



Pentester – Wie starte ich einen Angriff?

Modul D3.2

Referent: Dr. Jörg Cosfeld

Pentester – Eine Definition

Sicherheitsprüfungen eigener **Systeme** gibt es unter vielerlei Namen, zum Beispiel **Schwachstellenanalysten** und -bewertung oder **Ethical Hacker** oder eben **Penetrationstester**, kurz **Pentester**.



[1]

Pentester – Eine Definition

Spektrum reicht von **Sicherheitsanalysen einzelner Applikationen** oder Systeme bis hin zur **Simulation zielgerichteter Angriffe**.



[1]

Pentester – Eine Definition

Spektrum reicht von **Sicherheitsanalysen einzelner Applikationen** oder Systeme bis hin zur **Simulation zielgerichteter Angriffe.**



[1]

Pentester – Eine Definition

Spektrum reicht von **Sicherheitsanalysen einzelner Applikationen** oder Systeme bis hin zur **Simulation zielgerichteter Angriffe.**

Red Team Assessments

Dabei überprüfen **Pentester**, wie gut Systeme und Mitarbeiter zur **Erkennung** und **Abwehr** von Angriffsversuchen ausgerüstet sind.

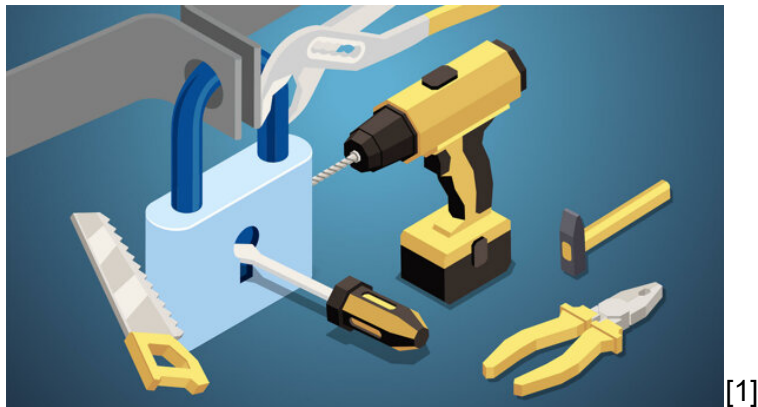


Pentester – Eine Definition

Spektrum reicht von **Sicherheitsanalysen einzelner Applikationen** oder Systeme bis hin zur **Simulation zielgerichteter Angriffe.**

Red Team Assessments

Dabei überprüfen **Pentester**, wie gut Systeme und Mitarbeiter zur **Erkennung** und **Abwehr** von Angriffsversuchen ausgerüstet sind.



Pentester – Eine Definition

Reminder Lecture 3.1.

Spektrum reicht von Sicherheitsanalysen einzelner Applikationen oder Systeme bis hin zur **Simulation zielgerichteter Angriffe.**

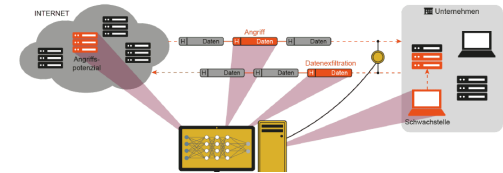
Red Team Assessments

Dabei überprüfen **Pentester**, wie gut Systeme und Mitarbeiter zur **Erkennung** und **Abwehr** von Angriffsversuchen ausgerüstet sind.

Frühwarnsysteme – Angriffe erkennen

Definition:

- Früh Angriffspotenziale und reale Angriffe zu erkennen, um rechtzeitig Warnhinweise zu geben.
- Sicherheit und Vertrauenswürdigkeit von IT-Systemen und IT-Infrastruktur nachhaltig zu erhöhen und widerstandsfähiger zu gestalten



Pentester – Eine Definition

Spektrum reicht von **Sicherheitsanalysen einzelner Applikationen** oder Systeme bis hin zur **Simulation zielgerichteter Angriffe.**

Red Team Assessments

Dabei überprüfen **Pentester**, wie gut Systeme und Mitarbeiter zur **Erkennung** und **Abwehr** von Angriffsversuchen ausgerüstet sind.

Inhalt dieser Vorlesung?

- **Unternehmen beauftragt uns als Pentester**

Pentester – Eine Definition

Spektrum reicht von **Sicherheitsanalysen einzelner Applikationen** oder Systeme bis hin zur **Simulation zielgerichteter Angriffe.**

Red Team Assessments

Dabei überprüfen **Pentester**, wie gut Systeme und Mitarbeiter zur **Erkennung** und **Abwehr** von Angriffsversuchen ausgerüstet sind.

Inhalt dieser Vorlesung?

- Unternehmen beauftragt uns als Pentester
- **Einbruch** in die Systeme des Unternehmens
Rheinische Post

Pentester – Eine Definition



Pentester – Eine Definition

Spektrum reicht von **Sicherheitsanalysen einzelner Applikationen** oder Systeme bis hin zur **Simulation zielgerichteter Angriffe.**

Red Team Assessments

Dabei überprüfen **Pentester**, wie gut Systeme und Mitarbeiter zur **Erkennung** und **Abwehr** von Angriffsversuchen ausgerüstet sind.

Inhalt dieser Vorlesung?

- Unternehmen beauftragt uns als Pentester
- **Einbruch** in die Systeme des Unternehmens
Rheinische Post
- **Ohne jegliche Vorkenntnisse**

Pentester – Eine Definition

Einbruch in die Rheinische Post: **RP ONLINE**

- Firma beauftragt einen Blackbox – Test
- Wir wissen nichts über das Zielsystem

7 Tage Zeit

Pentester – Eine Definition

Einbruch in die Rheinische Post: **RP ONLINE**

- Firma beauftragt einen **Blackbox – Test**
- Wir wissen nichts über das Zielsystem



Whitebox – Test, wir verfügen über Insider Wissen

Pentester – Eine Definition

Einbruch in die Rheinische Post: **RP ONLINE**

- Firma beauftragt einen **Blackbox – Test**
- Wir wissen nichts über das Zielsystem

Pentester – Eine Definition

Einbruch in die Rheinische Post:  RP ONLINE

- Firma beauftragt einen **Blackbox – Test**
- Wir wissen nichts über das Zielsystem

Erste Anhaltspunkte:



MITRE | ATT&CK®

Pentester – Eine Definition

Einbruch in die Rheinische Post:  RP ONLINE

- Firma beauftragt einen **Blackbox – Test**
- Wir wissen nichts über das Zielsystem

Erste Anhaltspunkte:



MITRE | ATT&CK®

- Globale Bibliothek an Techniken zum Angriff
- Umfasst Taktik, Technik und Softwareprodukte

Pentester – Eine Definition

ATT&CK®

Pentester – Eine Definition

Einbruch in die Rheinische Post: **RP ONLINE**

- Alle frei zugänglichen Quellen werden nach Informationen durchsucht

Enterprise



Windows



Drive by Compromise

Pentester – Eine Definition

Einbruch in die Rheinische Post:  RP ONLINE

- Alle frei zugänglichen Quellen werden nach Informationen durchsucht
- DNS Records werden durchsucht mit den tools **Spiderfoot** und **Shodan**.

Pentester – Eine Definition

Einbruch in die Rheinische Post: **RP ONLINE**



Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE



Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

- Alle frei zugänglichen Quellen werden nach Informationen durchsucht
- DNS Records werden durchsucht mit den tools **Spiderfoot** und **Shodan**.

Umfassendes Register an **IP Adressen** und **DNS Einträgen**.

Auch **Zertifikate**.

Pentester – Eine Definition

Einbruch in die Rheinische Post:  **RP ONLINE**

- Alle frei zugänglichen Quellen werden nach Informationen durchsucht
- DNS Records werden durchsucht mit den tools **Spiderfoot** und **Shodan**.

Spiderfoot gibt ein direkte Kategorie **Hackertarget** aus.

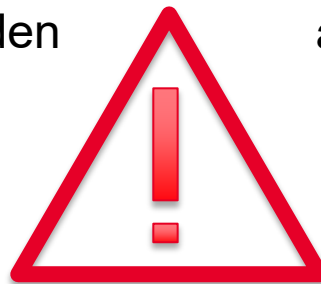
Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

- Alle frei zugänglichen Quellen werden nach Informationen durchsucht
- DNS Records werden durchsucht mit den tools **Spiderfoot** und **Shodan**.

Spiderfoot gibt ein direkte Kategorie **Hackertarget** aus.



Wir fallen hiermit schon auf!

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

- Alle frei zugänglichen Quellen werden nach Informationen durchsucht
- DNS Records werden durchsucht mit den tools **Spiderfoot** und **Shodan**.

Spiderfoot gibt ein direkte Kategorie **Hackertarget** aus.

Entweder wird es nur notiert oder direkt blockiert.

Pentester – Eine Definition

Einbruch in die Rheinische Post:  RP ONLINE

- Alle frei zugänglichen Quellen werden nach Informationen durchsucht
- DNS Records werden durchsucht mit den tools **Spiderfoot** und **Shodan**.

Spiderfoot gibt ein direkte Kategorie **Hackertarget** aus.

Entweder wird es nur notiert oder direkt blockiert.

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

- Alle frei zugänglichen Quellen werden nach Informationen durchsucht
- DNS Records werden durchsucht mit den tools **Spiderfoot** und **Shodan**.

Unternehmen durforsten ständig die Konkurrenz.

Es besteht ein Grundrauschen.

