**Workbook of Session 3**

**تمرین 2 : DNS Over Https چیست و چگونه در ویندوز پیاده سازی می شود؟**

DNS-over-HTTPS ترکیبی از دو فناوری است. اولین فناوری [DNS](https://rokida.com/110857-%d8%a2%db%8c%d8%a7-%d8%aa%d8%ba%db%8c%db%8c%d8%b1-%d8%af%d8%a7%d8%af%d9%86-%d8%b3%d8%b1%d9%88%d8%b1-dns-%d9%84%d8%a7%d8%b2%d9%85-%d8%a7%d8%b3%d8%aa/) (سرویس نام دامنه) و دومی پروتکل انتقال ابرمتن امن (HTTPS) است.

یعنی ارسال درخواست DNS بر روی HTTPS به جای HTTP. این یعنی هیچ شخص یا نهادی از بیرون قادر به مشاهده سایت‌هایی که از آنها بازدید می‌کنید نیست.

این ارتباط هم به طور کامل امن نیست – سرور DNS باید درخواست را کدگشایی کند تا سوال شما را تشخیص دهد. در این مرحله، ارائه دهنده سرور DNS می‌تواند درخواست‌های کاربران را ثبت کند تا مشخص شود که چه کاربری از چه سایتی بازدید کرده است اما به غیر از شما و ارائه دهنده سرویس DNS دیگران قادر به تحلیل و بررسی عادات وبگردی شما نیستند.

پیاده سازی در ویندوز:

در فایرفاکس به شرح زیر پیاده سازی می شود:

1. About: config
2. **network.trr.mode**
3. **تایپ گزینه مورد نظر :**

* 1 یعنی که DoH فعال باشد ولی فایرفاکس بین DNS معمولی و DoH هرکدوم که سریع تر بود رو استفاده می کند
* 2 یعنی که DoH فعال باشد و DNS معمولی به عنوان بکاپ کار کند
* 3 یعنی DoH فعال باشد و DNS معمولی غیر فعال باشد
* 5 یعنی که DoH غیر فعال باشد.

1. و یا می توانیم بگوییم از DNS-server گوگل و یا cloudflare استفاده کند:

<https://mozilla.cloudflare-dns.com/dns-query>

<https://dns.google/dns-query>

1. با تغییر **network.trr.bootstrapAddress می توانیم IP سرور DOH را اضافه کنیم.**

تمرین 3: DNS Tunneling

فراگیر بودن DNS می تواند روش های ظریفی را برای برقراری ارتباط و به اشتراک گذاری داده ها فراتر از اهداف پروتکل فعال کند. مجرمان سایبری می دانند که DNS به طور گسترده مورد استفاده قرار می گیرد و افراد به آن اعتماد می کنند. همین امر نشان دهنده اهمیت اقدامات امنیتی DNS است. علاوه بر این، از آنجا که DNS برای استخراج داده ها استفاده نمی شود، بسیاری از سازمان ها بر ترافیک DNS خود جهت جلوگیری از فعالیت های مخرب، نظارت نمی کنند. در نتیجه، تعدادی از انواع حملات مبتنی بر DNS می توانند علیه شبکه های شرکت استفاده شوند. DNS Tunneling یا "تونل سازی DNS" یکی از این حملات است.

**عملکرد DNS Tunneling چگونه است؟**

حملات تونل سازی DNS از پروتکل DNS برای افزودن بدافزار و سایر داده ها از طریق مدل سرور-کلاینت، سوء استفاده می کنند.

1. مهاجم دامنه ای مانند example.com را ثبت می نماید. نام دامنه به سرور مهاجم اشاره می کند، جایی که یک بدافزار تونل سازی نصب شده است.
2. مهاجم کامپیوتری را که اغلب پشت فایروال یک شرکت قرار دارد، با بدافزار آلوده می کند. از آنجایی که درخواست‌های DNS همیشه مجاز به جابجایی و خروج از فایروال هستند، رایانه آلوده مجاز است درخواستی را به "مترجم DNS" یا DNS resolver ارسال کند. DNS resolver سروری است که درخواست‌های آدرس IP را به سرورهای دامنه اصلی و سطح بالا ارسال می‌کند.
3. DNS resolver کوئری را به سرور تحت کنترل مهاجم هدایت می کند، جایی که برنامه تونل سازی نصب شده است. اکنون ارتباطی بین قربانی و مهاجم از طریق DNS resolver برقرار شده است. از این تونل می توان برای استخراج داده ها یا سایر اهداف مخرب استفاده کرد. از آنجایی که هیچ ارتباط مستقیمی بین مهاجم و قربانی وجود ندارد، ردیابی رایانه مهاجم دشوارتر است. نمودار زیر نحوه عملکرد DNS Tunneling را نشان می دهد.

