Name: Shreya Singh Id: 2022pct0019

ASSIGNMENT: 3 DNSSEC

DNSSEC validation for a given domain name using Verisign labs.

Domain: raspberrypi.org

Domain Name: raspberrypi.org

Analyzing DNSSEC problems for raspberrypi.org

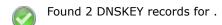
	Found 2 DNSKEY records for . DS-20326/SHA-256 verifies DNSKEY-20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG-20326 and DNSKEY-20326/SEP verifies the DNSKEY RRset
org	Found 1 DS records for org in the . zone DS=26974/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=46780 and DNSKEY=46780 verifies the DS RRset Found 3 DNSKEY records for org DS=26974/SHA-256 verifies DNSKEY=26974/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=26974 and DNSKEY=26974/SEP verifies the DNSKEY RRset
raspberrypi.org	Found 1 DS records for raspberrypi.org in the org zone DS-2371/SHA-256 has algorithm ECDSAP256SHA256 Found 1 RRSIGs over DS RRset RRSIG-61110 and DNSKEY-61110 verifies the DS RRset Found 2 DNSKEY records for raspberrypi.org DS-2371/SHA-256 verifies DNSKEY-2371/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG-2371 and DNSKEY-2371/SEP verifies the DNSKEY RRset tony.ns.cloudflare.com is authoritative for raspberrypi.org raspberrypi.org A RR has value 172.67.36.98 Found 1 RRSIGs over A RRset RRSIG-3450S and DNSKEY-3450S verifies the A RRset
raspberrypi.org	 april.ns.cloudflare.com is authoritative for raspberrypi.org raspberrypi.org A RR has value 104.22.0.43 Found 1 RRSIGs over A RRset RRSIG-34505 and DNSKEY-34505 verifies the A RRset

Move your mouse over any $\ensuremath{\mathbf{8}}$ or $\ensuremath{\mathbf{\Delta}}$ symbols for remediation hints.

W-4 - ---- 7 T-4 ---- -- -- -- -- 4--- --

Step 1: Root server : - [.]

dig +dnssec DNSKEY . @8.8.8.8

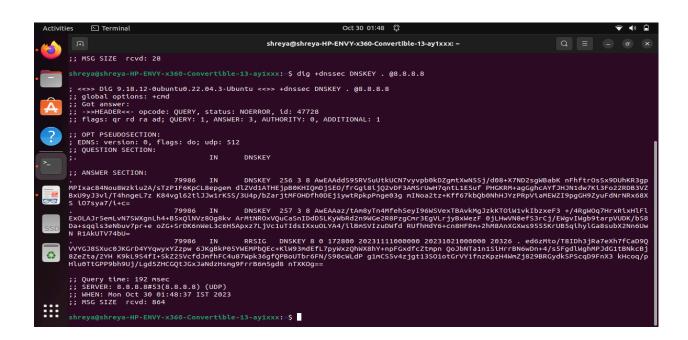


DS=20326/SHA-256 verifies DNSKEY=20326/SEP

Found 1 RRSIGs over DNSKEY RRset

RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset

It is giving DNSKEY of root . here there are two DNSKEY first one is ZSK and second one is KSK .



Step 2: Top level domain server :-(com)

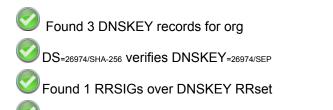
dig +dnssec DNSKEY com @8.8.8.8

Found 1 DS records for org in the . zone

OS=26974/SHA-256 has algorithm RSASHA256

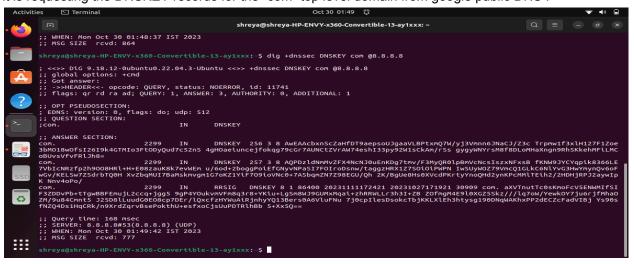
Found 1 RRSIGs over DS RRset

RRSIG=46780 and DNSKEY=46780 verifies the DS RRset



It is requesting the DNSKEY records for the "com" top level domain from google public DNS.

RRSIG=26974 and DNSKEY=26974/SEP verifies the DNSKEY RRset



Step 3: dig +dnssec com. DS @8.8.8.8 Requesting DS(Delegation signer) record for the "com" TLD server from google public DNS server .

```
hreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:~$ dig +dnssec com. DS @8.8.8.8
  <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> +dnssec com. DS @8.8.8.8
;; global options: +cmd
 ; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38233
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
  EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
                                                      DS
;; ANSWER SECTION:
                                81581
                                           IN
                                                                  30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CF C41
com.
com. 81581 IN RRSIG DS 8 1 86400 202311110500000 202310290400000 46780 . wD83D0CF+Gbwle3F1Xax
S3Hjiy6aUwIPOLBT3LWc+7X LcCjijtSWLU6J+r0yILBFVzBX/zjiPxFUTXNEkhVjz8kxwZFG8nkcP1B Uw+JX/TG+NxarQyo6ljbzZXwGTvU2tZKDuiG1
RTzoc F3lyTO+0NR17bLIQbSlnZKq+PnX9vQXm6jdQqwmJojuub8pERah513HS REaGAe7nOy2g9wb6K8HtVoUrT771AbQlu/pRMR3UnNbJ12fqCbWoW0f
30VnAmy/61W5l1/XPUSeYp8BTczFoubgwQ8RXjh72MVo cH/ODg==
;; Query time: 156 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
   WHEN: Mon Oct 30 01:50:43 IST 2023
;; MSG SIZE rcvd: 367
```



DS=2371/SHA-256 has algorithm ECDSAP256SHA256

Found 1 RRSIGs over DS RRset

RRSIG=61110 and DNSKEY=61110 verifies the DS RRset

Found 2 DNSKEY records for raspberrypi.org

DS=2371/SHA-256 verifies DNSKEY=2371/SEP

Found 1 RRSIGs over DNSKEY RRset

RRSIG=2371 and DNSKEY=2371/SEP verifies the DNSKEY RRset

april.ns.cloudflare.com is authoritative for raspberrypi.org

raspberrypi.org A RR has value 104.22.0.43

Found 1 RRSIGs over A RRset

RRSIG=34505 and DNSKEY=34505 verifies the A RRset

DNSKEY record for the raspberrypi.org domain from google public DNS server .

```
hreya@shreya-HP-ENVY-x360-Converttble-13-ay1xxx:-$ dig +dnssec DNSKEY raspberrypi.org @8.8.8.8
; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> +dnssec DNSKEY raspberrypi.org @8.8.8.8;; global options: +cmd
 ; Got answer:
,, duct answer.
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26677
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
                                                    DNSKEY
;raspberrypi.org.
                                          IN
 ; ANSWER SECTION:
raspberrypi.org.
iUzy1L53eKGQ==
                               3600
                                          IN
                                                    DNSKEY 257 3 13 mdsswUyr3DPW132mOi8V9xESWE8jTo0dxCjjnopKl+GqJxpVXckHAeF+ KkxLbxILfDLUT0rAK9
raspberrypi.org.
1x8fGAa2XhSA==
                               3600
                                          IN
                                                    DNSKEY 256 3 13 oJMRESz5E4gYzS/q6XDrvU1qMPYIjCWzJaOau8XNEZeqCYKD5ar0IRd8 KqXXFJkqmVfRvMGPmM
raspberrypi.org. 3600 IN RRSIG DNSKEY 13 2 3600 20231205040123 20231005040123 2371 raspberrypi.org. rCU7MmQPa8hSmcj
AqoDqypnxFBVr/rct9t969Z1JmK8pz7Cm4Xgu4mrF 4JkpiBSrAfdRjY7ti/o+FDsaH1pbxQ==
   SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
WHEN: Mon Oct 30 01:52:12 IST 2023
  MSG SIZE rcvd: 315
```

Step 5: dig +dnssec DNSKEY raspberrypi.org DS @8.8.8.8

Performing queries for the DNSKEY records and another for the DS record for raspberrypi.org domain from Google public DNS server.

```
shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:-$ dig +dnssec DNSKEY raspberrypi.org DS @8.8.8.8
;; Warning, extra type option
; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> +dnssec DNSKEY raspberrypi.org DS @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 59332
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
raspberrypi.org. IN DS
;; ANSWER SECTION:
raspberrypi.org. 3600 IN DS 2371 13 2 6984AB832CEC75FC12324E60859BB6100AF26D797F0D06468C802EA8 D71E522A
raspberrypi.org. 3600 IN RRSIG DS 8 2 3600 20231115152550 20231025142550 61110 org. GSe7TAEXMSVQcaiXMtAETP9DUUIpMkW
t7ZzpP8X6+E6rDillXlDDsiMG w0L3fBtpRc2CSTrPGEqYPPLB1BatB+NrSgcGMP+pICmkXZWJLKwzBCDD Nyv/Z0o7YrK17Cvo9gDHDwA1YvxYU3kgL9Aomr56HlWG+hXPk
RDSA9nX SqQ=
;; Query time: 332 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Oct 30 01:53:09 IST 2023
;; MSG SIZE rcvd: 255
```

Step 6: dig +dnssec raspberrypi.org @8.8.8.8

It will retrieve RRSIG and DNSKEY records for raspberrypi.org.

```
shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:-$ dig +dnssec raspberrypi.org @8.8.8.8

; <<>> DiG 9.18.12-@ubuntu@.22.@4.3-Ubuntu <<>> +dnssec raspberrypi.org @8.8.8.8

;; global options: +cmd
;; Got answer:
;; ->>HEADER<-<- opcode: QUERY, status: NOERROR, id: 63711
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
raspberrypi.org. IN A

;; ANSWER SECTION:
raspberrypi.org. 300 IN A 172.67.36.98
raspberrypi.org. 300 IN A 104.22.1.43
raspberrypi.org. 300 IN A 104.22.1.43
raspberrypi.org. 300 IN RRSIG A 13 2 300 20231030212912 20231028192912 34505 raspberrypi.org. Km3Ib1+aZXF28d11Ukuz
rwhNAZ8JHBBGWJF5668w@Qn/x/O8L2T97X22 Z2bDuShKNv3cxq1xlJ900RXdIOdICA==

;; Query time: 60 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Oct 30 01:59:12 IST 2023
;; MSG SIZE rcvd: 203
```