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

- DNS Records werden durchsucht mit den tools **Spiderfoot** und **Shodan**.
- Snippets im DNS Ergebnis verraten erste Serverstrukturen
 - **VPN – OWA - CITRIX**

Pentester – Eine Definition

Einbruch in die Rheinische Post:  **RP ONLINE**

- DNS Records werden durchsucht mit den tools **Spiderfoot** und **Shodan**.
- Snippets im DNS Ergebnis verraten erste Serverstrukturen
 - **VPN – OWA – CITRIX**
- **Open TCP Ports** können zu bestimmter Software passen
 - **VoIP Anlage** benötigt gewisse offene Ports

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

- DNS Records werden durchsucht mit den tools **Spiderfoot** und **Shodan**.
- Snippets im DNS Ergebnis verraten erste Serverstrukturen
 - **VPN – OWA – CITRIX**
- RP-online betreibt einen **apache Webserver**

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE



The screenshot shows the WinFuture website interface. At the top, there's a navigation bar with 'Startseite', 'Ticker', 'Downloads', 'Videos', 'Forum', 'Preisvergleich', and 'Mehr'. Below this is a secondary navigation bar with 'Internet', 'Sicherheit', 'Sicherheitslücken', 'Meltdown und Spectre', 'Hacker', 'Viren & Trojaner', and 'Spam & Phishing'. The main content area features a news article titled 'Apache: Zero Day-Lücke lässt den Server sehr sensible Daten leaken'. The article text states: 'Der meistgenutzte Webserver der Welt hat mit einem gravierenden Sicherheitsproblem zu kämpfen. Eine Zero-Day-Schwachstelle in Apache sollte von allen Nutzern der Software umgehend gepatcht werden, um mögliche gravierende Folgen zu verhindern.' To the right of the article, there's a sidebar with metadata: 'Datum: Mittwoch, 06.10.2021 10:39 Uhr', 'Mehr: Sicherheitslücken', 'Autor: Christian Kahle', and '1 Kommentar'.

- RP-online betreibt einen **apache Webserver**

Pentester – Eine Definition

Einbruch in die Rheinische Post:

~~RP ONLINE~~

Hochschule Düsseldorf
University of Applied Sciences

HSD

- DNS Records zeigen
 - **HSD hat zwei DNS Server**

The screenshot displays two DNS record entries for the domain `zdns01.hs-duesseldorf.de` and `zdns02.hs-duesseldorf.de`. Each entry includes a toolbar with icons for Internet Name, DNS Resolver, and other tools. The DNS records show the following information:

- Internet Name: `zdns01.hs-duesseldorf.de` (highlighted in orange)
- DNS Resolver: `zdns01.hs-duesseldorf.de` (highlighted in orange)
- Domain Whois: `zdns01.hs-duesseldorf.de` (highlighted in orange)
- Whois: `zdns01.hs-duesseldorf.de` (highlighted in orange)
- Restricted rights.
- Terms and Conditions of Use

The same information is displayed for `zdns02.hs-duesseldorf.de` (highlighted in yellow).

Pentester – Eine Definition

Einbruch in die Rheinische Post:



- Einsatz des tools Nessus
 - **Ports der Adressen werden abgescannt**

Pentester – Eine Definition

Einbruch in die Rheinische Post:



- Einsatz des tools Nessus
 - **Ports der Adressen werden abgescannt**



**Der Goldstandard in Sachen Schwachstellenbewertung.
Konzipiert für die moderne Angriffsoberfläche.**

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

- Einsatz des tools Nessus
 - Ports der Adressen werden abgescannt



**Der Goldstandard in Sachen Schwachstellenbewertung.
Konzipiert für die moderne Angriffsoberfläche.**

Kostenlos testen > Jetzt kaufen ▾

Nessus Professional kaufen

Nessus® ist der umfassendste Schwachstellen-Scanner auf dem Markt. Nessus Professional unterstützt Sie bei der Automatisierung des Scan-Prozesses, spart Zeit in Ihren Compliance-Zyklen und ermöglicht Ihnen die Einbindung Ihres IT-Teams.

Mehrjahreslizenz kaufen und sparen! Mit Advanced Support erhalten Sie rund um die Uhr, 365 Tage im Jahr Zugang zum Support – per Telefon, Chat und über die Community.

LIZENZ AUSWÄHLEN

Mehrjahreslizenz kaufen und sparen!

<input checked="" type="radio"/>	1 Jahr - 4.463,69 €* Weitere Informationen
<input type="radio"/>	2 Jahre - 8.704,18 €* (Sie sparen 223,18 €) Weitere Informationen
<input type="radio"/>	3 Jahre - 12.721,48 €* (Sie sparen 669,55 €) Weitere Informationen

Support und Training hinzufügen

<input checked="" type="checkbox"/>	Advanced Support - 526,68 € 24x365 Access to phone, email, community, and chat support. Weitere Informationen
<input type="checkbox"/>	On-Demand Training - 256,77 € 1 Jahr Zugriff auf den Online-Videokurs „Nessus Fundamentals“ für 1 Person. Weitere Informationen

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

The screenshot shows the Nessus Scans interface. The top navigation bar includes the Nessus logo, 'Scans', and 'Settings' tabs. On the right, there are icons for help, notifications, and a user profile labeled 'locdoc89'. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Customized Reports, Terrascan). The main area is titled 'My Scans' and features a search bar with '4 Scans' results. Below is a table of scans:

<input type="checkbox"/>	Name	Schedule	Last Scanned		
<input type="checkbox"/>	apache l4j rp-online.de	On Demand	✓ Today at 12:12 PM	▶	✕
<input type="checkbox"/>	rp-online.de	On Demand	✓ Today at 11:38 AM	▶	✕
<input type="checkbox"/>	rp-online	On Demand	✓ Today at 11:31 AM	▶	✕
<input type="checkbox"/>	HSD	On Demand	✓ Today at 11:27 AM	▶	✕

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

The screenshot displays the Nessus web interface. The top navigation bar includes the Nessus logo, 'Scans', and 'Settings' tabs. On the left, a sidebar lists 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Customized Reports, Terrascan). The main content area shows the 'Nessus SYN scanner' plugin details. It includes a 'Description' section with a note about SYN scans being less intrusive than TCP scans, a 'Solution' section advising to use an IP filter, and an 'Output' section showing a scan result for port 80/tcp on www.rp-online.de. On the right, a 'Plugin Details' sidebar lists attributes: Severity (Info), ID (11219), Version (1.45), Type (remote), Family (Port scanners), Published (February 4, 2009), and Modified (August 15, 2022). Below this, a 'Risk Information' section shows a 'Risk Factor: None'.

INFO Nessus SYN scanner

Description
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution
Protect your target with an IP filter.

Output

```
Port 80/tcp was found to be open
```

To see debug logs, please visit individual host

Port	Hosts
80 / tcp / www	www.rp-online.de

Plugin Details

Severity: Info
ID: 11219
Version: 1.45
Type: remote
Family: Port scanners
Published: February 4, 2009
Modified: August 15, 2022

Risk Information

Risk Factor: None

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

The screenshot displays the Nessus web interface. The top navigation bar includes the Nessus logo, 'Scans', and 'Settings' tabs. On the left sidebar, there are sections for 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Customized Reports, Terrascan). The main content area shows the 'Nessus SYN scanner' plugin details. It includes a description of the plugin as a SYN 'half-open' port scanner, a note about its intrusiveness compared to TCP scans, and a solution to protect targets with an IP filter. The 'Output' section shows a scan result for port 234/tcp on the host www.rp-online.de. On the right, the 'Plugin Details' section lists metadata such as Severity (Info), ID (11219), Version (1.45), Type (remote), Family (Port scanners), Published date (February 4, 2009), and Modified date (August 15, 2022). The 'Risk Information' section at the bottom right indicates a 'Risk Factor: None'.

INFO Nessus SYN scanner

Description
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution
Protect your target with an IP filter.

Output

Port 234/tcp was found to be open

To see debug logs, please visit individual host

Port	Hosts
234 / tcp / ssh	www.rp-online.de

Plugin Details

Severity: Info
ID: 11219
Version: 1.45
Type: remote
Family: Port scanners
Published: February 4, 2009
Modified: August 15, 2022

Risk Information
Risk Factor: None

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

The screenshot displays the Nessus web interface. The top navigation bar includes the Nessus logo, 'Scans', and 'Settings' tabs. On the left sidebar, there are sections for 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Customized Reports, Terrascan). The main content area shows the 'Nessus SYN scanner' plugin details. It includes a description of the SYN 'half-open' port scanner, a note about its intrusiveness compared to TCP scans, and a solution to protect targets with an IP filter. The 'Output' section shows a scan result for port 443/tcp on www.rp-online.de. On the right, the 'Plugin Details' sidebar lists metadata such as Severity (Info), ID (11219), Version (1.45), Type (remote), Family (Port scanners), Published date (February 4, 2009), and Modified date (August 15, 2022). The 'Risk Information' section at the bottom right indicates a 'Risk Factor: None'.

nessus Scans Settings

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Terrascan

INFO Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

Port 443/tcp was found to be open

To see debug logs, please visit individual host

Port	Hosts
443 / tcp / www	www.rp-online.de

Plugin Details

Severity: Info
ID: 11219
Version: 1.45
Type: remote
Family: Port scanners
Published: February 4, 2009
Modified: August 15, 2022

Risk Information

Risk Factor: None

Pentester – Eine Definition

Einbruch in die Rheinische Post:



Portscan protection der Firewall verhindert.

- **Ports 80, 234, 443 sind common Ports**

Pentester – Eine Definition

Einbruch in die Rheinische Post:



Portscan protection der Firewall verhindert.

- **Ports 80, 234, 443 sind common Ports**
- **Keinen Mehrwert generiert.**

Pentester – Eine Definition

Einbruch in die Rheinische Post:



Portscan protection der Firewall verhindert.

- **Ports 80, 234, 443 sind common Ports**
- **Keinen Mehrwert generiert.**

Weitere Schwachstellensuche notwendig.

Pentester – Eine Definition

Einbruch in die Rheinische Post:



Portscan protection der Firewall verhindert.

- **Ports 80, 234, 443 sind common Ports**
- **Keinen Mehrwert generiert.**

Weitere Schwachstellensuche notwendig.

Pentester – Eine Definition

Einbruch in die Rheinische Post:



Portscan protection der Firewall verhindert.