DNS tunneling تقریباً 20 سال است که وجود دارد. دو بدافزار Morto و Feederbot برای تونل سازی DNS استفاده می شوند. حملات اخیر تونل سازی توسط این بدافزارها، مربوط به گروه DarkHydrus می شود که نهادهای دولتی خاورمیانه را در سال 2018 هدف قرار داد و هنوز فعال است.

**جلوگیری از DNS tunneling**

DNS ابزار بسیار قدرتمندی است که تقریبا همه جا مورد استفاده قرار می‌گیرد و به برنامه‌ها و سیستم‌ها اجازه می‌دهد منابع و سرویس‌هایی را جستجو کنند که با آنها تعامل دارند. DNS یک پایه ارتباطی را فراهم می کند که پروتکل های سطح بالاتر و قدرتمندتر را قادر می سازد تا فعالیت کنند. با این حال ممکن است از نظر امنیتی نادیده گرفته شود، به خصوص زمانی که بدافزار از طریق پروتکل های ایمیل منتشر شده یا با استفاده از HTTP دانلود می گردد. به همین دلیل، DNS برای دشمنانی که به دنبال یک پروتکل همیشه در دسترس و نادیده گرفته شده هستند، گزینه مناسبی است.

سازمان‌ها می‌توانند به روش‌های مختلف مانند استفاده از پلتفرم های امنیت شبکه یا فناوری های متن باز، در برابر عملکرد DNS Tunneling از خود دفاع کنند. این نوع دفاع می تواند اشکال مختلفی داشته باشد، برخی از آنها در ادامه آورده شده اند:

- مسدود کردن نام های دامنه، IP ها یا مناطق جغرافیایی بر اساس سابقه قبلی یا احساس خطر کردن.

- قوانین مربوط به کوئری های جستجوی DNS با ظاهری عجیب.

- قوانین مربوط به طول، نوع یا اندازه کوئری های DNS خروجی و ورودی.

- تجزیه و تحلیل رفتار کاربر یا سیستم که به طور خودکار ناهنجاری‌ها را شناسایی می‌کند. مانند زمانی که دامنه‌های جدیدی با روش دسترسی و فرکانس غیرعادی، قصد اتصال دارند.

تمرین 8 : 5 IRAN NAS on Shodan

[91.238.0.4](https://www.shodan.io/host/91.238.0.4)

* 91.238.0.soratgostar.net
* [Sorat Gostar Abr Datis LLC](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+org%3A%22Sorat+Gostar+Abr+Datis+LLC%22)
* https://www.shodan.io/static/flags/16/IR-caec555e.png[Iran, Islamic Republic of](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+country%3A%22IR%22), [Tehran](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+city%3A%22Tehran%22)

\xc8\x02\x00m\x00\x00\x00\x00\x00\x00\x00\x01\x80\x08\x00\x00\x00\x00\x00\x02\x80\x08\x00\x00\x00\x02\x01\x00\x80\n\x00\x00\x00\x03\x00\x00\x00\x01\x80\n\x00\x00\x00\x04\x00\x00\x00\x00\x00\x08\x00\x00\x00\x06\x00\x01\x80\x17\x00\x00\x00\x07ImamDC-**NAS**-6.48.6\x00\x0e\x00\x00\x00\x08MikroTik\x80\x0...

2024-02-18T00:58:30.456391

[91.237.254.1](https://www.shodan.io/host/91.237.254.1)

* 91.237.254.soratgostar.net
* [Sorat Gostar Abr Datis LLC](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+org%3A%22Sorat+Gostar+Abr+Datis+LLC%22)
* https://www.shodan.io/static/flags/16/IR-caec555e.png[Iran, Islamic Republic of](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+country%3A%22IR%22), [Tehran](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+city%3A%22Tehran%22)

\xc8\x02\x00m\x00\x00\x00\x00\x00\x00\x00\x01\x80\x08\x00\x00\x00\x00\x00\x02\x80\x08\x00\x00\x00\x02\x01\x00\x80\n\x00\x00\x00\x03\x00\x00\x00\x01\x80\n\x00\x00\x00\x04\x00\x00\x00\x00\x00\x08\x00\x00\x00\x06\x00\x01\x80\x17\x00\x00\x00\x07ImamDC-**NAS**-6.48.6\x00\x0e\x00\x00\x00\x08MikroTik\x80\x0...

