**22: Lab 22 - Assisted - DNS Security**
*Security+ (Exam SY0-701)*


Congratulations, you passed!

*Duration: 32 minutes, 13 seconds*

☑ **confirm if @lab.Variable(DNSThreat) is 'badsite.ru'** *Score: 1*
Select the **Score** button to validate this task:
`Value matched ...`

☑ What is the approximate time interval between type 1 queries to badsite.ru? *Score: 1*

- ○ 1 second
- ◉ 5 seconds
- ○ 20 seconds
- ○ 1 minute

Congratulations, you have answered the question correctly.

☑ **confirm that the file /root/block-DNS.sh contains "mv /tmp/hosts /etc/hosts"** *Score: 1*
Select the **Score** button to validate this task:
```
The string 'mv /tmp/hosts /etc/hosts' is present in the file
Task complete
```

☑ Which of the following statements are true in regards to the output from the `ping` command just entered? *Score: 1*

- ○ The FQDN resolves to a public IP address
- ○ No ECHO_REPLIES are received
- ◉ The domain name resolves to the loopback address
- ○ The query operations are being filtered

Congratulations, you have answered the question correctly.

☑ **confirm that /var/spool/cron/crontab/root contains "0 3 * * * /bin/bash /root/block-DNS.sh"** *Score: 1*
Select the **Score** button to validate this task:
```
The string '0 3 * * * /bin/bash /root/block-DNS.sh' is present in the file
Task complete
```

If there is an abuse or a problem related to the domain name comptia.org, what contact point should be used to report the issue? *Score: 1*

- armando.ns.cloudflare.com
- dns@cloudflare.com
- abuse@dns.cloudflare.com
- abuse@dns.cloudflare.com

Congratulations, you have answered the question correctly.

Why is beaconing an important IoC to look for? *Score: 1*

- It indicates active malware attempting to contact a C&C.
- It is evidence of buffer overflow exploits.
- It is triggered by any malicious activity.
- It may use polymorphism to hide its identity.

Congratulations, you have answered the question correctly.

What is the primary limitation of the automation used to block access to malicious FQDNs? *Score: 1*

- it protects against both the FQDN and the related IP address
- it blocks reverse lookups
- it allows secure access to the FQDNs of concern
- It only protects the individual system where it runs

Congratulations, you have answered the question correctly.

In what two modes can nslookup be used? (Select two) *Score: 1*

- [x] Interactive
- [ ] Recursive
- [ ] Automatic
- [ ] Iterative
- [x] Non-interactive

Congratulations, you have answered the question correctly.

Which option in dig will let you select the DNS record type to return? *Score: 1*

- -r
- -t
- -d
- -z

Congratulations, you have answered the question correctly.

What is the repeated attempt to resolve a FQDN on a regular interval by unknown software called? *Score: 1*

- port scanning
- DNS spoofing
- shell injection
- beaconing

Congratulations, you have answered the question correctly.