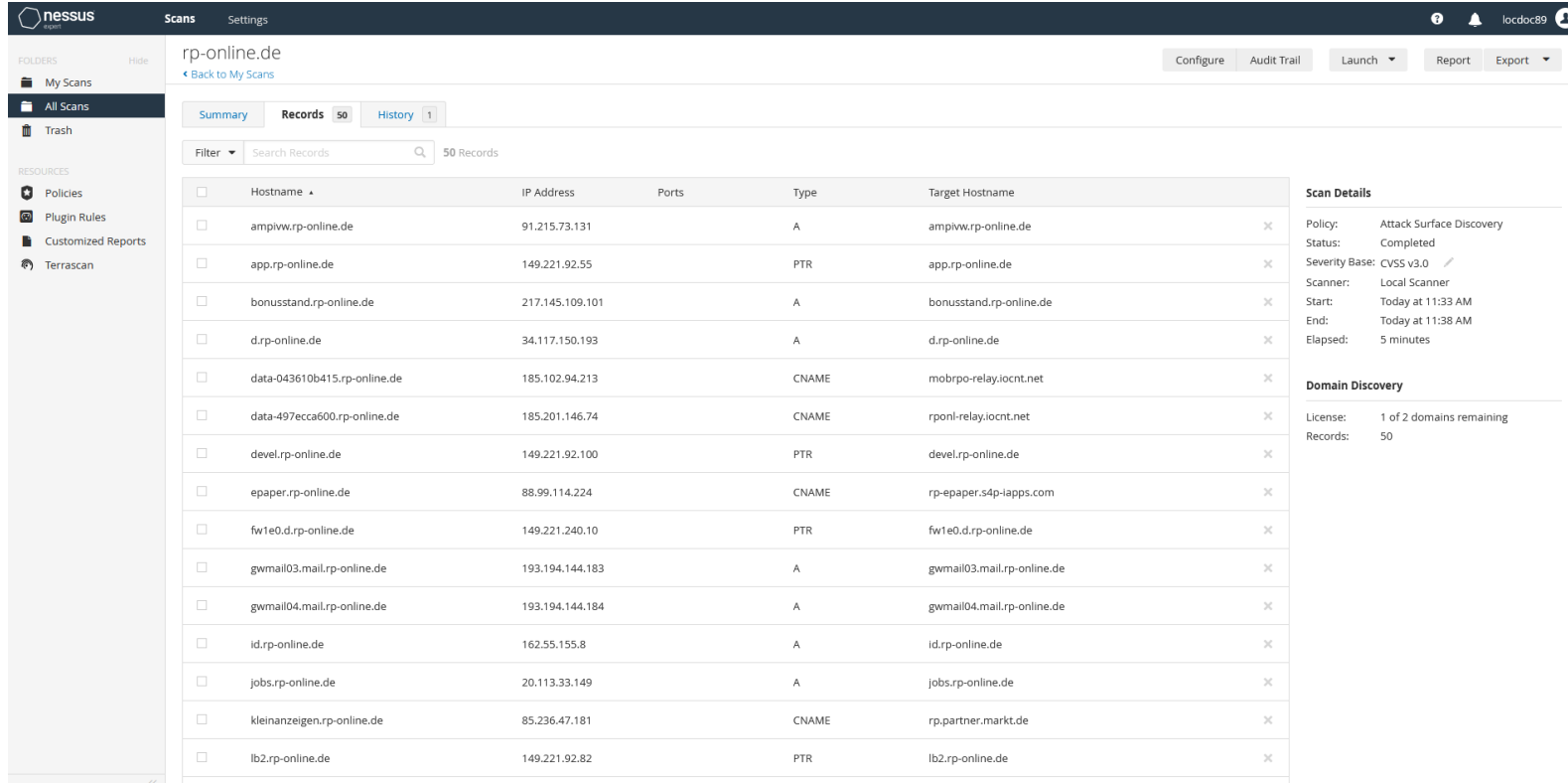
- **Ports 80, 234, 443 sind common Ports**
- **Keinen Mehrwert generiert.**



Ansurfen aller IP Adressen. Mit dem Fully-Qualified Domain Name

FQDN

Pentester – Eine Definition



The screenshot displays the Nessus web interface for a scan of **rp-online.de**. The interface includes a sidebar with navigation options like Folders, My Scans, All Scans, Trash, Resources, Policies, Plugin Rules, Customized Reports, and Terrascan. The main content area displays a table of scan results for **rp-online.de**, including Hostname, IP Address, Ports, Type, and Target Hostname. The table lists 15 entries, such as **ampiwv.rp-online.de**, **app.rp-online.de**, **bonusstand.rp-online.de**, **d.rp-online.de**, **data-043610b415.rp-online.de**, **data-497ecca600.rp-online.de**, **devel.rp-online.de**, **epaper.rp-online.de**, **fw1e0.d.rp-online.de**, **gwmail03.mail.rp-online.de**, **gwmail04.mail.rp-online.de**, **id.rp-online.de**, **jobs.rp-online.de**, **kleinanzeigen.rp-online.de**, and **lb2.rp-online.de**. The right sidebar shows Scan Details (Policy: Attack Surface Discovery, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 11:33 AM, End: Today at 11:38 AM, Elapsed: 5 minutes) and Domain Discovery (License: 1 of 2 domains remaining, Records: 50).

Hostname	IP Address	Ports	Type	Target Hostname
ampiwv.rp-online.de	91.215.73.131		A	ampiwv.rp-online.de
app.rp-online.de	149.221.92.55		PTR	app.rp-online.de
bonusstand.rp-online.de	217.145.109.101		A	bonusstand.rp-online.de
d.rp-online.de	34.117.150.193		A	d.rp-online.de
data-043610b415.rp-online.de	185.102.94.213		CNAME	mobrpo-relay.iocnt.net
data-497ecca600.rp-online.de	185.201.146.74		CNAME	rponl-relay.iocnt.net
devel.rp-online.de	149.221.92.100		PTR	devel.rp-online.de
epaper.rp-online.de	88.99.114.224		CNAME	rp-epaper.s4p-iapps.com
fw1e0.d.rp-online.de	149.221.240.10		PTR	fw1e0.d.rp-online.de
gwmail03.mail.rp-online.de	193.194.144.183		A	gwmail03.mail.rp-online.de
gwmail04.mail.rp-online.de	193.194.144.184		A	gwmail04.mail.rp-online.de
id.rp-online.de	162.55.155.8		A	id.rp-online.de
jobs.rp-online.de	20.113.33.149		A	jobs.rp-online.de
kleinanzeigen.rp-online.de	85.236.47.181		CNAME	rp.partner.markt.de
lb2.rp-online.de	149.221.92.82		PTR	lb2.rp-online.de

Pentester – Eine Definition

The screenshot displays the Nessus web interface. On the left, a sidebar contains navigation links for 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Customized Reports, Tarrscan). The main content area is titled 'rp-online.de / Details' and includes a 'Back to Records' link. A red rectangle highlights the 'Attack Surface Discovery' plugin button. Below this, the 'Description' states: 'This plugin provides a view into your external attack surface by discovering DNS records and subdomains related to your top level domains.' The 'Output' section shows a report for 'tools.rp-online.de[149.221.198.195]' with details like 'Initial data: true', 'Full data available: 2022-11-04T10:33:57.000Z', 'Data refreshed: 2022-11-09T10:38:59.920Z', 'Record type: A', and 'IP: 149.221.198.195'. A table below the output shows 'Port' as 'N/A' and 'Hosts' as 'tools.rp-online.de-A[149.221.198.195-tools.rp-online.de]'. On the right, 'Plugin Details' lists: Severity: Info, ID: 161479, Version: 1.8, Type: remote, Family: Misc, Published: July 11, 2022, Modified: October 17, 2022. 'Risk Information' shows 'Risk Factor: None'.

nessus

Scans Settings

rp-online.de / Details

Configure Audit Trail Launch Report Export

Details

Attack Surface Discovery

Description

This plugin provides a view into your external attack surface by discovering DNS records and subdomains related to your top level domains.

Output

```
Report for tools.rp-online.de[149.221.198.195] (tools.rp-online.de):  
Initial data: true  
Full data available: 2022-11-04T10:33:57.000Z  
Data refreshed: 2022-11-09T10:38:59.920Z  
Record type: A  
IP: 149.221.198.195
```

To see debug logs, please visit individual host

Port	Hosts
N/A	tools.rp-online.de-A[149.221.198.195-tools.rp-online.de]

Plugin Details

Severity: Info
ID: 161479
Version: 1.8
Type: remote
Family: Misc.
Published: July 11, 2022
Modified: October 17, 2022

Risk Information

Risk Factor: None

Pentester – Eine Definition

Einbruch in die Rheinische Post:



<https://d.rp-online.de/>

<https://bonusstand.rp-online.de/>

<https://tools.rp-online.de/>



Ansurfen aller IP Adressen. Mit dem Fully-Qualified Domain Name

FQDN

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

<https://d.rp-online.de/>

<https://bonusstand.rp-online.de/>

<https://tools.rp-online.de/>

**Kann direkt
angegriffen
werden.**



Ansurfen aller IP Adressen. Mit dem Fully-Qualified Domain Name

FQDN

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

<https://d.rp-online.de/>

<https://bonusstand.rp-online.de/>

<https://tools.rp-online.de/>

**Lahmlegen
durch DDoS**



**Kann direkt
angegriffen
werden.**



Ansurfen aller IP Adressen. Mit dem Fully-Qualified Domain Name
FQDN

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

<https://mail.kunstakademie-duesseldorf.de/>

<https://tools.rp-online.de/>



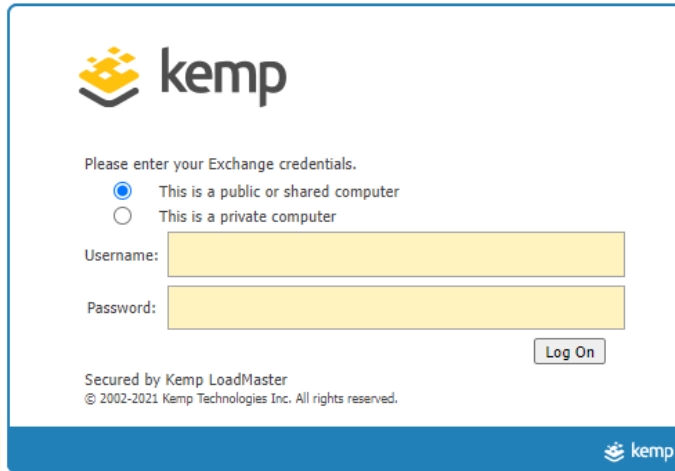
Ansurfen aller IP Adressen. Mit dem Fully-Qualified Domain Name

FQDN

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE



 **kemp**

Please enter your Exchange credentials.

