Accessible RDP Report

A scan report for your network/constituency

@shadowserver

contact@shadowserver.org

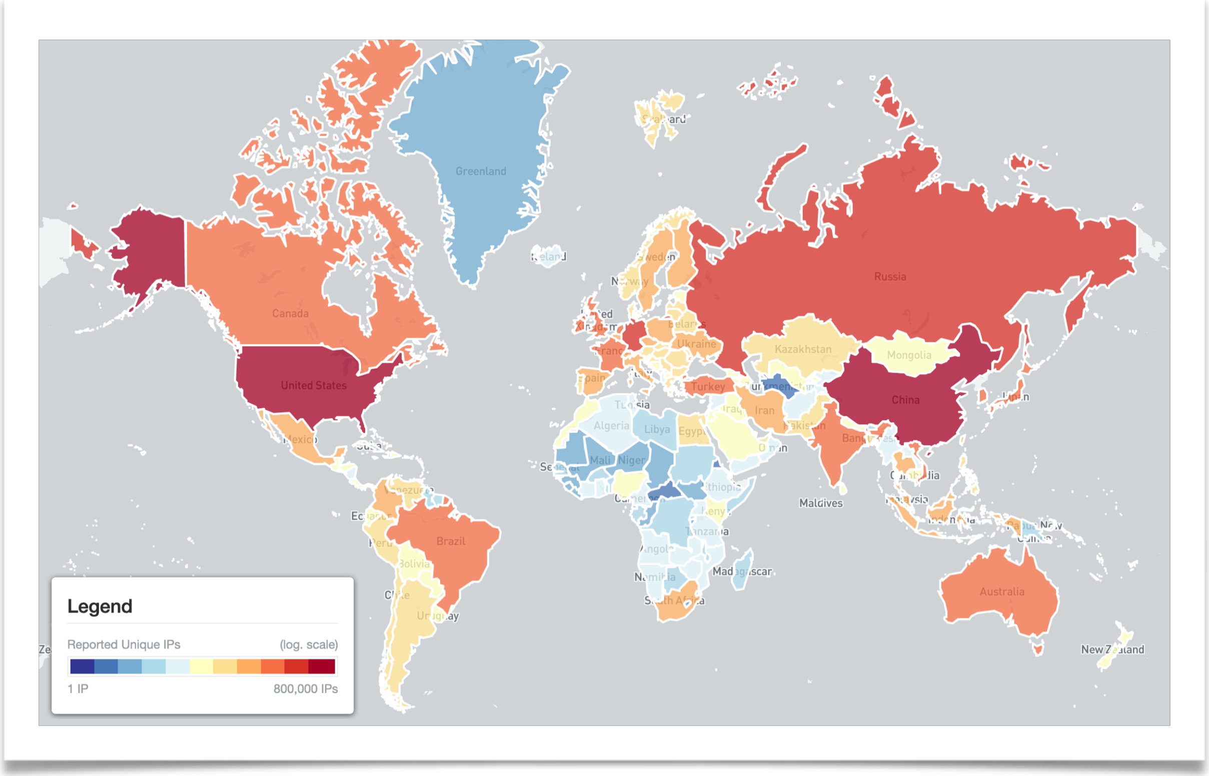
SHADOWSERVER.ORG

Presentation Aims & Objectives

- Introduce Accessible RDP
- Highlight a sample Accessible RDP report
- Describe key features of the report
- Demonstrate how a National CERT can action an Accessible RDP report
- Offer guidance on how to protect and secure RDP
- Provide a key list of Shadowserver online resources to enable report subscription and use

Accessible RDP - Summary

- Remote Desktop Protocol - developed by Microsoft
- Access to remote PC or virtual apps and desktops
- Misconfigured RDP can allow access to vulnerable hosts
- Allows for information-gathering on a target host via SSL certificate capture
- Remote working makes RDP a high attack vector for brute-force attack and exploits



Internet-wide Scanning

- Shadowserver scans the entire IPv4 Internet for 70 different network protocols every day, and also performs IPv6 scans based on IPv6 hitlists for selected protocols
- These are primarily "hello" type port/application scans
- Shadowserver does not exploit any vulnerability
- Scans allow for identifying misconfigured, vulnerable or abusable devices, unnecessarily exposed attack surfaces, or are simply just population enumeration
- Read more on why we scan at: https://www.shadowserver.org/news/the-scannings-will-continue-until-the-internet-improves/

Internet-wide Scanning - RDP

- RDP services are a popular attack vector
- The goal of this project is to identify openly accessible systems that have the RDP service running and report them back to the network owners for notification
- We query all computers with routable IPv4 addresses that are not firewalled from the internet on port 3389/tcp with an RDP negotiation request and capturing the response
- If a host replies affirmatively, we follow that query up with an attempt to fetch the client's SSL certificate

Bluekeep/CVE-2019-0708

- "A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction".

