مرکز تخصصی
آپا دانشگاه کردستان

سامانه پویش سرور ایمیل ویرا

msscanner.uok.ac.ir

مرکز آپا دانشگاه کردستان

cert.uok.ac.ir
cert@uok.ac.ir
087-33611415


قابلیت‌های ابزار
Domain Check
Banner Check
SPF Record
DMARC Check
PTR Record
ESMTP
HELP Command
VRFY Check
Spam check
EXPN Check
AUTH Check
DNS Black List
Open Relay
سامانه پویش سرور ایمیل ویرا
ابزاری جهت بررسی امنیتی سرورهای ایمیل و راهنمای پیکربندی امن
شروع پویش
SIRT
ابزاری جهت بررسی امنیتی سرورهای ایمیل
و راهنمای پیکربندی امن
VIRA
Mail Server Scanner
msscanner.uok.ac.ir
KURD
SIRT
مرکز آپا دانشگاه کردستان

سامانه پویش سرور ایمیل ویرا با آدرس msscanner.uok.ac.ir دارای قابلیت‌های زیر است:

۱-Domain Check

این قابلیت به بررسی دامنه مورد نظر و سرورهای ایمیلی که بر روی آن فعال هستند، می‌پردازد. در این بخش در صورتی که کاربر آدرس دامنه را به‌جای آدرس سرور ایمیل وارد نماید با جستجو و استفاده از رکورد MX، آدرس ایمیل سرورهای فعال در این دامنه را بدست می‌آورد. در شکل ۱ و ۲ سرورهای ایمیل فعال بر روی دامنه دانشگاه کردستان و گوگل نمایش داده شده است.

```
root@kali:~# nslookup -type=mx uok.ac.ir
Server:         192.168.109.2
Address:        192.168.109.2#53

Non-authoritative answer:
uok.ac.ir       mail exchanger = 10 mail.uok.ac.ir.

Authoritative answers can be found from:
mail.uok.ac.ir  internet address = 2.182.201.7
```

شکل ۱: بررسی MX Record دانشگاه کردستان

```
root@kali:~# nslookup -type=mx google.com
Server:         192.168.109.2
Address:        192.168.109.2#53

Non-authoritative answer:
google.com      mail exchanger = 40 alt3.aspmx.l.google.com.
google.com      mail exchanger = 10 aspmx.l.google.com.
google.com      mail exchanger = 50 alt4.aspmx.l.google.com.
google.com      mail exchanger = 30 alt2.aspmx.l.google.com.
google.com      mail exchanger = 20 alt1.aspmx.l.google.com.

Authoritative answers can be found from:
alt3.aspmx.l.google.com internet address = 108.177.10.26
alt3.aspmx.l.google.com has AAAA address 2607:f8b0:4003:c14::1a
aspmx.l.google.com      internet address = 173.194.222.26
aspmx.l.google.com      has AAAA address 2a00:1450:4010:c05::1b
alt4.aspmx.l.google.com internet address = 209.85.145.26
alt4.aspmx.l.google.com has AAAA address 2607:f8b0:4001:c1e::1b
alt2.aspmx.l.google.com internet address = 173.194.202.26
alt2.aspmx.l.google.com has AAAA address 2607:f8b0:400e:c00::1a
alt1.aspmx.l.google.com internet address = 108.177.97.26
alt1.aspmx.l.google.com has AAAA address 2404:6800:4008:c00::1a
```

شکل۲: بررسی MX Record مربوط به گوگل

مقدار Mail Exchanger =10 میزان اهمیت سرور پست الکترونیکی را نشان می‌دهد و هرچه عدد آن کمتر باشد دارای اولویت بیشتری است.

Banner Check-۲

در زمان اتصال اولیه به سرور ایمیل، Banner دریافت شده از سمت سرور ممکن است شامل نوع و نسخه سرویس ایمیل هدف باشد. مهاجم با استفاده از این اطلاعات خواهد توانست، با بهره‌برداری از آسیب‌پذیری‌های سرویس استفاده شده، سرور ایمیل را مورد حمله قرار دهد.