☒ This is a public or shared computer
☐ This is a private computer

Username:

Password:

Secured by Kemp LoadMaster
© 2002-2021 Kemp Technologies Inc. All rights reserved.

 **kemp**

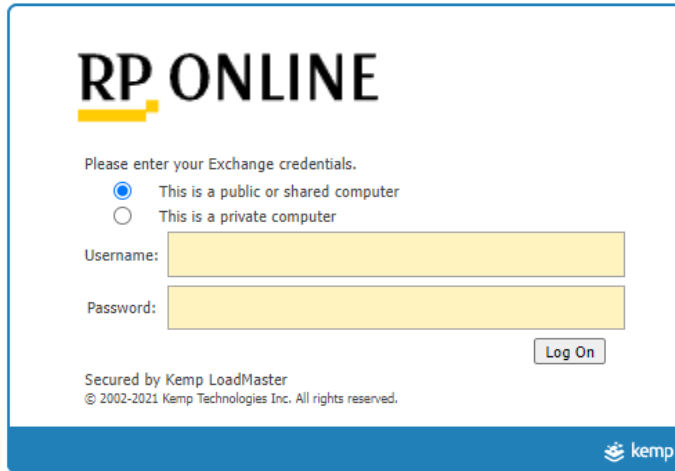
Kunstakademie Düsseldorf verfügt
über eine Web Application Firewall

WAF

Load Balancer schützt vor DDoS

Pentester – Eine Definition

Einbruch in die Rheinische Post:

A screenshot of the RP ONLINE login page. The page has a white background with a blue border. At the top left is the "RP ONLINE" logo. Below it, the text "Please enter your Exchange credentials." is displayed. There are two radio buttons: the first is selected and labeled "This is a public or shared computer", and the second is unselected and labeled "This is a private computer". Below these are two yellow input fields for "Username:" and "Password:". A "Log On" button is located to the right of the password field. At the bottom left, it says "Secured by Kemp LoadMaster" and "© 2002-2021 Kemp Technologies Inc. All rights reserved.". At the bottom right is the Kemp logo.

Annahme:

Reverse Proxy ist exestiert für

<https://tools.rp-online.de/>

Pentester – Eine Definition

Einbruch in die Rheinische Post:



Keine offenen Schwachstellen erkennbar.

Was verleibt als Notnagel?

Pentester – Eine Definition

Einbruch in die Rheinische Post:



Keine offenen Schwachstellen erkennbar.

Was verleibt als Notnagel?

Faktor Mensch



Pentester – Eine Definition

Einbruch in die Rheinische Post:



Keine offenen Schwachstellen erkennbar.

Was verleiht als Notnagel?

Faktor Mensch

**Wir versuchen eine Phishing
Attacke.**



Pentester – Eine Definition

Einbruch in die Rheinische Post:



- Zurück zu Spinderfoot.
- Ausgabe der Mailadresse durchsuchen.

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

Overview Correlations... Browse by... Starred Annotated Visualize... Settings State Logs									
Data Summary > Data Type: Email Address (49 results)									
Data Element					Source Data Element				
<input type="checkbox"/>	Email Address	Skymem	0	1	Internet Name	SpiderFoot UI	134	0	
	hf@rp-online.de				rp-online.de				
<input type="checkbox"/>	Email Address	Skymem	0	1	Internet Name	SpiderFoot UI	134	0	
	datenschutz@rp-online.de				rp-online.de				
<input type="checkbox"/>	Email Address	Skymem	0	1	Internet Name	SpiderFoot UI	134	0	
	regiobilder@rp-online.de				rp-online.de				
<input type="checkbox"/>	Email Address	Skymem	0	1	Internet Name	SpiderFoot UI	134	0	
	opinio@rp-online.de				rp-online.de				
<input type="checkbox"/>	Email Address	Skymem	0	1	Internet Name	SpiderFoot UI	134	0	
	feedback@rp-online.de				rp-online.de				

Pentester – Eine Definition

Einbruch in die Rheinische Post:



- Zurück zu Spinderfoot.
- Ausgabe der Mailadresse durchsuchen.

Wegwerf Mailadresse fragt nach dem Uploadbereich einer Initiativ Bewerbung.

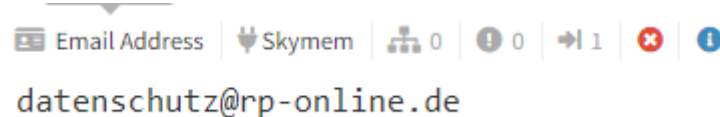
Pentester – Eine Definition

Einbruch in die Rheinische Post:



- Zurück zu Spinderfoot.
- Ausgabe der Mailadresse durchsuchen.

Wegwerf Mailadresse fragt nach Datenschutzbeschwerde.



Wir erhalten folgende Signatur in der Antwort.

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

Ihre

Rheinische Post

RHEINISCHE POST Neuß-Oberebendorfer Zeitung BERGISCHE MORGENPOST

SOLINGER MORGENPOST RP ONLINE

Rheinische Post Verlagsgesellschaft mbH

Leserservice

Zülpicher Straße 10 · 40196 Düsseldorf

Tel. +49 (211) 505-1111

leserservice.app@rheinische-post.de

www.rp-online.de

www.rheinischepostmediengruppe.de

twitter.com/rponline

facebook.com/rponline

Vorsitzender des Aufsichtsrats: Felix Droste

Geschäftsführer: Johannes Werle, Patrick Ludwig, Hans Peter Bork, Matthias Körner

Sitz Düsseldorf · Amtsgericht Düsseldorf HRB 68

USt-IdNr.: DE 121 306 412

**Wegwerf Mailadresse fragt nach
Datenschutzbeschwerde.**

Email Address Skymem 0 0 1 x i

datenschutz@rp-online.de

**Wir erhalten folgende Signatur in
der Antwort.**

Pentester – Eine Definition

Einbruch in die Rheinische Post:

RP ONLINE

Ihre

Rheinische Post

RHEINISCHE POST Neuß-Oberebendorfer Zeitung BERGISCHE MORGENPOST

SOLINGER MORGENPOST RP ONLINE

Rheinische Post Verlagsgesellschaft mbH

Leserservice

Zülpicher Straße 10 · 40196 Düsseldorf

Tel. +49 (211) 505-1111

leserservice.app@rheinische-post.de

www.rp-online.de

www.rheinischepostmediengruppe.de

twitter.com/rponline

facebook.com/rponline

Vorsitzender des Aufsichtsrats: Felix Droste

Geschäftsführer: Johannes Werle, Patrick Ludwig, Hans Peter Bork, Matthias Körner

Sitz Düsseldorf · Amtsgericht Düsseldorf HRB 68

USt-IdNr.: DE 121 306 412

**Wegwerf Mailadresse fragt nach
Datenschutzbeschwerde.**

Email Address Skymem 0 0 1 x i

datenschutz@rp-online.de

**Wir erhalten folgende Signatur in
der Antwort.**

Pentester – Eine Definition

Einbruch in die Rheinische Post:

Ihre

Rheinische Post

RHEINISCHE POST Neuß-Oberebener Zeitung BERGISCHE MORGENPOST

SOLINGER MORGENPOST RP ONLINE

Rheinische Post Verlagsgesellschaft mbH

Leserservice

Zülpicher Straße 10 · 40196 Düsseldorf

Tel. +49 (211) 505-1111

leserservice.app@rheinische-post.de

www.rp-online.de

www.rheinischepostmediengruppe.de

twitter.com/rponline

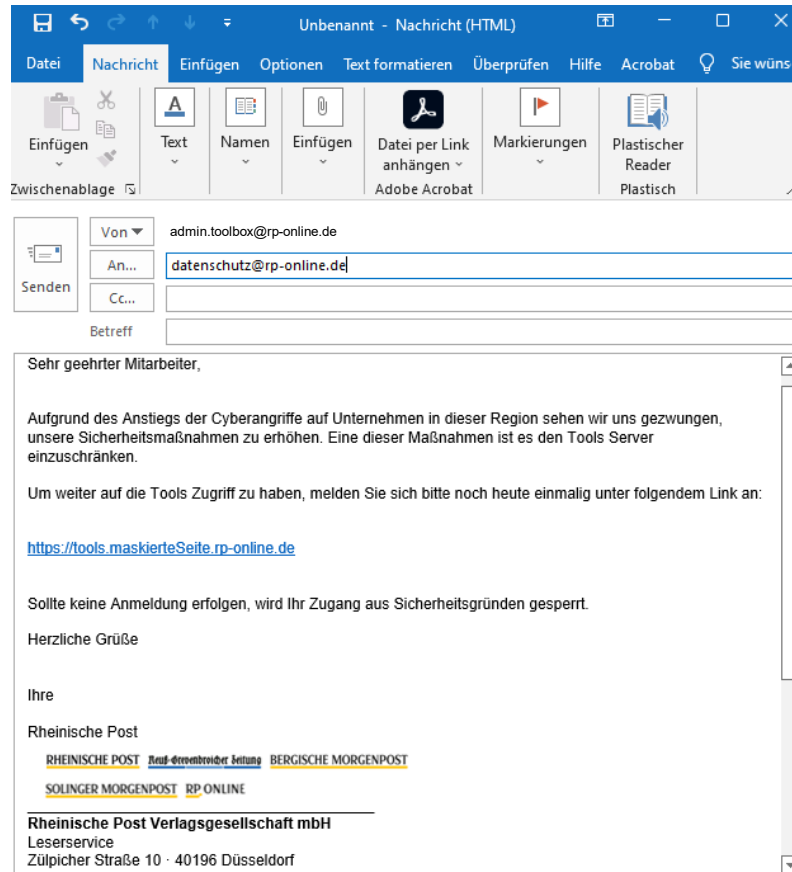
facebook.com/rponline

Vorsitzender des Aufsichtsrats: Felix Droste

Geschäftsführer: Johannes Werle, Patrick Ludwig, Hans Peter Bork, Matthias Körner

