Hacker Halted USA EC-Council

TECHNOLOGY & B THE ZOMBIE APOCAL YPSE

How to create permanent Domain Administrator privilege Balazs Bucsay

ATLANTA, GEORGIA www.hackerhalted.com

Bio / Balazs Bucsay

- Hungarian Hacker
- 14 years of experience in IT-Security
- Strictly technical certificates: OSCE, OSCP, GIAC GPEN
- Currently working for world's second largest mobile company (Vodafone)

Bio / Balazs Bucsay

- Started with ring0 debuggers and disassemblers in 2000 (13 years old)
- Major project in 2009: GI John a distributed password cracker (22 years old)
- 27 years old right now
- Webpage: <u>http://rycon.hu</u>
- Twitter: @xoreipeip
- Linkedin: <u>http://hu.linkedin.com/pub/balazs-bucsay/</u> <u>30/911/379</u>



mimikatz

- Made by Benjamin Delpy (gentilkiwi) Big up!
- First version was introduced in 2007 (v0.1)
- Right now it is at 2.0 alpha (Windows only)
- http://blog.gentilkiwi.com/mimikatz
- Exploiting conceptional bugs/features, not vulnerabilities

Hacker Halted

- Lots of features (not a full list):
 - Pass the hash
 - Exporting protected unexportable private keys
 - Credential dumps (even cleartext)
 - and of course Golden Ticket

Me and mimikatz

- Love at first sight
- Daily usage in penetration testing
- Hacker's best friend!
- First English documentation about the Golden Ticket
- First presentation in Hungarian

Golden Ticket

- Post Exploitation Technique
- Backdoor for unlimited time (20 years default)
- Offensive side: good fun, easy to use backdoor
- Defensive side: hard problem to solve
- Well known feature of Kerberos, not a bug
- Cannot be fixed

Cerberus

© Allison Smith, Amosiak Interactive week



Kerberos





Application server (e.g. Fileserver)

Kerberos

- Developed by MIT (v5 1993)
- Main goal to ensure secure communication and authentication over an insecure channel
- Single Sign On
- Mutual authentication with tickets
- Tickets are encrypted
- Encryption keys are stored in the AD
- Supported authentication protocol since Windows 2000

Ticket Granting Ticket

- Similar to a passport
- Issued by the Authentication Service (Government)
- User's password is needed to create the ticket
- Default session is valid for 10 hours
- Circumvents the need for password

PASSPORT



United States of America



Service Ticket

- Similar to a visa (issued by the Embassy)
- Ticket Granting Service issues the Service Ticket
- Service Ticket contains the information for authentication
- Sending Service Ticket to the Service results in session

	BH3a vis	а POCCUЙСКАЯ ФЕДЕРАЦИЯ RUSSIAN FEDERATION ДВУ	0 2844728 кратная от 11
	3 19.12.06 1 8 CWA	5 29.12.06/27.01.07 12	30 1 BAW29606
Poles	4 First nam 5 12345678	e Last name 6 7 39 23.06.1956 МУЖ	19 NETPER, WITHTONN
4111114	18 ТУРИЗМ, (13 000 Альянс	004 Трэвел с-петербург 3656-406	7-291206
RUSS	IA 9		

<<<<<<<<<>>202205443<<<8USA2306566M<<<<<<<0WAS2960674

Hacker Halted



Ticket Granting Service Request

232 13.4393240 192.168.254.100	192.168.254.1	KRB5	1603 TGS-REQ
233 13.4395400 192.168.254.1	192.168.254.100	TCP	60 88→49448 [ACK] Seq=1 Ack=1550 Win=65536 Len=0
234 13.4404180 192.168.254.1	192.168.254.100	TCP	1514 [TCP segment of a reassembled PDU]
235 13.4404190 192.168.254.1	192.168.254.100	KRB5	117 TGS-REP
236 13.4404510 192.168.254.100	192.168.254.1	TCP	54 49448→88 [ACK] Seq=1550 Ack=1524 Win=65536 Le
237 13.4405850 192.168.254.100	192.168.254.1	TCP	54 49448→88 [FIN, ACK] Seq=1550 Ack=1524 Win=655
238 13.4408930 192.168.254.100	192.168.254.101	SMB2	1751 Session Setup Request
220 12 4/10060 102 160 25/ 1	100 160 054 100	TCD	60 99 40449 FACKI 500-1524 Ack-1551 Win-65526 Lo