  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708

- Shadowserver Accessible RDP scan checks for this vulnerability and also reports if it is found as part of the scan

- Bluekeep scans results can be found in the cve20190708_vulnerable column, set to Y if vulnerability is found

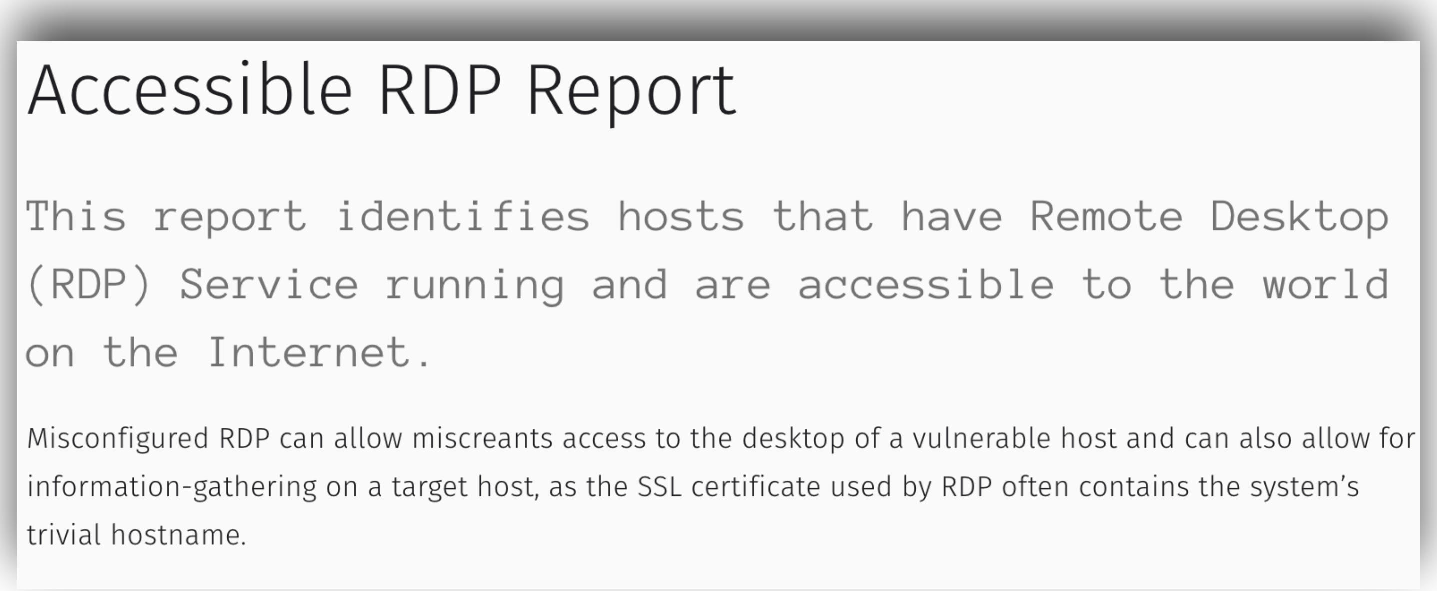
Accessible RDP Report

- Dedicated RDP Scanning Project site: https://scan.shadowserver.org/rdp/
- Report is available as a file in CSV format
- Filename contains scan_rdp
- All timestamps are in UTC
- Reports can be sent as e-mail attachments, or downloaded via HTTP or obtained via a RESTful API
- For more documentation on API access, please visit the below URLs and send a request for access to contact@shadowserver.org