Sitz Düsseldorf · Amtsgericht Düsseldorf HRB 68

UST-IdNr.: DE 121 306 412



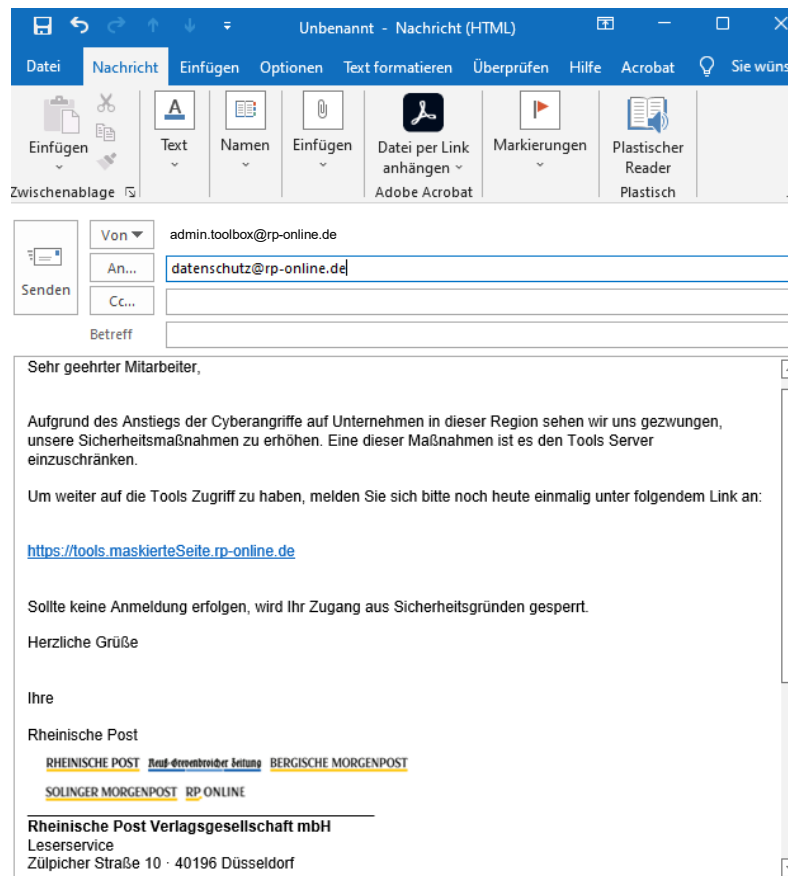
Pentester – Eine Definition

Einbruch in die Rheinische Post:

```

  _____
 /_ _ _ _ _ \
| 7phisher  |
|_____    |
|          |
| Version : 2.3.1
|
| [-] Tool Created by htr-tech (tahmid.rayat)
|
| [::] Select An Attack For Your Victim [::]
|
| [01] Facebook      [11] Twitch      [21] DeviantArt
| [02] Instagram    [12] Pinterest   [22] Badoo
| [03] Google        [13] Snapchat    [23] Origin
| [04] Microsoft     [14] LinkedIn   [24] DropBox
| [05] Netflix       [15] Ebay        [25] Yahoo
| [06] Paypal         [16] Quora       [26] Wordpress
| [07] Steam          [17] Protonmail  [27] Yandex
| [08] Twitter        [18] Spotify    [28] StackoverFlow
| [09] Playstation   [19] Reddit     [29] Vk
| [10] Tiktok         [20] Adobe      [30] XBOX
| [31] Mediafire      [32] Gitlab     [33] Github
| [34] Discord
|
| [99] About          [00] Exit
|
| [-] Select an option : 0

```



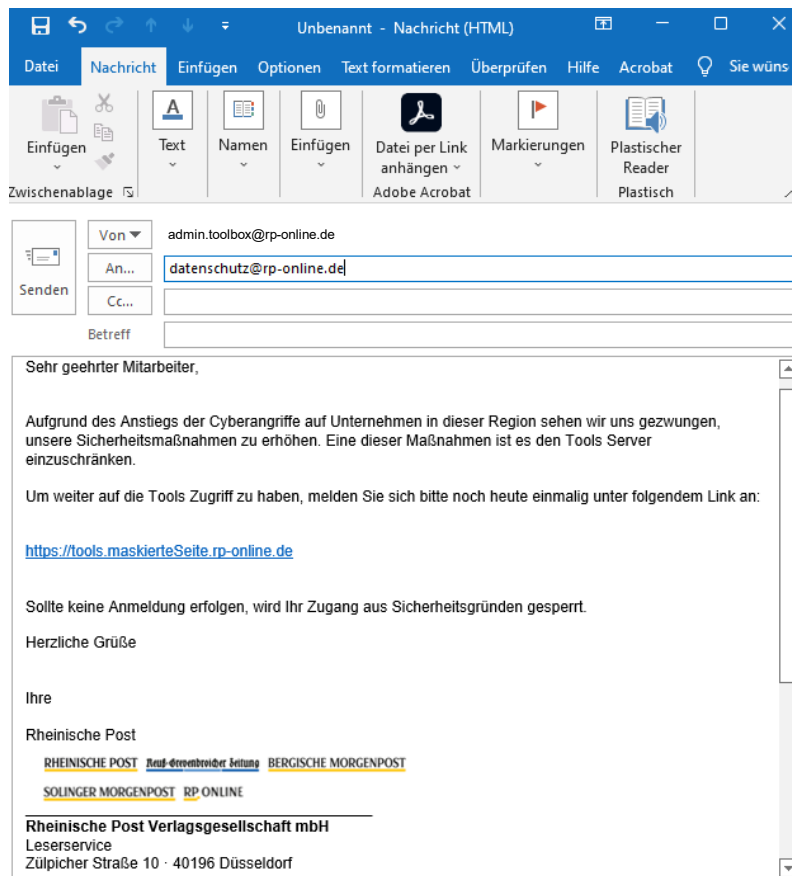
Pentester – Eine Definition

Einbruch in die Rheinische Post:



Zphisher baut uns die Fake Website

<https://tools.maskierteSeite.rp-online.de>



Pentester – Eine Definition

Einbruch in die Rheinische Post:



Zphisher baut uns die Fake Website

<https://tools.maskierteSeite.rp-online.de>

RHEINISCHE POST

Haben Sie ein Zeitungs-Abonnement?
[Schalten Sie hier Ihren Zugang frei.](#)

ANMELDUNG

E-MAIL *

PASSWORT *

[PASSWORT VERGESSEN?](#)

ANMELDEN

Noch nicht registriert? [Hier registrieren](#)

Pentester – Eine Definition

Einbruch in die Rheinische Post:

Data Element

<input type="checkbox"/>	Email Address	Skymem	0	0	1	0	1
	hf@rp-online.de						
<input type="checkbox"/>	Email Address	Skymem	0	0	1	0	1
	datenschutz@rp-online.de						
<input type="checkbox"/>	Email Address	Skymem	0	0	1	0	1
	regiobilder@rp-online.de						
<input type="checkbox"/>	Email Address	Skymem	0	0	1	0	1
	opinio@rp-online.de						
<input type="checkbox"/>	Email Address	Skymem	0	0	1	0	1
	feedback@rp-online.de						
<input type="checkbox"/>	Email Address	Skymem	0	0	1	0	1
	sp@rp-online.de						
<input type="checkbox"/>	Email Address	Skymem	0	0	1	0	1
	frank@rp-online.de						
<input type="checkbox"/>	Email Address	Skymem	0	0	1	0	1



Unbenannt - Nachricht (HTML)

Datei Nachricht Einfügen Optionen Text formatieren Überprüfen Hilfe Acrobat Sie wüns

Einfügen Text Namen Einfügen Datei per Link anhängen Markierungen Plastischer Reader

Zwischenablage

Von admin.toolbox@rp-online.de

An... datenschutz@rp-online.de

Cc...

Betreff

Sehr geehrter Mitarbeiter,

Aufgrund des Anstiegs der Cyberangriffe auf Unternehmen in dieser Region sehen wir uns gezwungen, unsere Sicherheitsmaßnahmen zu erhöhen. Eine dieser Maßnahmen ist es den Tools Server einzuschränken.

Um weiter auf die Tools Zugriff zu haben, melden Sie sich bitte noch heute einmalig unter folgendem Link an:

<https://tools.maskierteSeite.rp-online.de>

Sollte keine Anmeldung erfolgen, wird Ihr Zugang aus Sicherheitsgründen gesperrt.