⊕ Frame 232: 1603 bytes on wire (12824 bits), 1603 bytes captured (12824 bits) on interface 0 Ethernet II, Src: Vmware_0a:c6:a0 (00:0c:29:0a:c6:a0), Dst: Vmware_91:1c:b9 (00:0c:29:91:1c:b9) H Internet Protocol Version 4, Src: 192.168.254.100 (192.168.254.100), Dst: 192.168.254.1 (192.168.254.1) Transmission Control Protocol, Src Port: 49448 (49448), Dst Port: 88 (88), Seq: 1, Ack: 1, Len: 1549
Kerberos

Record Mark: 1545 bytes

0... = Reserved: Not set .000 0000 0000 0000 0110 0000 1001 = Record Length: 1545

tqs-req

pvno: 5

msg-type: krb-tgs-reg (12)

- padata: 2 items

0040	06	01	a1	03	02	01	05	a2	03	02	01	0c	a3	82	04	e4		
0050	30	82	04	e0	30	82	04	c5	a1	03	02	01	01	a2	82	04	00	
0060	bc	04	82	04	b8	6e	82	04	b4	30	82	04	b0	a0	03	02	n	.0
0070	01	05	a1	03	02	01	0e	a2	07	03	05	00	00	00	00	00		
0080	a3	82	04	03	61	82	03	ff	30	82	03	fb	a0	03	02	01	a	0
0090	05	a1	0c	1b	0a	47	4f	4c	44	45	4e	2e	44	4f	4d	a2	GOL	DEN.DOM.
00a0	1f	30	1d	a0	03	02	01	02	a1	16	30	14	1b	06	6b	72	.0	0kr
00b0	62	74	67	74	1b	0a	47	4f	4c	44	45	4e	2e	44	4f	4d	btgtGO	LDEN.DOM
00c0	a3	82	03	с3	30	82	03	bf	a0	03	02	01	12	a1	03	02	0	
00d0	01	02	a2	82	03	b1	04	82	03	ad	c9	b3	09	c0	b8	8d		
~~ ~	C		-	-1	10	1.7	-	1 -	1.0		1. 72	C 1						







Keys

- NTLM/AES hashes of the entities from Active Directory
- Ticket Granting Ticket is encrypted with the *krbtgt* user's hash
- Service Tickets are encrypted with the server's and the session key

krbtgt user

User name ull Name Comment User's comment Country/region code Account active Account expires

Password last set Password expires assword changeable assword required lser may change password

Workstations allowed ogon script. User profile Home directory ast logon

ogon hours allowed

Local Group Memberships *Denied RODC Password Global Group memberships *Domain Users The command completed successfully.

krbtgt

Key Distribution Center Service Account

000 (System Default) No Never

9/1/2014 10:08:25 PM 10/13/2014 10:08:25 PM 9/2/2014 10:08:25 PM Yes Yes

A11

Never

A11



krbtgt user

- Default, must have Active Directory account
- Previous Domain Controller compromise
- krbtgt user NTLM/AES hash dump
- Arbitrary Ticket Granting Ticket can be created with the *krbtgt* user's hash

What does it mean for us?



UNLIMITED ACCESS

FOR UNLIMITED TIME TO ANY COMPUTER





Mitigation

- No real way to do this
- It is a feature and not a bug
- Change password of *krbtgt* (twice)
- Long-time tickets could be a problem
- There can be outage in some services (Lync, Sharepoint)

Thank you

Q&A

EC-Council

Hacker Halted USA