SPF Record-۳

Sender Policy Framework یا به اختصار SPF یک DNS Record می‌باشد که آدرس‌های IP مجاز به ارسال ایمیل از طرف دامنه شما را مشخص می‌کند. سرور ایمیل زمانی که یک ایمیل دریافت می‌کند صحت آدرس IP ارسال کننده آن را با استفاده از SPF Record بررسی خواهد کرد و درصورتی که تایید(Pass) نشود آن را در گروه هرزنامه قرار می‌دهد. در شکل ۳ نحوه بدست آوردن SPF نمایش داده شده است.

```
root@kali:~# nslookup -type=txt google.com
Server:         192.168.109.2
Address:        192.168.109.2#53

Non-authoritative answer:
google.com      text = "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com      text = "v=spf1 include:_spf.google.com ~all"
google.com      text = "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="
google.com      text = "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com      text = "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"

Authoritative answers can be found from:

root@kali:~# nslookup -type=txt uok.ac.ir
Server:         192.168.109.2
Address:        192.168.109.2#53

Non-authoritative answer:
uok.ac.ir       text = "v=spf1 mx a ip4:2.182.201.7 ~all"

Authoritative answers can be found from:
```

شکل۳: بدست آوردن رکورد SPF

DMARC Check-٤

DMARC یک DNS Record می‌باشد که بر پایه SPF Record و DKIM Record جهت جلوگیری از جعل ایمیل استفاده می‌شود. DMARC یک مکانیزم می‌باشد که ضعف‌های موجود در SPF Record و DKIM Record را تا حدودی برطرف کرده است.

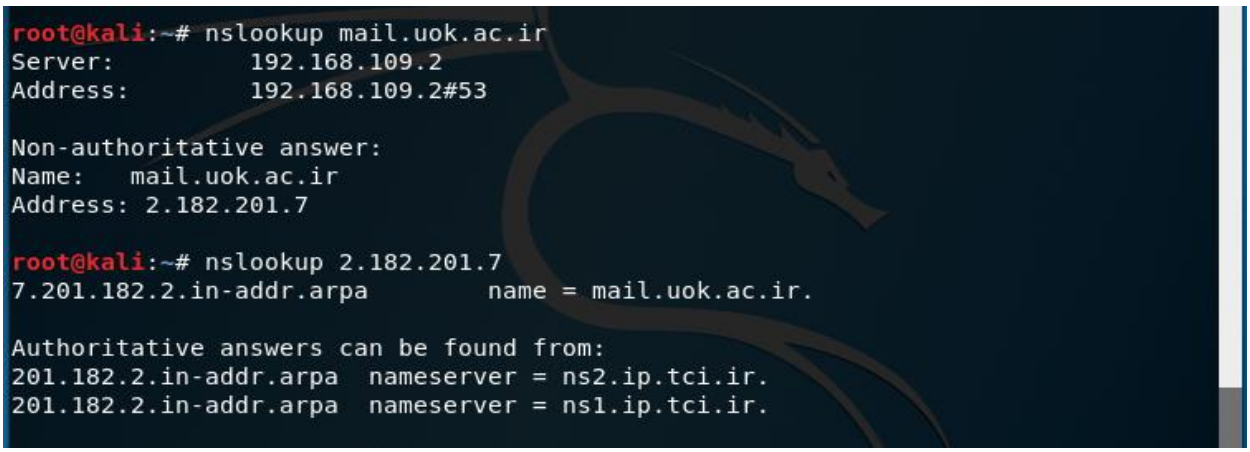
DKIM (Domain Keys Identified Mail) یک تکنیک احراز هویت ایمیل است که به گیرنده اجازه می‌دهد بررسی کند که یک ایمیل واقعاً توسط صاحب دامنه‌ای مجاز ارسال‌شده است. این روند با استفاده از امضاء دیجیتال در ایمیل انجام می‌شود. امضاء DKIM سرآیندی است که به پیام اضافه می‌شود و با رمزگذاری این امر را تضمین می‌کند. هنگامی‌که گیرنده تشخیص دهد که این ایمیل با امضاء معتبر DKIM امضاء شده است، مطمئن می‌شود قسمت‌هایی از ایمیل مانند بدنه و دیگر ویژگی‌ها تغییر نکرده‌اند. امضاء DKIM برای کاربران نهایی قابل‌مشاهده نیست و اعتبارسنجی در سطح سرور انجام می‌شود. اجرای استاندارد DKIM اگر از DKIM Record به همراه DMARC وSPF استفاده شود، باعث بهبود قابلیت ارسال ایمیل می‌شود. با در نظر گرفتن این حالت می‌توان دامنه خود را در برابر ایمیل‌های مخرب ارسال‌شده محافظت کرد. اگرچه، در عمل اگر از DKIM Record به همراه DMARC وSPF استفاده کنید، نتایج مؤثرتری به دست می‌آیند. در بررسی DMARC از SPF و DKIM استفاده می‌شود. آن‌ها با هم‌افزایی به بهترین نتیجه برای امنیت در تحویل ایمیل دست پیدا می‌کنند.