Herzliche Grüße

Ihre

Rheinische Post

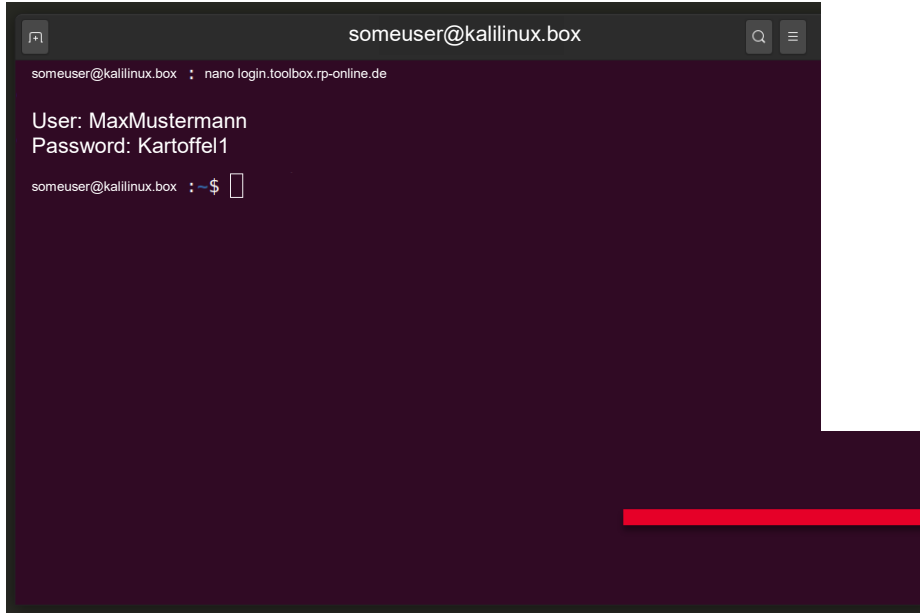
RHEINISCHE POST ~~Neu-dienstreiber Zeitung~~ BERGISCHE MORGENPOST

SOLINGER MORGENPOST RP ONLINE

Rheinische Post Verlagsgesellschaft mbH
Leserservice
Zülpicher Straße 10 · 40196 Düsseldorf

Pentester – Eine Definition

Einbruch in die Rheinische Post:



```
someuser@kalilinux.box : nano login.toolbox.rp-online.de
User: MaxMustermann
Password: Kartoffel1
someuser@kalilinux.box : ~$
```

RHEINISCHE POST

Haben Sie ein Zeitungs-Abonnement?
[Schalten Sie hier Ihren Zugang frei.](#)

ANMELDUNG

E-MAIL *

MaxMustermann

PASSWORT *

Kartoffel1

[PASSWORT VERGESSEN?](#)

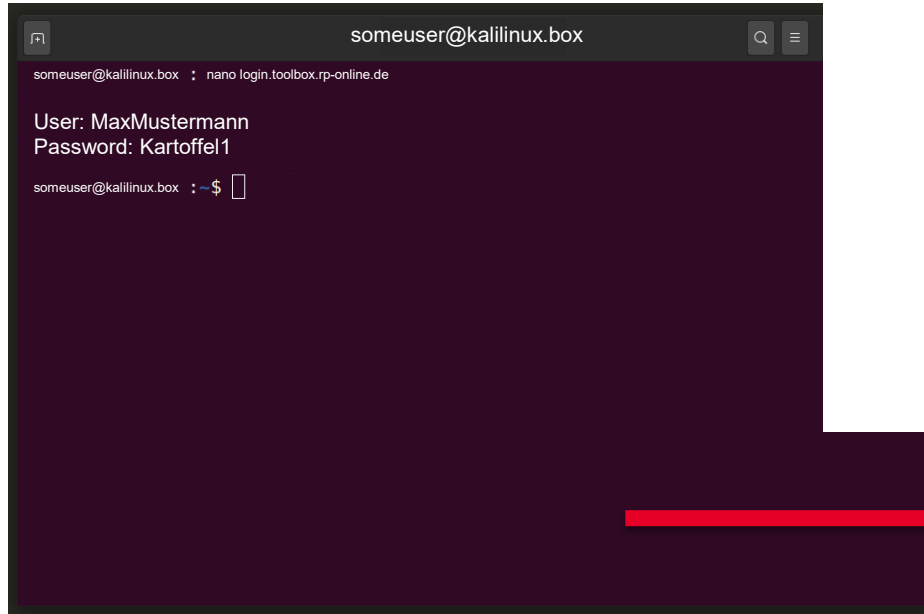
ANMELDEN

Noch nicht registriert? [Hier registrieren](#)

Pentester – Eine Definition

RHEINISCHE POST

Einbruch in die Rheinische Post:

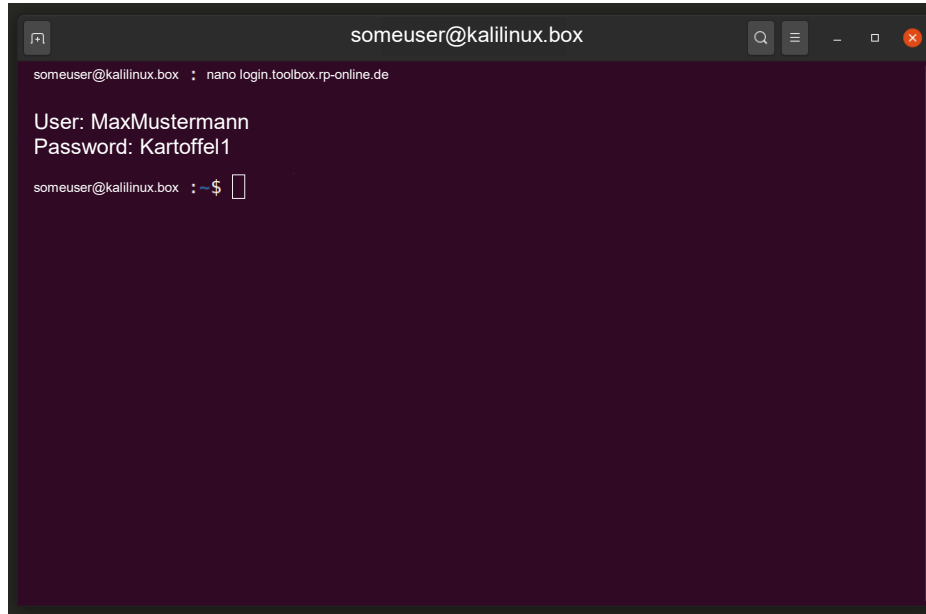


Download des VPN Clients zur Toolbox.

Download

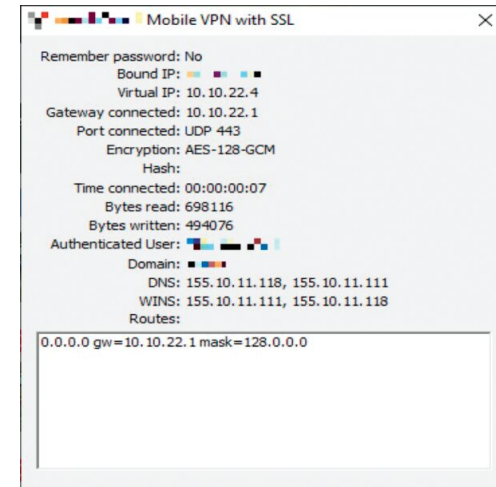
Pentester – Eine Definition

Einbruch in die Rheinische Post:



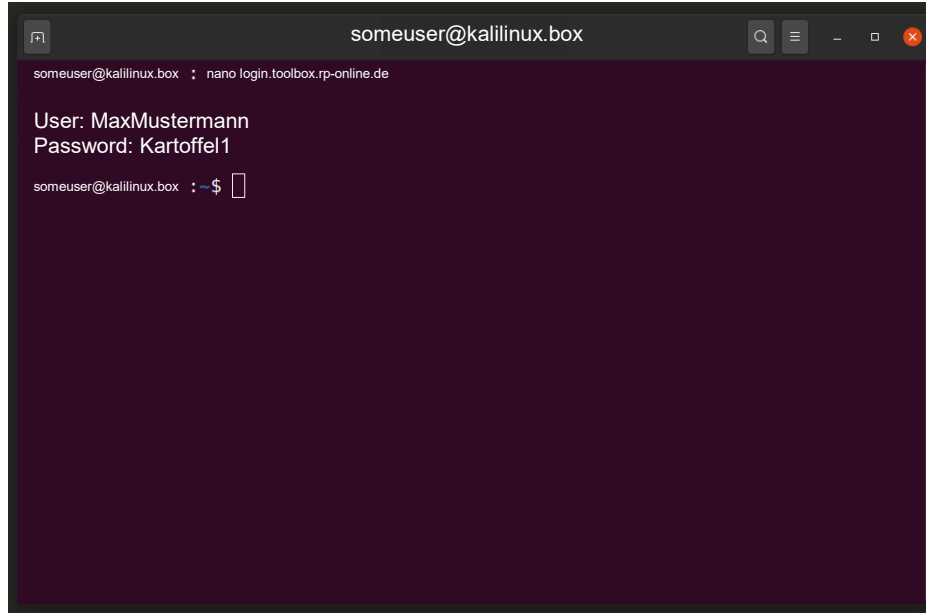
A terminal window titled 'someuser@kalilinux.box' with a dark purple background. The prompt is 'someuser@kalilinux.box :'. The command 'nano login.toolbox.rp-online.de' has been executed. The output shows a login prompt: 'User: MaxMustermann' followed by 'Password: Kartoffel1'. The prompt returns to 'someuser@kalilinux.box :-\$'.

RP ONLINE



Pentester – Eine Definition

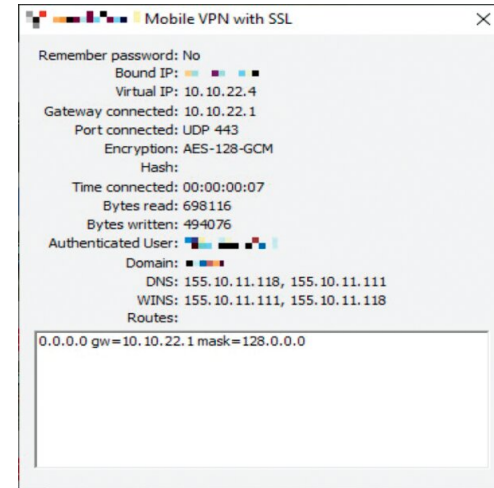
Einbruch in die Rheinische Post:



```
someuser@kalilinux.box : nano login.toolbox.rp-online.de
User: MaxMustermann
Password: Kartoffel1
someuser@kalilinux.box :~$
```

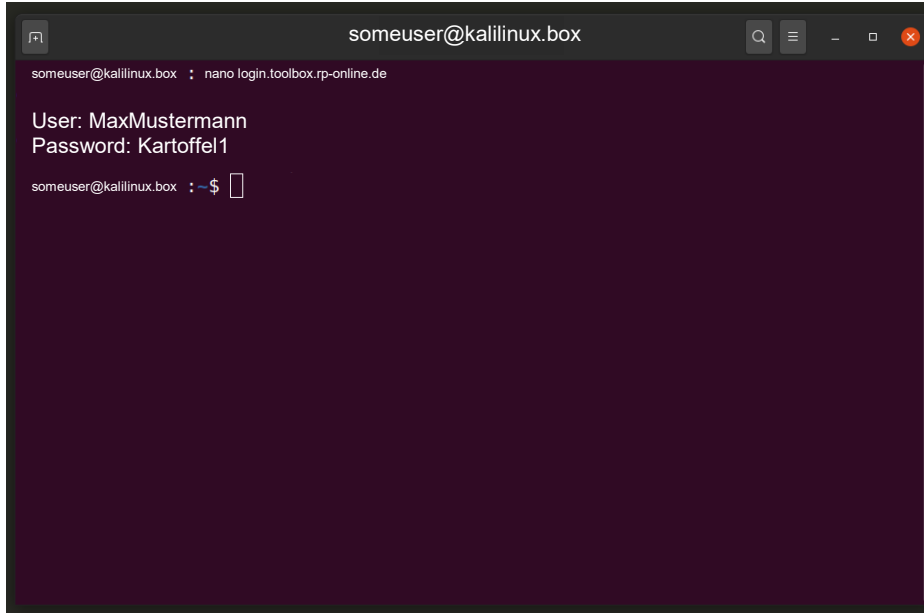
Haben wir die AD
Logon Details?

RP ONLINE



Pentester – Eine Definition

Einbruch in die Rheinische Post:



```
someuser@kalilinux.box : nano login.toolbox.rp-online.de
User: MaxMustermann
Password: Kartoffel1
someuser@kalilinux.box : ~$
```

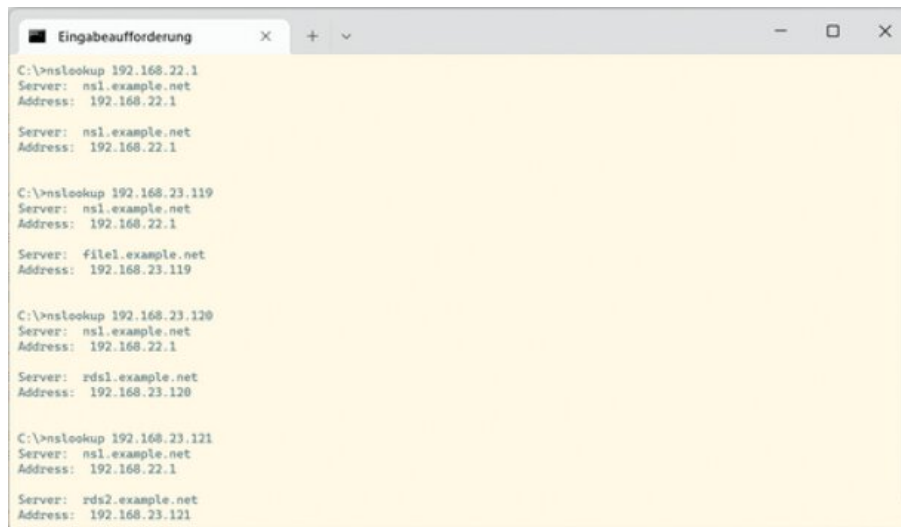
**Haben wir die AD
Logon Details?**

Ping auf das Anmeldeskript
des Domain Controllers.

Netlogon funktioniert.

Pentester – Eine Definition

Einbruch in die Rheinische Post:



```
Eingabeaufforderung
C:\>nslookup 192.168.22.1
Server: ns1.example.net
Address: 192.168.22.1

Server: ns1.example.net
Address: 192.168.22.1

C:\>nslookup 192.168.23.119
Server: ns1.example.net
Address: 192.168.22.1

Server: file1.example.net
Address: 192.168.23.119

C:\>nslookup 192.168.23.120
Server: ns1.example.net
Address: 192.168.22.1

Server: rds1.example.net
Address: 192.168.23.120

C:\>nslookup 192.168.23.121
Server: ns1.example.net
Address: 192.168.22.1

Server: rds2.example.net
Address: 192.168.23.121
```

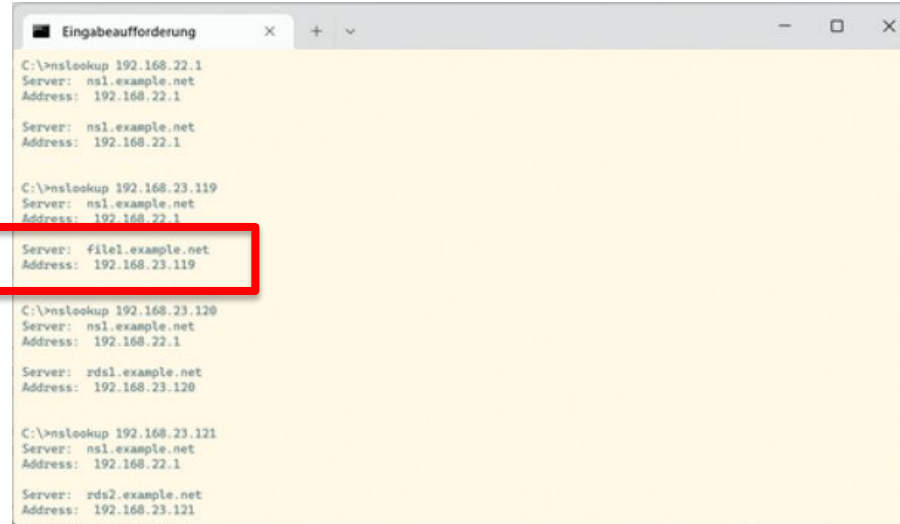
Manuelle Erkundung
der Netzwerklandschaft

Nslookup

Reverse Lookup
Methode um
Servernamen und
Adressen zu finden.

Pentester – Eine Definition

Einbruch in die Rheinische Post:



```
C:\>nslookup 192.168.22.1
Server: ns1.example.net
Address: 192.168.22.1

Server: ns1.example.net
Address: 192.168.22.1

C:\>nslookup 192.168.23.119
Server: ns1.example.net
Address: 192.168.22.1

Server: file1.example.net
Address: 192.168.23.119

C:\>nslookup 192.168.23.120
Server: ns1.example.net
Address: 192.168.22.1

Server: rds1.example.net
Address: 192.168.23.120

C:\>nslookup 192.168.23.121
Server: ns1.example.net
Address: 192.168.22.1

Server: rds2.example.net
Address: 192.168.23.121
```

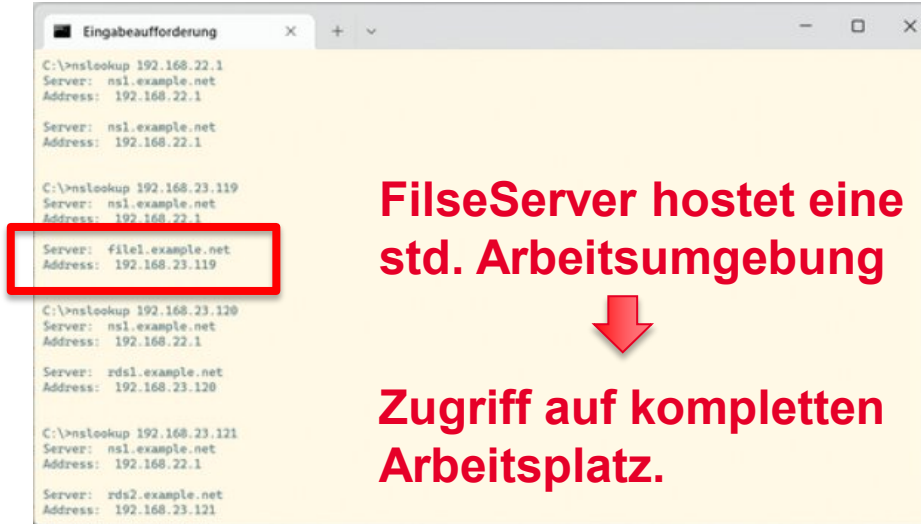
Manuelle Erkundung
der Netzwerklandschaft

Nslookup

Reverse Lookup
Methode um
Servernamen und
Adressen zu finden.

Pentester – Eine Definition

Einbruch in die Rheinische Post:



```
C:\>nslookup 192.168.22.1
Server: ns1.example.net
Address: 192.168.22.1

Server: ns1.example.net
Address: 192.168.22.1

C:\>nslookup 192.168.23.119
Server: ns1.example.net
Address: 192.168.22.1

Server: file1.example.net
Address: 192.168.23.119

C:\>nslookup 192.168.23.120
Server: ns1.example.net
Address: 192.168.22.1

Server: rds1.example.net
Address: 192.168.23.120

C:\>nslookup 192.168.23.121
Server: ns1.example.net
Address: 192.168.22.1

Server: rds2.example.net
Address: 192.168.23.121
```

**FilseServer hostet eine
std. Arbeitsumgebung**

**Zugriff auf kompletten
Arbeitsplatz.**

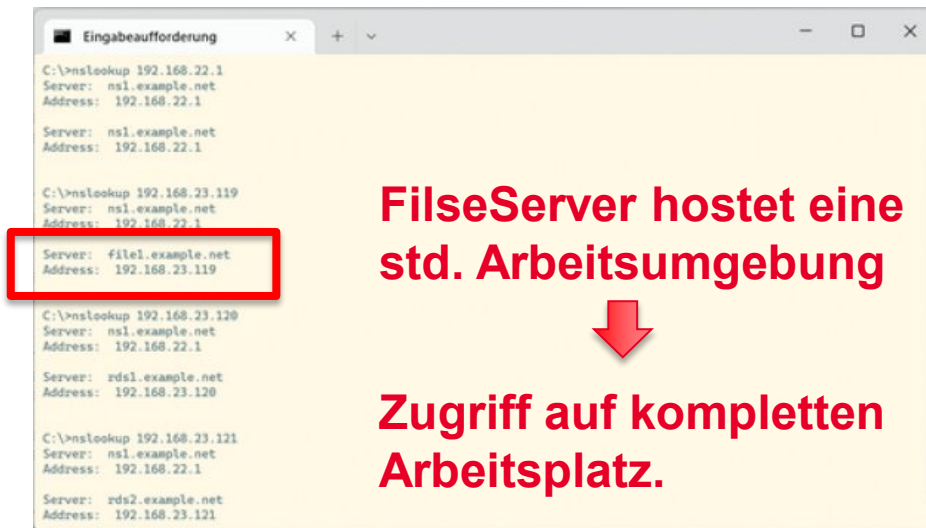
Manuelle Erkundung
der Netzwerklandschaft

Nslookup

Reverse Lookup
Methode um
Servernamen und
Adressen zu finden.

Pentester – Eine Definition

Einbruch in die Rheinische Post:



```
C:\>nslookup 192.168.22.1
Server: ns1.example.net
Address: 192.168.22.1

Server: ns1.example.net
Address: 192.168.22.1

C:\>nslookup 192.168.23.119
Server: ns1.example.net
Address: 192.168.22.1

Server: file1.example.net
Address: 192.168.23.119

C:\>nslookup 192.168.23.120
Server: ns1.example.net
Address: 192.168.22.1

Server: rds1.example.net
Address: 192.168.23.120

C:\>nslookup 192.168.23.121
Server: ns1.example.net
Address: 192.168.22.1

Server: rds2.example.net
Address: 192.168.23.121
```

**FilseServer hostet eine
std. Arbeitsumgebung**

**Zugriff auf kompletten
Arbeitsplatz.**

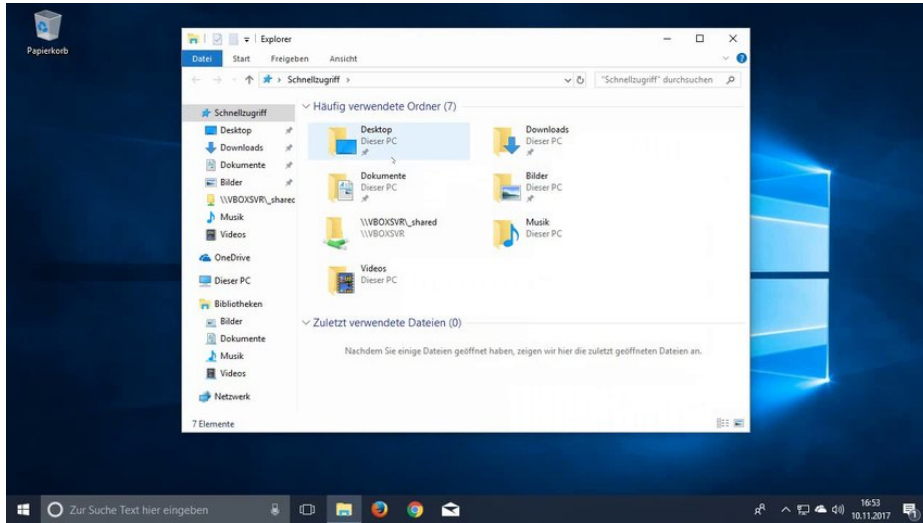
Manuelle Erkundung
der Netzwerklandschaft

Nslookup

Reverse Lookup
Methode um
Servernamen und
Adressen zu finden.

Pentester – Eine Definition

Einbruch in die Rheinische Post:

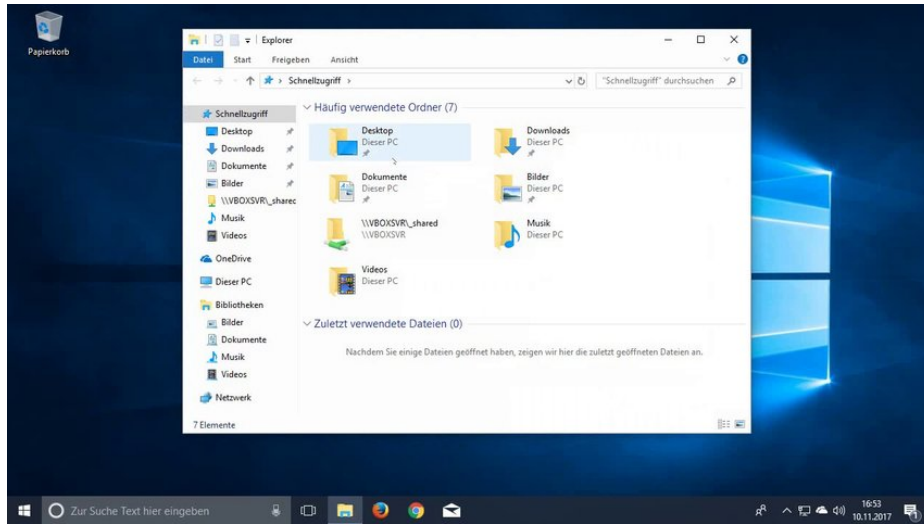


**Pentester zippt alle
Dateien auf dem
Fileserver.**

**Und beweist damit sein
Eindringen.**

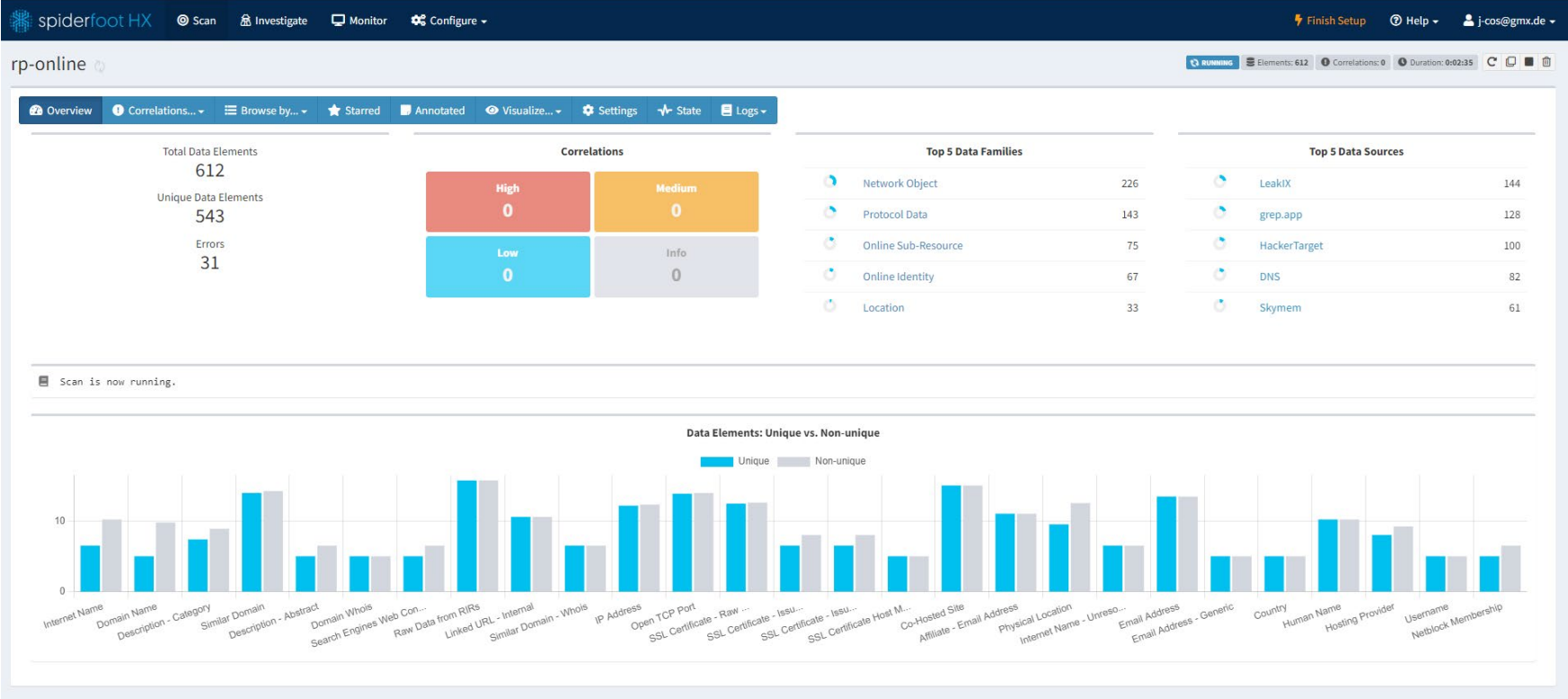
Pentester – Eine Definition

Einbruch in die Rheinische Post:



**Hacker hätten nun
Ransom Software
aufspielen können.**

Backup Slides



Backup Slides

TOTAL RESULTS

4


TOP PORTS

443	3
80	1

TOP ORGANIZATIONS

Intersolute GmbH	3
DigitalOcean, LLC	1

 View Report

 View on Map

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

RP 301 Moved Permanently

91.215.73.131
x.rp-digital.de
[Intersolute GmbH](#)
 Germany, Düsseldorf

SSL Certificate

Issued By:
|- Common Name:
R3

|- Organization:
Let's Encrypt


Issued To:
|- Common Name:
x.rp-digital.de

Supported SSL Versions:
TLSv1.2, TLSv1.3

HTTP/1.1 301 Moved Permanently
Date: Thu, 03 Nov 2022 06:19:22 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Location: <https://rp-online.de/>
Content-Length: 229
Content-Type: text/html; cha...

2022-11-03T06:19:22.937529

RP 301 Moved Permanently

91.215.73.175
175.net73.intersolute.de
x.rp-digital.de
[Intersolute GmbH](#)
 Germany, Düsseldorf

SSL Certificate

Issued By:
|- Common Name:
R3

|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
x.rp-digital.de

Supported SSL Versions:
TLSv1.2, TLSv1.3

HTTP/1.1 301 Moved Permanently
Date: Tue, 01 Nov 2022 00:49:16 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Location: <https://rp-online.de/>
Content-Length: 229
Content-Type: text/html; cha...

2022-11-01T00:49:16.991709