2024-02-17T19:46:50.602926

[188.75.99.30](https://www.shodan.io/host/188.75.99.30)

* [Baqiyatallah University Of Medical Sciences](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+org%3A%22Baqiyatallah+University+Of+Medical+Sciences%22)
* https://www.shodan.io/static/flags/16/IR-caec555e.png[Iran, Islamic Republic of](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+country%3A%22IR%22), [Pāsārgād](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+city%3A%22P%C4%81s%C4%81rg%C4%81d%22)

mDNS:

services:

8080/tcp http:

path=/

Name=QNAP-**NAS**

Address=188.75.99.30

answers:

PTR:

\_http.\_tcp.local

\_smb.\_tcp.local

\_qmobile.\_tcp.local

\_qdiscover.\_tcp.local

\_workstation.\_tcp.local

2024-02-17T18:32:33.363755

[46.100.47.28](https://www.shodan.io/host/46.100.47.28)

* [Telecommunication Company of Tehran](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+org%3A%22Telecommunication+Company+of+Tehran%22)
* https://www.shodan.io/static/flags/16/IR-caec555e.png[Iran, Islamic Republic of](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+country%3A%22IR%22), [Tehran](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+city%3A%22Tehran%22)

[self-signed](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+tag%3Aself-signed)

# ****SSL Certificate****

* Issued By:
  + |- Common Name: **QNAP NAS**
  + |- Organization: **QNAP Systems, Inc.**
* Issued To:
  + |- Common Name:**QNAP NAS**
  + |- Organization:**QNAP Systems, Inc.**

Supported SSL Versions:  
**TLSv1.2, TLSv1.3**

HTTP/1.1 200 OK

Date: Sat, 17 Feb 2024 17:42:55 GMT

Server:

X-Frame-Options: SAMEORIGIN

Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval' ; object-src 'self' ; worker-src 'self' blob:

Content-type: text/html; charset=UTF-8

Last-modified: Fri, 28 Jan 2022 23:11:23 GM...

2024-02-17T18:18:40.847769

[89.41.42.179](https://www.shodan.io/host/89.41.42.179)

* [Asiatech Data Transmission Co.](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+org%3A%22Asiatech+Data+Transmission+Co.%22)
* https://www.shodan.io/static/flags/16/IR-caec555e.png[Iran, Islamic Republic of](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+country%3A%22IR%22), [Tehran](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+city%3A%22Tehran%22)

[self-signed](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+tag%3Aself-signed)

# ****SSL Certificate****

* Issued By:
  + |- Common Name: **QNAP NAS**
  + |- Organization: **QNAP Systems, Inc.**
* Issued To:
  + |- Common Name:**QNAP NAS**
  + |- Organization:**QNAP Systems, Inc.**

Supported SSL Versions:  
**TLSv1.2, TLSv1.3**

HTTP/1.1 200 OK

Date: Sat, 17 Feb 2024 18:18:40 GMT

Server:

X-Frame-Options: SAMEORIGIN

Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval' ; object-src 'self' ; worker-src 'self' blob:

Content-type: text/html; charset=UTF-8

Last-modified: Sat, 29 Jan 2022 03:03:37 GM...

2024-02-17T17:54:22.601201

[SRV-NAS&nbsp;-&nbsp;Synology&nbsp;NAS](https://www.shodan.io/host/80.210.30.65)

* 80.210.30.65
* [Telecommunication Company of Tehran](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+org%3A%22Telecommunication+Company+of+Tehran%22)
* https://www.shodan.io/static/flags/16/IR-caec555e.png[Iran, Islamic Republic of](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+country%3A%22IR%22), [Tehran](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+city%3A%22Tehran%22)
* [https://www.shodan.io/static/img/http-components/Synology%20DiskStation-d9a123d8.png](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+http.component%3A%22Synology+DiskStation%22)[https://www.shodan.io/static/img/http-components/Vue.js-65c1af32.png](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+http.component%3A%22Vue.js%22)[https://www.shodan.io/static/img/http-components/ExtJS-50d68088.png](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+http.component%3A%22ExtJS%22)

# ****SSL Certificate****

* Issued By:
  + |- Common Name: **Synology Inc. CA**
  + |- Organization: **Synology Inc.**
* Issued To:
  + |- Common Name:**synology**
  + |- Organization:**Synology Inc.**

Supported SSL Versions:  
**TLSv1.2**

HTTP/1.1 200 OK

Server: nginx

Date: Sat, 17 Feb 2024 17:54:22 GMT

Content-Type: text/html; charset="UTF-8"

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=20

Cache-control: no-store

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

X-Frame-Options: SA...