https://www.shadowserver.org/what-we-do/network-reporting/api-documentation/

https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/

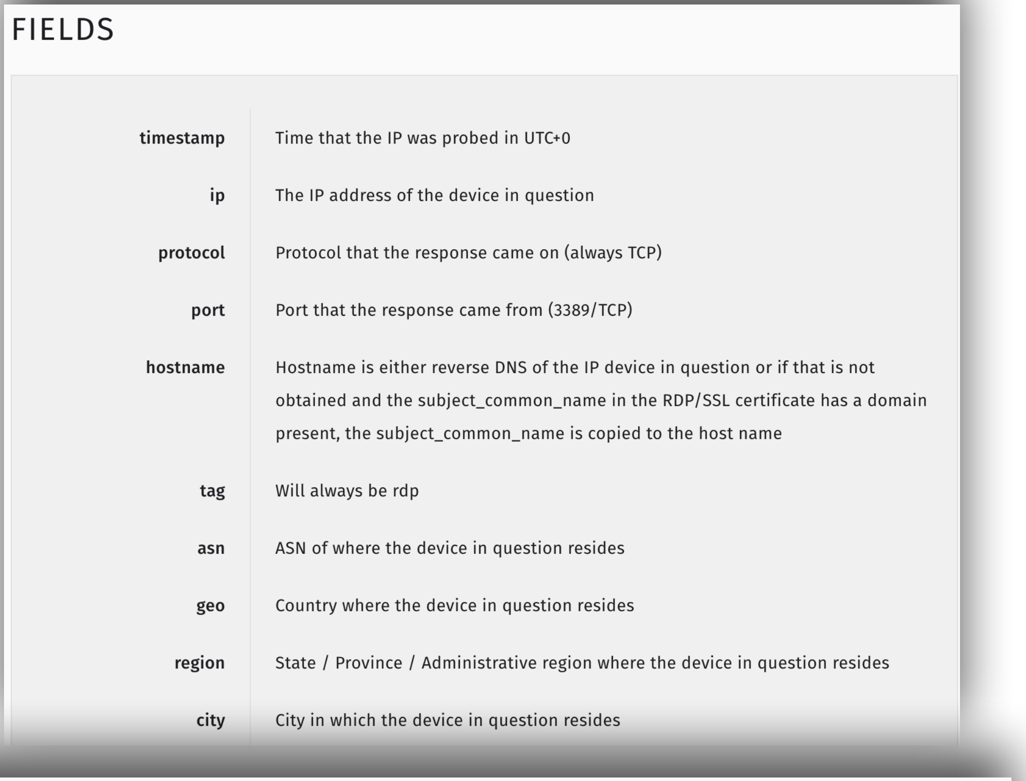
Accessible RDP Report



Accessible RDP Report

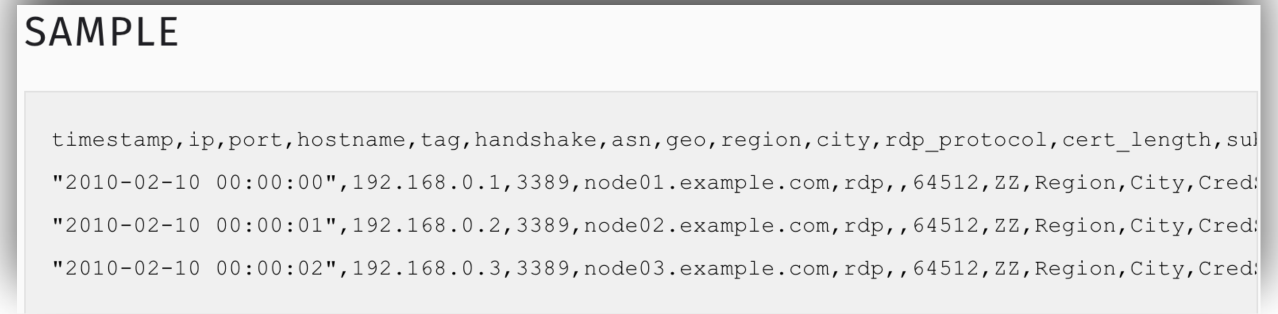
This report identifies hosts that have Remote Desktop (RDP) Service running and are accessible to the world on the Internet.

Misconfigured RDP can allow miscreants access to the desktop of a vulnerable host and can also allow for information-gathering on a target host, as the SSL certificate used by RDP often contains the system's trivial hostname.