امضاء DKIM توسط MTA (Mail Transfer Agent) تولید می‌شود و مجموعه منحصربه‌فرد به نام Hash Value را ایجاد می‌کند و این مقدار Hash در دامنه ذکرشده ذخیره می‌شود. پس از دریافت ایمیل، گیرنده می‌تواند امضاء DKIM را با استفاده از کلید عمومی ثبت‌شده در DNS تأیید کند. از این کلید برای رمزگشایی مقدار Hash در سرآیند استفاده می‌شود و مقدار Hash را از طریق ایمیل دریافتی مجدداً محاسبه می‌کند. اگر این دو امضا مربوط به DKIM یکسان باشند، MTA می‌داند که ایمیل تغییری نکرده است. این به کاربر تضمین می‌دهد که ایمیل درواقع از دامنه ذکرشده ارسال شده است.

DMARC با استفاده از DKIM وSPF ساخته‌شده است. آن‌ها باهم بهترین راه‌حل برای جلوگیری از جعل ایمیل و ایجاد اعتماد بیشتر به پست‌های الکترونیک را فراهم می‌کنند. DMARC فقط در صورتی کار می‌کند که SPF و DKIM تنظیم شده باشند.

PTR Record-٥

PTR Record یا Pointer Record یک DNS Record می‌باشد که برای تبدیل آدرس IP به دامنه استفاده می‌شود. در صورت عدم وجود این Record، در مواردی که گیرنده ایمیل آدرس IP دامنه را با دامنه ارسال کننده ایمیل مقایسه کند با مشکل مواجه خواهد شد و ایمیل دریافت شده را به عنوان هرزنامه دسته‌بندی می‌کند. نمونه‌ای از این رکورد در شکل ۴ نشان داده شده است.



شکل٤: بررسی PTR Record دانشگاه کردستان

ESMTP-۶

Extended SMTP یا به اختصار ESMTP، نسخه توسعه‌داده شده پروتکل SMTP اولیه است. در این پروتکل ویژگی‌هایی مانند رمزگذاری ایمیل از طریق SSL، امکان اتصال فایل‌های چندرسانه به ایمیل، محدودیت در اندازه ایمیل، انتقال همزمان یک ایمیل به چندین گیرنده و پیام‌های خطای استاندارد درصورت عدم تحویل به گیرنده افزوده شده است.

HELP Command-۷

در پروتکل SMTP با ارسال دستور HELP، دستورات و فرامینی که در سرور ایمیل فعال هستند، مشخص می‌شوند که می‌تواند منجر به افشای اطلاعات پیکربندی سرور ایمیل شود.

VRFY Check-۸

در پروتکل SMTP با استفاده از دستور VRFY می‌توان به وجود یا عدم وجود یک آدرس ایمیل در سرور پی برد و منجر به افشای اطلاعات می‌گردد. در حالت صحیح، دستور VERFY غیرفعال است.

EXPN Check-۹

با دستور EXPN لیست تمام آدرس‌های ایمیل فعال در سرور ایمیل نمایش داده می‌شود و منجر به افشای اطلاعات می‌گردد. در حالت امن دستور EXPN غیرفعال است.

