.com. A8kFmJ0mqrXMR+QZGbXfWnyf4jHqV4+F3iPAON+mXH+A6z5Ba3dCaTXi oBgxJK8WdcDzqOuPcYjfc
mu7EqE7v1/I/RXbLe0ckmaKSL/tsEvDvG2X 1U8d2HTMSgxdMzzqRWEInQ2A0CnazyHDUNHAXfg/DpcoXuhgKOPkfZE3 hazetFGUmd/IoAjju0955F5dkTkyXl9+/GzKh39uGkrM3rdD9GK
SRr+Js CsatJvx74CBPJ7AQNHCRHsmuhrIhACBpVh6/nG5S8B/CvmyQ/qtyNBKS EHUVae9fgRvMNeXmxhF5L2M1qneJCnvjR0SMHwEaeUiR6rkZHKDbA84 NgVj5mH7RAXHHRsMPMIAX
zos1iFdIThLk+KdZocotetM4+qv7BcPEAp n8egRADyRFQrXnUfknk8kyu5Y19FWsuqNZX7XjRdD2UYXtUehP7fsmXb ZRws3oPGK0Y4LttHgBC0kKqBZgk/L9q+1q2ZBASCyobzZzUcCm
QcdJZ GL2foZt2Dy14AlWu/mUGKQ9gPKEKxPqe6vVWj+JumRQqL4L6C0PO/csn YcAjMIBZM7pcRyzuWHDc95B93RahxCVG0ZgFk2jpqOhTsr4tDExTseP2 hMag8Rkr74T2TK2d3MDC4bX
Z5e4MbdIHghz7J22pSGarZ8jXqQI91cH 9gifFY/9q30=
NSEC3PARAM 7 2 0 20181120150154 20181021150154 47204 witrap.com. CRJZvX00vxa855N+/sj+XcyVRfyzFqz/OY96aK9J1HERgrV5Afn+turj zkpV6W0IHJDr4aPjS61b4
3jXexx2bBrY0aa57/mtmk7HQcz8ef/ivdGr TfLCCgPnUqM17Gk325tnEq3roF2+qb8U30F2KiCxpMr5nbUBUJz3fxj QK3yLggrXA2g9uMF6R+cyH+OGoBcIefJ19wTOGTGNm21G+BFtF
BngcyY OpopbGWLWwJNV3pD4PQ654J8RJhgZDaLpS9VMzIQjyjiff1bdtiDaYVK 2cW0F6/ugg1tm9b8K7/TMHauDwApIRvftGgIB5y3zgFji/4HI/B5KYw2 Mf7ShA==
CAA 7 2 86400 20181120150154 20181021150154 47204 witrap.com. Cvsr2Tm3HGkXoOeYPqzGkMumcCwCgXaReN7QNZqY9utLs7FSy5Jf3vNj 4XeX/qS02/Rtyrk0Ej3h7sG
Iy0C+gXaD05fiPgqKkBoAczsDpG371Rz IJTmebbqLu4G2Kb8MGLsVb2VWZ8Eo0x8BMovEduP6uMDYqC85g8NZfrmj S5JB0/31TwbW3GkTSCZ/mYfJg8m41S4V1LoKcrSdzPP6Vah1SH/Bo
hyc kaMpd2VT4h3kaCbP/elt+mHNbpdRfVfhzjPfG0tKDFdpbZf3jYGMCHS Wc2LGHH5TricjVwOZzEsL2BftoGNV8A0Bldx9oW57lgBdxYwH0BbgBjC G0nhJA==

```

References:

1. Bind 9 (<https://www.isc.org/downloads/bind/>)
2. nslookup (<https://linux.die.net/man/1/nslookup>)
3. dig (<https://linux.die.net/man/1/dig>)