FIELDS

timestamp	Time that the IP was probed in UTC+0
ip	The IP address of the device in question
protocol	Protocol that the response came on (always TCP)
port	Port that the response came from (3389/TCP)
hostname	Hostname is either reverse DNS of the IP device in question or if that is not obtained and the subject_common_name in the RDP/SSL certificate has a domain present, the subject_common_name is copied to the host name
tag	Will always be rdp
asn	ASN of where the device in question resides
geo	Country where the device in question resides
region	State / Province / Administrative region where the device in question resides
city	City in which the device in question resides



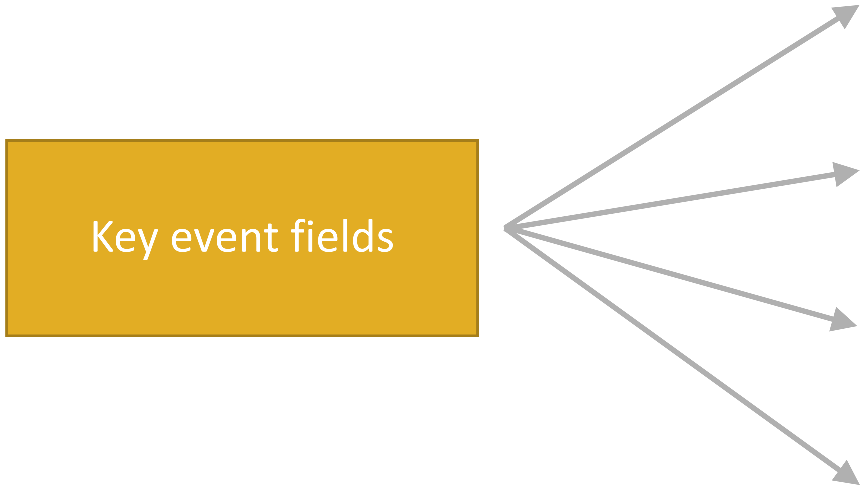
SAMPLE

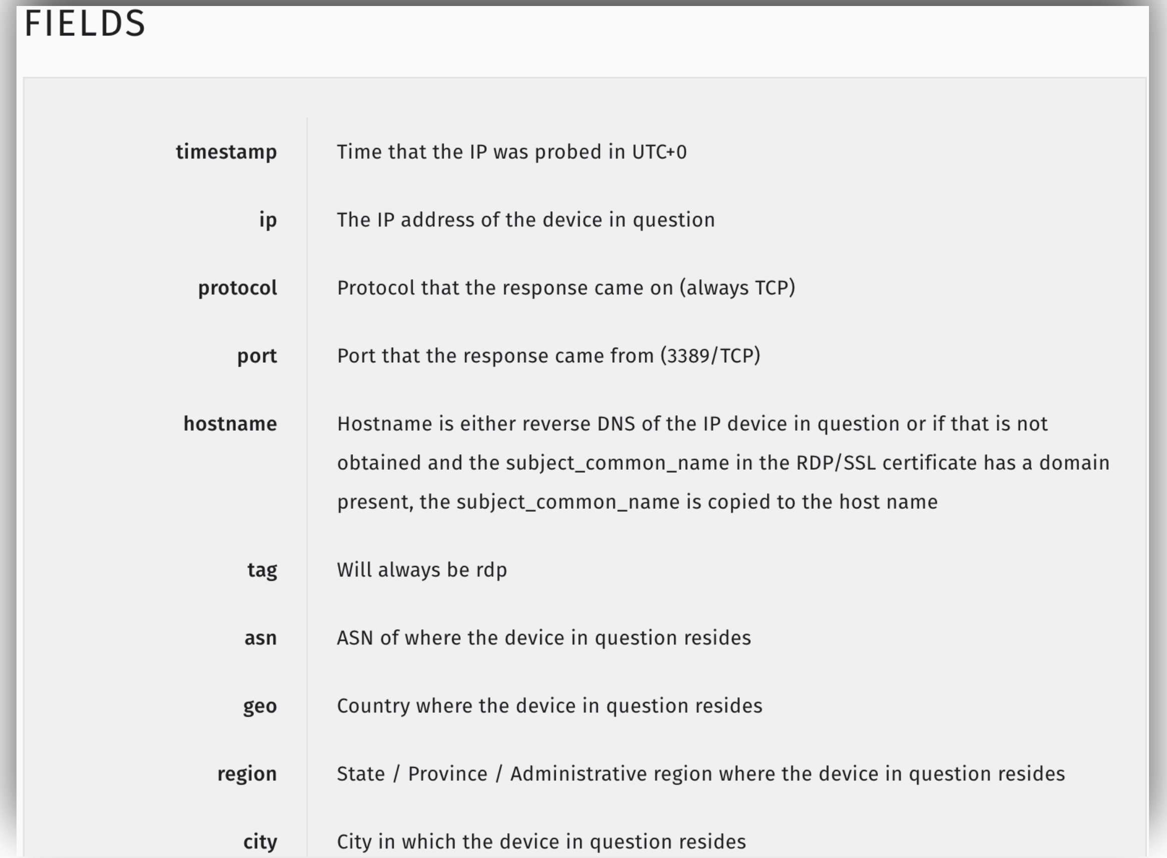
```
timestamp,ip,port,hostname,tag,handshake,asn,geo,region,city,rdp_protocol,cert_length,su
"2010-02-10 00:00:00",192.168.0.1,3389,node01.example.com,rdp,,64512,ZZ,Region,City,Cred
"2010-02-10 00:00:01",192.168.0.2,3389,node02.example.com,rdp,,64512,ZZ,Region,City,Cred
"2010-02-10 00:00:02",192.168.0.3,3389,node03.example.com,rdp,,64512,ZZ,Region,City,Cred
```