AUTH Check-۱۰

این بخش نوع احرازهویت SMTP یا به اختصار SMTP AUTH که توسط ایمیل‌سرور پشتیبانی می‌شود را تشخیص می‌دهد. معمولا در سرورهای ایمیل، احرازهویت برای کاربران اجباری می‌باشد.

DNS Black List -۱۱

لیست‌های سیاه متعددی برای تشخیص دامنه ایمیل‌سرورهایی که به ارسال هرزنامه معروف هستند، وجود دارد. هر کدام از این DNSBL معیارهای متفاوتی برای افزودن و یا حذف از لیست سیاه خود دارند. سرورهای ایمیل می‌توانند به گونه تنظیم شوند که ایمیلی دریافت شده از دامنه ثبت شده در DNSBL را رد یا علامت‌گذاری کنند.
لیست DNSBL که در این سامانه بررسی می‌شوند، به شرح زیر است:

1. all.s5h.net
2. b.barracudacentral.org
3. bl.spamcop.net
4. blacklist.woody.ch
5. bogons.cymru.com
6. cbl.abuseat.org

7. combined.abuse.ch
8. db.wpbl.info
9. dnsbl-1.uceprotect.net
10. dnsbl-2.uceprotect.net
11. dnsbl-3.uceprotect.net
12. dnsbl.anticaptcha.net
13. dnsbl.dronebl.org
14. dnsbl.sorbs.net
15. dnsbl.spfbl.net
16. drone.abuse.ch
17. duinv.aupads.org
18. dul.dnsbl.sorbs.net
19. dyna.spamrats.com
20. dynip.rothen.com
21. http.dnsbl.sorbs.net
22. ips.backscatterer.org
23. ix.dnsbl.manitu.net
24. korea.services.net
25. misc.dnsbl.sorbs.net
26. noptr.spamrats.com
27. orvedb.aupads.org
28. pbl.spamhaus.org
29. proxy.bl.gweep.ca
30. psbl.surriel.com
31. relays.bl.gweep.ca
32. relays.nether.net
33. sbl.spamhaus.org
34. singular.ttk.pte.hu
35. smtp.dnsbl.sorbs.net
36. socks.dnsbl.sorbs.net
37. spam.abuse.ch
38. spam.dnsbl.anonmails.de
39. spam.dnsbl.sorbs.net
40. spam.spamrats.com
41. spambot.bls.digibase.ca
42. spamrbl.imp.ch
43. spamsources.fabel.dk
44. ubl.lashback.com
45. ubl.unsubscore.com
46. virus.rbl.jp
47. web.dnsbl.sorbs.net
48. wormrbl.imp.ch
49. xbl.spamhaus.org
50. z.mailspike.net
51. zen.spamhaus.org
52. zombie.dnsbl.sorbs.net

۱۲-Open Relay Check

Open Relay، یک سرور ایمیل با پیکربندی نامناسب است که باعث می‌شود مهاجمان بتوانند به ایمیل سرور متصل شوند و با استفاده از آدرس‌های ایمیل جعلی اقدام به ارسال ایمیل کنند. به عنوان مثال مهاجم می‌تواند با استفاده از یک سرور ایمیل آسیب‌پذیر، به آدرس vuln.test.ir که دارای پیکربندی نامناسب است، اقدام به ارسال ایمیل از یک آدرس خارجی مانند admin@shop.ir به آدرس user1@shop.ir به منظور انجام حملات فیشینگ یا ارسال بدافزار به قربانی و یا سایر حملات، کند. این ضعف پیکربندی توسط سامانه پویش سرور ایمیل ویرا به راحتی قابل تشخیص است.

Email Spoofing-۱۳

در این سامانه، امکان ارسال هرزنامه با استفاده از سرور ایمیل هدف، مورد بررسی قرار داده می‌شود. به عنوان مثال در صورت استفاده سرور ایمیل mail.test.ir از پیکربندی نامناسب، این امکان بوجود می‌آید که مهاجم به سرور ایمیل عنوان شده متصل شود، سپس از یک آدرس جعلی یا اصلی داخلی مانند admin@test.ir به یک آدرس داخلی دیگر مانند Info@test.ir یک ایمیل با محتوای فیشینگ یا بدافزار یا هر محتوای دیگری ارسال کند.