RedTeam Pentesting

Mitbringsel aus dem Alltag
Star Wars in der niedersächsischen Provinz

Alexander Neumann
RedTeam Pentesting GmbH
kontakt@redteam-pentesting.de
https://www.redteam-pentesting.de

17. Januar 2023

Unser Alltag

Das tun, was man normalerweise nicht darf! Fast alles ist erlaubt!

Beispiel: Netzwerk-Penetrationstest

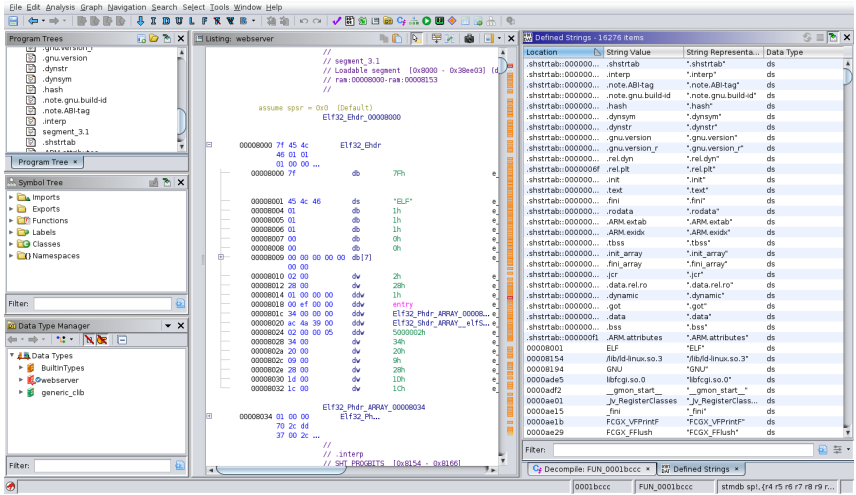
- Telefonanlage von Auerswald (COMpact 5500R) gefunden
- Bietet Passwort-Vergessen-Funktion
- Normaler Weg: Kunde kontaktiert Hersteller, bekommt Passwort

Erste Schritte

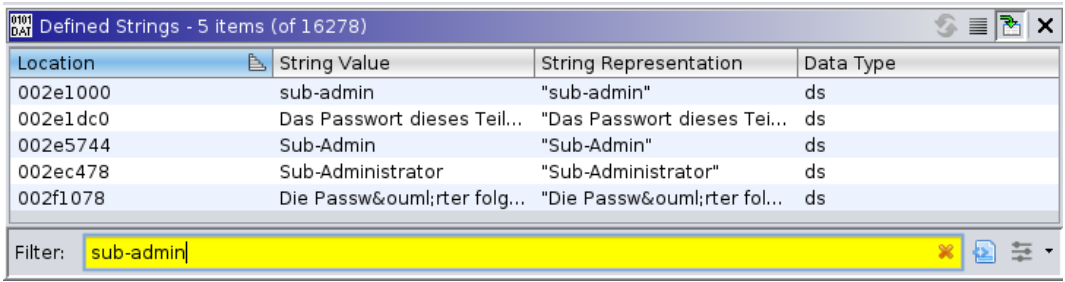
- Firmware heruntergeladen
- Entpackt, basiert auf Linux
- Programm `webserver` gefunden
- $\Rightarrow$ Ghidra

RedTeam Pentesting

Ghidra



Ghidra - Strings



RedTeam Pentesting

Ghidra - Vergleich Admin-Benutzer

RedTeam Pentesting

Ghidra - Vergleich „Schandelah“?

Decompile: web_getAccessLevel - (webserver)

```
504     puVar4 = input_password;
505 LAB_00015930:
506     if ((uVar9 & (uint)local_5f8) == 0) goto LAB_0001593c;
507 LAB_00015340:
508     iVar10 = strcmp((char *)username,"Schandelah");
509     if (iVar10 == 0) {
510       gen_password(0,&generated_password);
511       if (input_password == (undefined4 *)0x0) {
512         iVar10 = FUN_00121668(*param_1,param_1 + 0x10);
513         if (iVar10 != 0) goto LAB_00015ea8;
514       }
515       else {
516         iVar10 = strcmp((char *)input_password,(char *)&generated_password);
517         if (iVar10 == 0) {
    LAB_00015ea8:
```

OSINT #1


Schandelah – Wikipedia
de.wikipedia.org/wiki/Schandelah
Nicht angemeldet Diskussionsseite Beiträge Benutzerkonto erstellen Anmelden
Artikel Diskussion Lesen Bearbeiten Quelltext bearbeiten Versionsgeschichte
Wikipedia durchsuchen
Koordinaten: 52° 15′ 56″ N, 10° 41′ 15″ O
WIKIPEDIA
Die freie Enzyklopädie
Hauptseite
Themenportale
Zufälliger Artikel
Mitmachen
Artikel verbessern
Neuen Artikel anlegen
Autorenportal
Hilfe
Letzte Änderungen
Schandelah
Schandelah ist ein Dorf in Niedersachsen, 15 km östlich von Braunschweig gelegen. Schandelah gehört zur Gemeinde Cremlingen im Landkreis Wolfenbüttel und hat über 2000 Einwohner, einen Bahnhof, einen Kindergarten, eine Grundschule und einen Sportverein.
Inhaltsverzeichnis [Verbergen]
1 Geographie
1.1 Geopunkt Jurameer Schandelah
2 Geschichte
3 Politik
3.1 Ortsrat
Schandelah
Gemeinde Cremlingen
Höhe: 101 m
Einwohner: 2277 (31. Dez. 2017)[1]
Eingemeindung: 1. März 1974

OSINT #1

Wirtschaft und Infrastruktur [Bearbeiten | Quelltext bearbeiten]

Unternehmen [Bearbeiten | Quelltext bearbeiten]

Die Firma Auerswald GmbH & Co. KG, ein Hersteller von Telekommunikationsanlagen, unterhält am Ort eine Produktionsstätte.

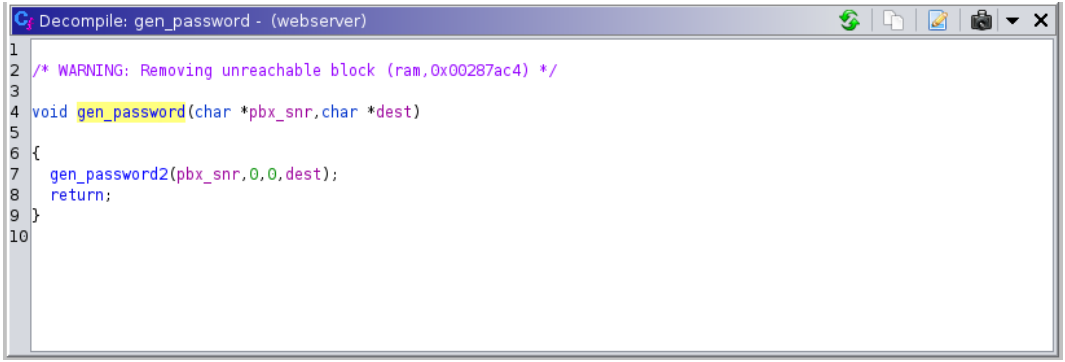
RedTeam Pentesting

Ghidra - Benutzer „Schandelah“

Decompile: web_getAccessLevel - (webserver)

```
504     puVar4 = input_password;
505 LAB_00015930:
506     if ((uVar9 & (uint)local_5f8) == 0) goto LAB_0001593c;
507 LAB_00015340:
508     iVar10 = strcmp((char *)username,"Schandelah");
509     if (iVar10 == 0) {
510       gen_password(0,&generated_password);
511       if (input_password == (undefined4 *)0x0) {
512         iVar10 = FUN_00121668(*param_1,param_1 + 0x10);
513         if (iVar10 != 0) goto LAB_00015ea8;
514       }
515       else {
516         iVar10 = strcmp((char *)input_password,(char *)&generated_password);
517         if (iVar10 == 0) {
    LAB_00015ea8:
```

Ghidra - Passwort



RedTeam Pentesting

Ghidra - Passwort #2

Decompile: gen_password2 - (webserver)

```
1
2  void gen_password2(char *pbx_snr,int include_lang,uint lang_index,char *dest)
3
4  {
```

```
58    local_84 = 0;
59    local_80 = 0;
60    lang = 0;
61    if (pbx_snr == (char *)0x0) {
62      pbx_snr = (char *)&local_84;
63      auer_getPbxSerialNumber(pbx_snr,0x21);
64    }
```

```
74    date_string = current_date_as_string(&local_3c,0x10);
75    __snprintf_chk(&local_c4,0x40,1,0x40,"%s%s%s%s",pbx_snr,"r2d2",date_string,&lang);
76    func_3518(&local_c4,&local_60);
77    auer_strncpy(dest,&local_60,8);
```

RedTeam Pentesting

Ghidra - Mysteriöse Funktion

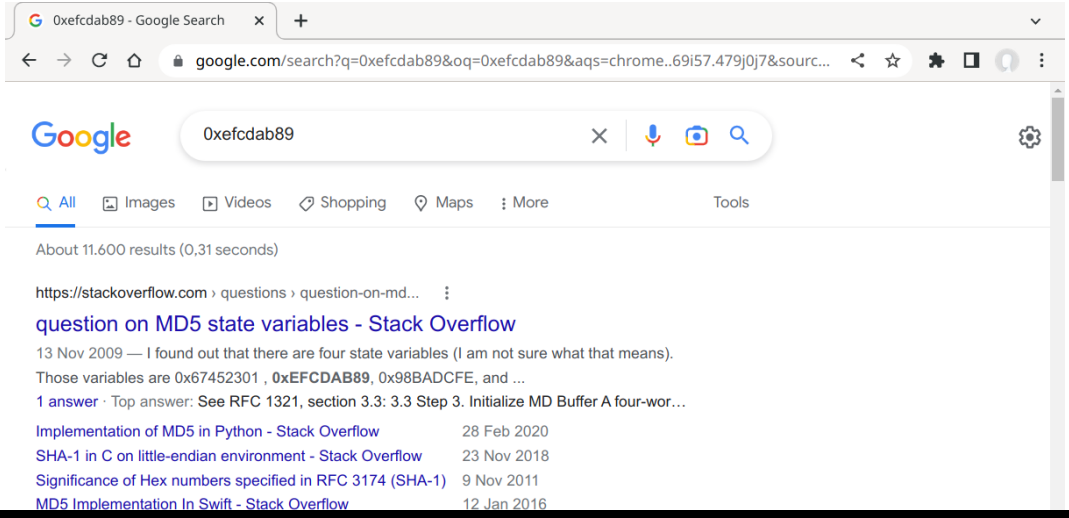
Decompile: func_3518 - (webserver)

```
1
2  void func_3518(char *data_src,char *data_dest)
3
4  {
5    size_t data_src_len;
6    undefined4 local_94;
7    undefined4 local_90;
8    undefined4 local_8c;
```

```
32   local_2c = __stack_chk_guard;
33   local_90 = 0xefcdab89;
34   local_94 = 0x67452301;
35   local_8c = 0x98badcfe;
36   local_88 = 0x10325476;
37   data_src_len = strlen(data_src);
38   md5_update(&local_94,data_src,data_src_len);
39   md5_finalize(&local_3c,&local_94);
40   *data_dest = "0123456789abcdef"[local_3c >> 4];
41   data_dest[1] = "0123456789abcdef"[local_3c & 0xf];
42   data_dest[2] = "0123456789abcdef"[local_3b >> 4];
43   data_dest[3] = "0123456789abcdef"[local_3b & 0xf];
```

RedTeam Pentesting

OSINT #2



RedTeam Pentesting

Ghidra - Passwort #2

Decompile: gen_password2 - (webserver)

```
60  lang = 0;
61  if (pbx_snr == (char *)0x0) {
62    pbx_snr = (char *)&local_84;
63    auer_getPbxSerialNumber(pbx_snr,0x21);
64  }
65  if (include_lang != 0) {
66    if (lang_index < 0x12) {
67      __strcpy_chk(&lang,(&language_table)[lang_index],8);
68    }
69    else {
70      lang = 0x2e6l2e6e;
71      local_28 = local_28 & 0xffffff00;
72    }
73  }
74  date_string = current_date_as_string(&local_3c,0x10);
75  __snprintf_chk(&local_c4,0x40,1,0x40,"%s%s%s%s",pbx_snr,"r2d2",date_string,&lang);
76  md5_as_hexstring(&local_c4,&local_60);
77  auer_strncpy(dest,&local_60,8);
78  if (local_24 == __stack_chk_guard) {
79    return;
80  }
81                    /* WARNING: Subroutine does not return */
```

Passwort für Benutzer `Schandelah` ausrechnen:

1. MD5(Seriennummer + `r2d2` + Datum)
2. Davon die ersten 7 Zeichen

Problem: Wie bekommt man Seriennummer und Datum?

Einfach das Gerät fragen:

```
$ curl --include https://192.168.1.2/about_state
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8;
[...]

{
  "pbx": "COMpact 5500R",
  "pbxType": 35,
  "pbxId": 0,
  "version": "Version 7.8A - Build 002  ",
  "serial": "1234123412",
  "date": "30.08.2021",
  [...]
}
```

RedTeam Pentesting

Shodan Maps Images Monitor Developer More..

SHODAN Explore Downloads Pricing http.title:"Auerswald" product:"lighttpd" Account

Shodan Report

`http.title:"Auerswald" product:"lighttpd"`

Total: 1,667

// GENERAL

Countries

Germany	1,615
Austria	24
Luxembourg	9
Netherlands	7
Belgium	5

- ★ Schwachstelle durch Auerswald in vier Wochen behoben
- ★ Im Gegensatz zu anderen großen Herstellern

RedTeam Pentesting

INTERESSIERT?
WERDE EINE*R VON UNS!

https://jobs.redteam-pentesting.de

RedTeam Pentesting GmbH
Alter Posthof 1
52062 Aachen
Deutschland