2024-02-17T15:16:58.554297

[SRV-NAS&nbsp;-&nbsp;Synology&nbsp;NAS](https://www.shodan.io/host/84.241.13.201)

* 84.241.13.201
* 84-241-13-201.shatel.ir
* [SHATEL DSL Network](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+org%3A%22SHATEL+DSL+Network%22)
* https://www.shodan.io/static/flags/16/IR-caec555e.png[Iran, Islamic Republic of](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+country%3A%22IR%22), [Tehran](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+city%3A%22Tehran%22)
* [https://www.shodan.io/static/img/http-components/Synology%20DiskStation-d9a123d8.png](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+http.component%3A%22Synology+DiskStation%22)[https://www.shodan.io/static/img/http-components/Vue.js-65c1af32.png](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+http.component%3A%22Vue.js%22)[https://www.shodan.io/static/img/http-components/ExtJS-50d68088.png](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+http.component%3A%22ExtJS%22)

# ****SSL Certificate****

* Issued By:
  + |- Common Name: **Synology Inc. CA**
  + |- Organization: **Synology Inc.**
* Issued To:
  + |- Common Name:**synology**
  + |- Organization:**Synology Inc.**

Supported SSL Versions:  
**TLSv1.2**

HTTP/1.1 200 OK

Server: nginx

Date: Sat, 17 Feb 2024 15:16:58 GMT

Content-Type: text/html; charset="UTF-8"

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=20

Cache-control: no-store

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

X-Frame-Options: SA...

2024-02-17T11:33:30.841737

[37.32.25.190](https://www.shodan.io/host/37.32.25.190)

* machi47.serpa.live
* [AbrArvan IaaS](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+org%3A%22AbrArvan+IaaS%22)
* https://www.shodan.io/static/flags/16/IR-caec555e.png[Iran, Islamic Republic of](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+country%3A%22IR%22), [Tehran](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+city%3A%22Tehran%22)

SSH-2.0-OpenSSH\_8.9p1 Ubuntu-3ubuntu0.6

Key type: ecdsa-sha2-nistp256

Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIsmfO67BHIFXxJCGzD2Vgop

**NaS**/dElymhiFTNBdbLTkahS7bK8SSbkE0e20lvJgMvNtwA3+sXW8OFePyzqQyvE=

Fingerprint: fb:47:20:c1:90:25:44:97:5f:d4:59:f7:df:b9:02:61

Kex Algorithms:

c...

2024-02-17T11:31:05.536743

[94.183.200.66](https://www.shodan.io/host/94.183.200.66)

* 94-183-200-66.shatel.ir
* [SHATEL DSL Network](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+org%3A%22SHATEL+DSL+Network%22)
* https://www.shodan.io/static/flags/16/IR-caec555e.png[Iran, Islamic Republic of](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+country%3A%22IR%22), [Tehran](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+city%3A%22Tehran%22)

HTTP/1.1 200 OK

Date: Sat, 17 Feb 2024 11:31:03 GMT

Server:

X-Frame-Options: SAMEORIGIN

Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval' ; object-src 'self' ; worker-src 'self' blob:

Content-type: text/html; charset=UTF-8

Last-modified: Mon, 20 Dec 2021 21:26:37 GM...

2024-02-17T10:48:48.676414

[Nas-Core&nbsp;-&nbsp;Synology&nbsp;DiskStation](https://www.shodan.io/host/185.42.24.154)

* 185.42.24.154
* [Cooperative Afra ertebatat-e-sabet-e Rasa Co](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+org%3A%22Cooperative+Afra+ertebatat-e-sabet-e+Rasa+Co%22)
* https://www.shodan.io/static/flags/16/IR-caec555e.png[Iran, Islamic Republic of](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+country%3A%22IR%22), [Tehran](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+city%3A%22Tehran%22)
* [https://www.shodan.io/static/img/http-components/Prototype-98546abb.png](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+http.component%3A%22Prototype%22)[https://www.shodan.io/static/img/http-components/ExtJS-50d68088.png](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+http.component%3A%22ExtJS%22)[https://www.shodan.io/static/img/http-components/Synology%20DiskStation-d9a123d8.png](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+http.component%3A%22Synology+DiskStation%22)

HTTP/1.1 200 OK

Server: nginx

Date: Sat, 17 Feb 2024 10:58:30 GMT

Content-Type: text/html; charset="UTF-8"

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=20

Vary: Accept-Encoding

Cache-control: no-store

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=blo...