https://www.shadowserver.org/what-we-do/network-reporting/accessible-rdp-report/

Example Scan Report - Accessible RDP

timestamp	IP	protocol	port	Hostname	tag	asn	Geo	Region	city	cve20190708_vulnerable	bluekeep_vulnerable
05/03/2022 00:02	65.21.143.XX	tcp	3389	XXXX	rdp	24940	FI	UUSIMAA	HELSINKI	N	N



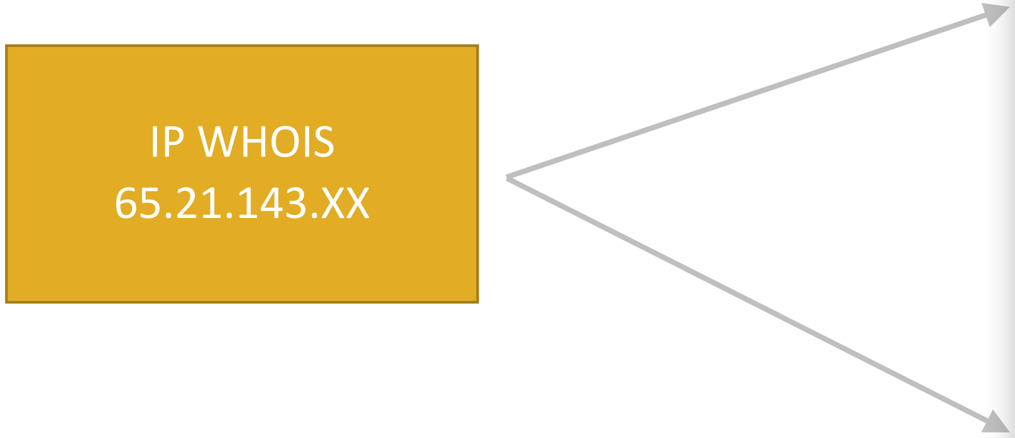


FIELDS

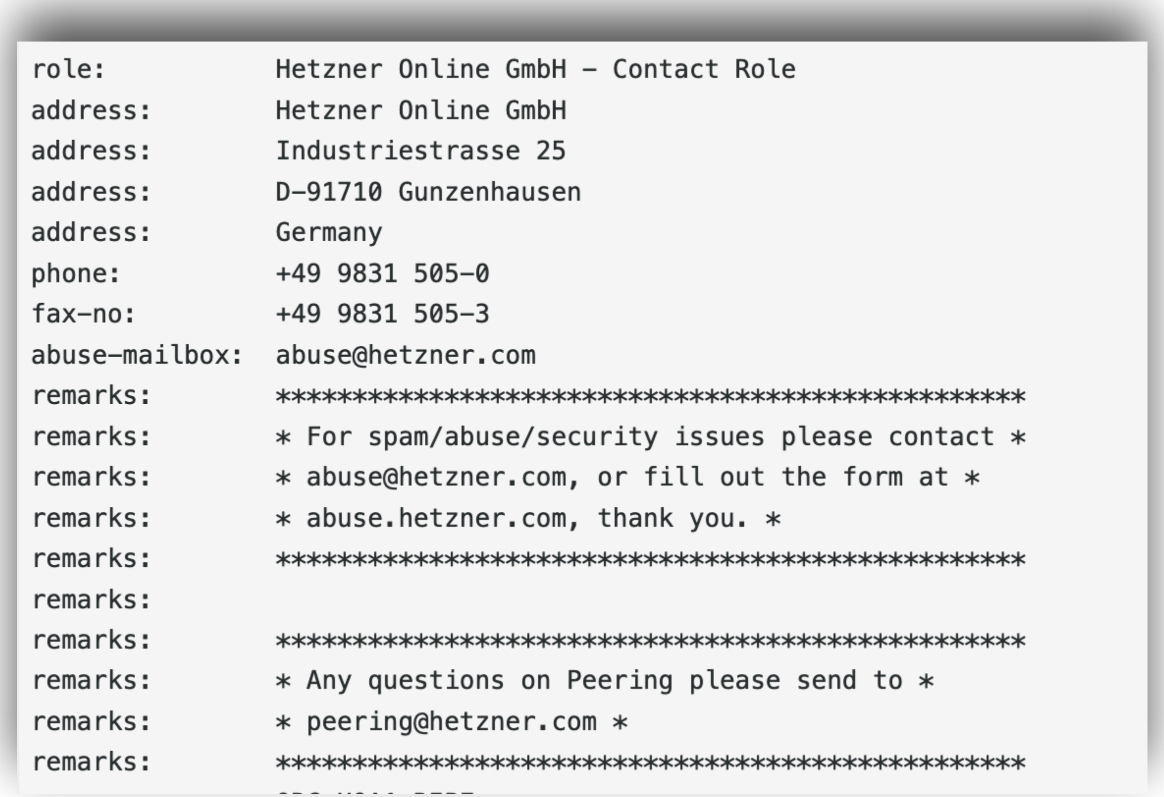
timestamp	Time that the IP was probed in UTC+0
ip	The IP address of the device in question
protocol	Protocol that the response came on (always TCP)
port	Port that the response came from (3389/TCP)
hostname	Hostname is either reverse DNS of the IP device in question or if that is not obtained and the subject_common_name in the RDP/SSL certificate has a domain present, the subject_common_name is copied to the host name
tag	Will always be rdp
asn	ASN of where the device in question resides
geo	Country where the device in question resides
region	State / Province / Administrative region where the device in question resides
city	City in which the device in question resides

Example Scan Report - Accessible RDP

timestamp	IP	protocol	port	Hostname	tag	asn	Geo	Region	city	cve20190708_vulnerable	bluekeep_vulnerable
05/03/2022 00:02	65.21.143.XX	tcp	3389	XXXX	rdp	24940	FI	UUSIMAA	HELSINKI	N	N



IP WHOIS
65.21.143.XX



```
role:           Hetzner Online GmbH - Contact Role
address:        Hetzner Online GmbH
address:        Industriestrasse 25
address:        D-91710 Gunzenhausen
address:        Germany
phone:          +49 9831 505-0
fax-no:         +49 9831 505-3
abuse-mailbox:  abuse@hetzner.com
remarks:        ************************************************
remarks:        * For spam/abuse/security issues please contact *
remarks:        * abuse@hetzner.com, or fill out the form at *
remarks:        * abuse.hetzner.com, thank you. *
remarks:        ************************************************
remarks:
remarks:        ************************************************
remarks:        * Any questions on Peering please send to *
remarks:        * peering@hetzner.com *
remarks:        ************************************************
```

Accessible RDP - PROTECT

- Ensure network devices are up to date and patched
- Use two-factor authentication, and implement lockout policies
- Firewall management to restrict RDP sessions by IP address
- Limit RDP access to a specific user group and disable domain admin to access RDP
- Tunnel access via VPN, IPSec, SSH
- Network monitoring for anomalous detections e.g. repeated failed attempts from external IP access

SHADOWSERVER

Verifying our results

- False positives are not really possible with this scan
- If you would like to test your own device to verify it has RDP accessible, try the nmap command: "nmap -v --script=ssl-cert -p 3389 [IP]”
    - Make sure your queries are not being filtered
- Remember the scan results we share are for the previous day (up to 24 hour delay)

Summary & Key Report Pages

Reports overview

- https://www.shadowserver.org/what-we-do/network-reporting/get-reports/
- https://www.shadowserver.org/what-we-do/network-reporting/
- https://www.shadowserver.org/what-we-do/network-reporting/accessible-rdp-report/

Report Updates

- https://www.shadowserver.org/news-insights/
- Twitter @shadowserver
- Mailing list access send request to contact@shadowserver.org and request access to public@shadowserver.org
- Or subscribe directly at https://mail.shadowserver.org/mailman/listinfo/public

Reports API

- Request access to contact@shadowserver.org
- https://www.shadowserver.org/what-we-do/network-reporting/api-documentation/
- https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/

SHADOWSERVER

Lighting the way to a more secure Internet

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG