TAKING A LEAK ON THE NETWORK: LITTLE THINGS THAT GIVE AN ATTACKERS IDENTITY AWAY

Adrian Crenshaw





About Adrian

- I run Irongeek.com
- I have an interest in InfoSec education
- I don't know everything I'm just a geek with time on my hands
- (ir)Regular on the ISDPodcast <u>http://www.isd-podcast.com/</u>



What information is leaking out about your (or someone else's) box while connected to a network?

- Outright identification
- Shrinking of the "anonymity set"
 - An anonymity set is the total number of possible candidates for the identity of an entity. Reducing the anonymity set means that you can narrow down the suspects.



Why this talk?

- Because Rob told me to come up with something
- I'm in a privacy class, and intended to use it as a project (but ended up working with I2P instead)
- Call to research on the topic
- "The quieter you become the more you can hear." Baba Ram Dass (and since I'm not a shiftless hippy that dosn't bathe, I just think of it as the BackTrack Linux slogan)



Who might this talk interest

- Pentesters
- "Pro Bono Pentesters"
- Attackers
- IDS and Log Watchers
- Incident Response, and people who want to test Incident Response



Clean Room Box

- I advocate making a "Clean Room Box" if you can afford it.
- Separate boot partition is the 2nd best option
- "Clean Room VM" May be an option
- Most of the mitigations I mention can be taken in the Clean Room
- For legitimate pentesters, this also helps keep customer data separate



Just a few leaks, of many

- MAC Address left in logs
- Browser tabs that automatically open
- Network scans that automatically use the credentials of the logged in user
- WiFi SSID Probes
- Host name/NetBIOs name broadcasts
- Last DHCP lease renew
- Other apps? (Skype, IM, IRC, etc)



MAC Address left in logs

eth0 Link encap:Ethernet HWaddr 00:0c:29:cb:37:89
inet
addr:192.168.127.129 Bcast:192.168.127.255 Mask:255.255.255.0
<pre>inet6 addr: fe80::20c:29ff:fecb:3789/64 Scope:Link</pre>
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1102 errors:0 dropped:0 overruns:0 frame:0
TX packets:1396 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:108974 (108.9 KB) TX bytes:92538 (92.5 KB)
Interrupt:19 Base address:0x2000
Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . :
Description Broadcom 802.11n Network Adapter
Physical Address
DHCP Enabled No
Autoconfiguration Enabled : Yes
Link-local IPv6 Address :
fe80::blce:9626:799a:5f41%14(Preferred)
IPv4 Address
Subnet Mask
Default Gateway
DHCPv6 IAID
DHCPv6 Client DUID
8D-BC-BE
DNS Servers

- In theory MAC addresses are unique (but not really)
- Can be spoofed, but good luck proving that it was Bob Swim
- First 6 HEX digits are the vendor's OUI (Organizationally Unique Identifier) <u>http://standards.ieee.org/regauth/oui/oui.txt</u>

I wonder if any vendors store this information?

Mitigation

- Change it if possible: <u>http://www.irongeek.com/i.php?page=security/changemac</u>
- Linux: ifconfig eth0 down hw ether 00:00:00:00:00:01 ifconfig eth0 up
- Windows:

Regedit or some tools (but some card drivers just say no or require the same OUI)

MadMacs http://www.irongeek.com/i.php?page=security/madmacs-mac-spoofer

Smac http://www.klcconsulting.net/smac/



Related

IPv6 Stateless Address Autoconfiguration

https://www.defcon.org/images/defcon-15/dc15-presentations/Lindqvist/Whitepaper/dc-15-lindqvist-WP.pdf

This example may be local only, and non-routable, sort of like 169.254.0.0/16 in IPv4

eth0 Link encap:Ethernet HWaddr 00:0c:29:cb:37:89 inet addr:192.168.127.129 Bcast:192.168.127.255 Mask:255.255.255.0 inet6 addr: fe80::20c:29ff:fecb:3789/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:1102 errors:0 dropped:0 overruns:0 frame:0 TX packets:1396 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:108974 (108.9 KB) TX bytes:92538 (92.5 KB) Interrupt:19 Base address:0x2000



Browser tabs that automatically open

What does it say about you?



- Just the names of the sites give tons on information
- Plaintext login information
- Imagine using Facebook during a pentest?
- Even if SSL is used, DNS queries give away information about the sites visited
- Headers (browser type, version, plugins)

Thanks to d4ncingd4n for reminding me to add headers



Mitigation

- Dedicated browser for certain activities
- Limit plugins
- Keep changing user agent (or make sure it's very generic)
- Don't have the browser do anything automatically
 - Passwords
 - Forms
 - Tabs



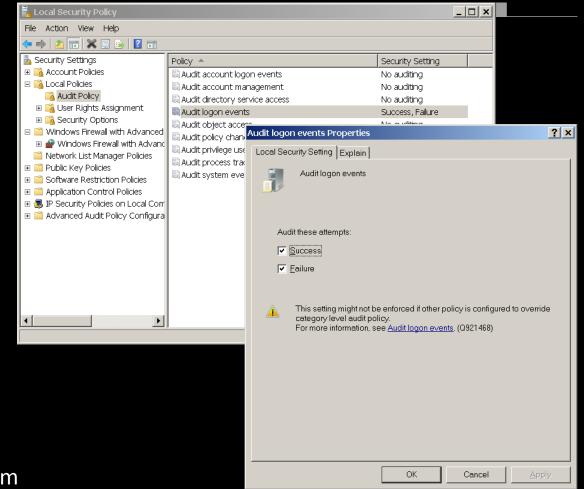
Network scans that automatically use the credentials of the logged in user

Watch out for "Use current credentials"

Y	🛠 SoftPerfect Network Scanner [portable mode]														
]	Eile View Actions Options Bookmarks Help														
]	📄 🗁 🔚 🛅 😤 👫 🔁 🗹 🔏 🚮 📆 🖳 📰 😰 🙆 🏠 Web-site														
IP Range From 0.0.0.0 To 0.0.0 V Start Scanning 🕶															
[IΡ	Address	Host Name	MAC Address	Response Time	Port SNN	4P Log								
	+	👮 192.168.10.82	TOSHIBA	00-00-39-9D-E1-A1	0 ms										
	+	🧕 192.168.10.85	CAN	00-30-84-88-6D-7B	0 ms	21									
		🧕 192.168.10.92	DOM	00-E0-4C-67-EE-AD	10 ms										
	-	🧕 192.168.10.1	EVA	00-50-22-B5-80-65	0 ms										
		MOVIES													
		— 🧰 мРЗ													
		🗝 😯 C\$													
		🕀 ADMIN\$													
		🕀 D\$													
		🖻 English													
		🧕 192.168.10.1	ROM	00-C0-DF-0F-EB-EF	0 ms	21									
		🧕 192.168.10.1	SNCOMP	00-C0-DF-01-B1-C9	10 ms	21									
		🧕 192.168.10.1			0 ms										
		🧕 192.168.10.1		00-0C-6E-A5-64-5A											
	+	🧕 192.168.10.1	1.2.3.4	00-02-44-35-27-3E	0 ms										
R	.ead	ly	Threads	Devices 220	/ 220 Scan										



Auditing matters





Share type matters

Local Security Policy			4					
<u>File Action View H</u> elp								
🗢 🔿 🞽 💼 💥 🖬 😖								
Ga Account Policies Ga Local Policies	Policy A Microsoft network server: Server SPN target name validation level Network access: Allow anonymous SID/Name translation	Security Setting A Not Defined Disabled						
Audit Policy Jeer Rights Assignment Security Options Windows Firewall with Advanced Security Network List Manager Policies	Network access: Do not allow anonymous enumeration of SAM ac Metwork access: Do not allow anonymous enumeration of SAM ac Network access: Do not allow storage of passwords and credenti Network access: Let Everyone permissions apply to anonymous u	Enabled Disabled		ocal Computer Policy\Computer Configuration\Windows Settings\Security Settings\Lo Window Help				
Network List Manager Policies Definition Control Policies Get Application Control Policies Get Application Control Policies Get Policies on Local Computer	Network access: Named Pipes that can be accessed anonymously Network access: Remotely accessible registry paths Network access: Remotely accessible registry paths and sub-paths Network access: Restrict anonymous access to Named Pipes and	· · ·		Policy A Security Setting				
 B and a secarity roles on Exercisingular Advanced Audit Policy Configuration 	 Network access: Shares that can be accessed anonymously Network access: Shares that can be accessed anonymously Network access: Sharing and security model for local accounts Network security: Allow Local System to use computer identity fo Network security: Allow Local System NULL session fallback 	Not Defined Classic - local users authe Not Defined Not Defined	5hutdown)	Microsoft network server: Digitally sign communications (dr Disabled Microsoft network server: Disconnect clients when logon h Enabled Microsoft network server: Disconnect clients when logon h Enabled Metwork access: Allow anonymous SID/Name translation Disabled Wetwork access: Do not allow anonymous enumeration of Enabled	bled bled bled			
	Network Security: Allow PKU2U authentication requests to this co Network security: Configure encryption types allowed for Kerberos Network security: Do not store LAN Manager hash value on next Network security: Force logoff when logon hours expire		ies d Policy Lockout Policy	Image: Second	ibled ibled ibled			
	Network security: LAN Manager authentication level Network security: LDAP client signing requirements Network security: Minimum session security for NTLM SSP based ()	Send NTLMv2 response o Negotiate signing Require 128-bit encryption	icy hts Assignment Options	Network access: Remotely accessible registry paths System	MNAP,COMNOD tem\CurrentCon MCFG,DF5\$ ssic - local users			
			licies striction Policies	Image: Network security: Do not store LAN Manager hash value o Disat Image: Network security: Force logoff when logon hours expire Disat	bled			
		H - Securit H - I Securit H - I Administrative Ter H - I Administrative Ter H - I Administrative Ter H - I Securit H - I Securit		Wetwork security: LDAP client signing requirements Nego Wetwork security: Minimum session security for NTLM SSP No m Network security: Minimum session security for NTLM SSP No m	d LM & NTLM re			
				Image: Second	bled 🗉			
				Image: System cryptography: Use FIPS compliant algorithms for e Disat Image: System objects: Default owner for objects created by me Objects Image: System objects: Require case insensitivity for non-Window Enable Image: System objects: Strengthen default permissions of internal Enable	ect creator bled			
ttp://Irongeek.cor	m		>	exposition objects: Strengthen default permissions of internal Enab	Died 💌			

What shows in the logs depends on share type

Event Properties		? 🗙 🗍	ivent Prop	erties		? 🛽
Event			Event			
	ecurity		D <u>a</u> te: Timor	10/15/2010 <u>Sou</u>		
Ti <u>m</u> e: 3:25:05 PM Category: Ad Typ <u>e</u> : Success A Event <u>I</u> D: 68	-		Ti <u>m</u> e: Typ <u>e</u> :	3:21:21 PM Cat Failure Aud Eve		Int Logon
User: NT AUTHORITY\SYSTEM			User:	NT AUTHORITY	-	
Computer: IG-TEST20GB			_	IG-TEST20GB	10101EM	
	🖁 Event Properties - Event 462	25. Microsoft Wi			×	
Description: Logon attempt by: MICROSOFT_AU Logon account: Guest Source Workstation: PC Error Code: 0x0 For more information, see Help and S http://go.microsoft.com/fwlink/event	General Details Subject: Security ID: Account Name: Account Domain: Logon ID: Log Na <u>m</u> e: Security	PC∖adrian adrian PC 0x25713	1			TICATION_PACKAGE_V1_0
Da <u>t</u> a:			sk Category:	-	57 [
	Level: Information User: N/A OpCode: Info More Information: Event Log	Co	ywords: ompute <u>r</u> :	Audit Failure PC		×
ОК						Cancel Apply
//Irongeek.com	Сору				<u>C</u> lose	Set

Mitigation

- Use a different account
- Use a non-specific user name
- If the tool has an option for "use other credentials", try using it, keeping in mind "Trust but verify"
- "Shift+Right-Click ->Run As" works wonders



Related

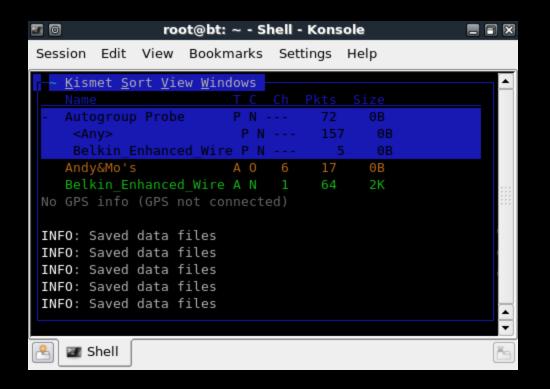
- When auditing logins causes security problems
- A successful login right after a failed one, with a user name that matched your password complexity rules? Hum, let me think here. ⁽³⁾
- PEBKAC Attack

http://www.irongeek.com/i.php?page=security/pe bkac-attack-passwords-in-logs



WiFi SSID Probes

SSID probes, not like the alien kind





- Depends on OS and configuration
- Sometimes probes are sent from a wireless client saying "hey, are you out there?" to a previously used SSID (Wireless Network Name)
- Network names may be significant (now I know what comics you like, where you go to school, and where you get coffee)
- Geolocation:
 - Google Street View?
 - Wigle it, just a little bit! <u>https://wigle.net/gps/gps/main/query/</u>



Mitigation

 Clean out
 Disable a
 Another r to useless

Use a sup

L

AN-Of-The-Dead Wireless Network Properties									
Connection Security									
Name:	LAN-Of-The-Dead								
SSID:	LAN-Of-The-Dead								
Network type:	Access point								
Network availability:	All users								
Connect auto <u>m</u> ati	ically when this network is in range								
Connect to a more	e greferred network if available								
Connect even if t	he network is not broadcasting its name (SSID)								
😻 Copy this network	<u>cprofile to a USB flash drive</u>								

OK

Cancel

home rofiles

×

ID is just a bad



Host name/NetBIOs name broadcasts

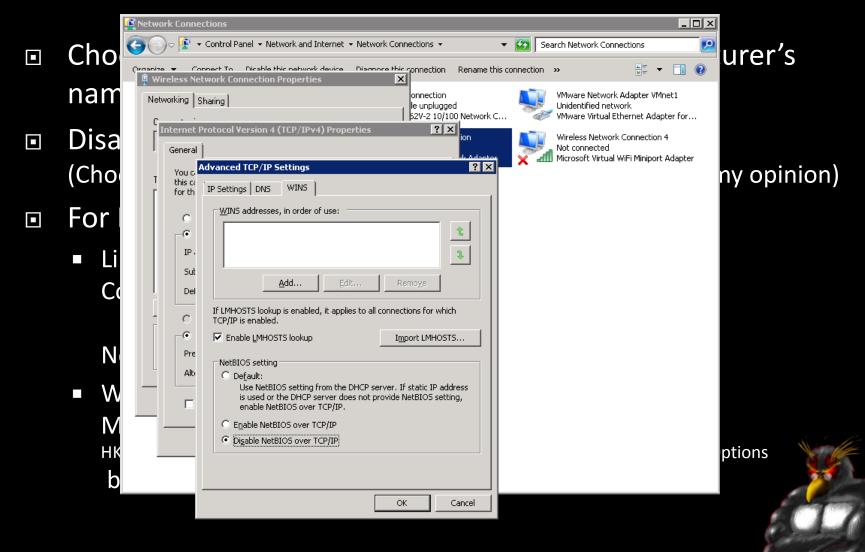
What does your name say about you?

DHCP Clients		
Host Name	IP Address	MAC Address Client Lease Time
ig-test20gb *	192.168.1.141	System Properties
*	192.168.1.109 192.168.1.139	Computer Name Hardware Advanced System Protection Remote
BobbysWorld	192.168.1.108	Computer Walle Hardware Advanced System Protection Remote
WET610N	192.168.1.130	Windows uses the following information to identify your computer
glenn-lappy	192.168.1.110	on the network.
рс РС	192.168.1.134	
cthulhu	192.168.1.103	Computer description:
*	192.168.1.102	En avenuelle UKählen Consultation Ukteuria
WebCamRotate	192.168.1.253	For example: "Kitchen Computer" or "Mary's Computer".
Webcallikolale	192,100,1,233	
		Full computer name: skynet
		Workgroup: WORKGROUP To use a wizard to join a domain or workgroup, click Network ID Network ID. Network ID
		To rename this computer or change its domain or <u>Change</u> workgroup, click Change.
tp://Irongeek.c	om	OK Cancel Apply

- DHCP can have a host name option
- NetBIOs naming traffic says "hey, I'm here"
- Direct probe may also list name

Microsoft - Wireshark	
Eile Edit Yiew Go Capture Analyze Statistics Telephony Tools Help	
	२. 🔍 🔟 🔐 🗹 🕵 % 😫
Filter: 📃 🔻 Expression Clear /	Apply
No. Time Source Destination Pro	tocol 🔺 Info
8810 306.982338 192.168.1.13 192.168.1.255 BR	OWSERBrowser Election Req
	OWSERRequest Announcement
	OWSERRequest Announcement
	OWSERDomain/Workgroup Ann
	OWSERRequest Announcement
	OWSERRequest Announcement
	OWSERLocal Master Announc
	Þ
🗷 Frame 8789: 219 bytes on wire (1752 bits), 219 bytes capt	ured (1752 bits)
⊡ Internet Protocol, Src: 192.168.1.13 (192.168.1.13), Dst:	
□ User Datagram Protocol, Src Port: netbios-dgm (138), Dst	Port: netbios-dgm (138)
Source port: netbios-dgm (138)	
Destination port: netbios-dgm (138)	
Length: 185	
⊞ Checksum: 0×d99a [validation disabled]	
🗉 NetBIOS Datagram Service	
🗉 SMB (Server Message Block Protocol)	
■ SMB MailSlot Protocol	
B Microsoft Windows Browser Protocol	
Command: Request Announcement (0x02)	
Unused flags: 0x00	
Response Computer Name: SKYNET	
	► The second se
00b0 00 00 00 09 00 56 00 03 00 01 00 01 00 02 00 1a	V
	MAILSL OT\BROWS
	SKYN ET.
	*
Response Computer Name (browser.res Packets: 12408 Displayed: 12408 Marked: 0 Dropped:	0 Profile: Default

Mitigation



Last DHCP lease renew

What other networks have you been on?

0								et	h0: Ca	pturing	g - V	Niresł	nark										1 🕅
<u>F</u> ile	<u>E</u> dit	<u>V</u> ie	w <u>c</u>	<u>io</u>	<u>C</u> aptu	re <u>A</u>	nalyze	<u>S</u> tat	istics	Telep	hon	<u>y T</u> o	ols <u>I</u>	<u>H</u> elp									
		Ø	e	ک			*	۲	\equiv	٩	0	0	9	0	•				Ð		R		•
F <u>i</u> lter:											•	E <u>x</u> pre	ssion	Cl	ea <u>r</u>	App <u>l</u>	У						
		Sou	rce				Destir	nation			Pro	tocol	Info										
		fe80)::68	377:d	096:b	fe:8	ff02:	c			SSD	P	M-SE	ARCH	* H	TTP/	1.1						10
		fe80)::68	377:d	096:b	fe:8	ff02::	:1:2			DHC	Pv6	Soli	cit									
		fe80)::68	377:d	096:b	fe:8	ff02::	c			SSD	P	M-SE	ARCH	* H	TTP/	1.1						
		fe80)::68	377:d	096:b	fe:8	ff02::	C			SSD	P	M-SE	ARCH	* H	TTP/	1.1						
				b:37			Broad				ARP						127.2				168.12	27.12	2
							Vmware				ARP							0:50:					
					129		206.33		.254		DHC							actio	n II) OX	f4170f	f55	
							ff02:				SSD			ARCH									
				377:d	096:b		ff02:				SSD			ARCH									
		0.0.					255.25				DHC							actio	n II) OX	e51af7	746	
					254		192.10				ICM			(pi	U .								
				127.			192.10				ICM			(pi							F 4 6-		
		192.	168.	127.	254		192.10	58.12	/.129		DHC	P	DHCP	OTTO	er	-	Irans	actio	n II) ()X	e51af7		Ē
•												*******										••	J
▶ Eth	erne	t II,	, Sro	: Vr	nware_	cb:3	7:89 (00:0c	:29:c	b:37:8	9),	Dst:	Vmwa	re_fo	d:c0	:13	(00:5	0:56:	fd:c	0:13	3)		[
▶ Int	erne	t Pro	otoco	ol, S	Src: 1	192.1	68.127	.129	(192.	168.12	7.1	29),[Ost:	206.3	33.12	27.2	54 (2	06.33	.127	7.25	4)		
0000	00 5	50 56	fd	c0 1	3 00	0c 2	9 cb 3	37 89	08 00	45 00		.PV)	.7	.E.								
0010					0 40					. ce 21		.H@											
0020	7f f	e 00	44	00 4	3 01	34 2	26 6b (01 01	06 00) f4 17	7		C.4 8										
0030	0f 5	55 00	00	00 0	0 ce	21 7	'f 81 (00 00	00 00	00 00		.U											L.
O Inte	ernet	Proto	col (ip), 2	0 byte	es o	Pac	kets:	135 Di	splayed	d: 1:	35 Ma	, rked:	0			Pro	ofile: D	Defau	ult			

- Sometimes DHCP info gets sent when you move from network to network
- If the last DHCP server handed out a non routable (like 192.168.*.*) it may not be a big issue
- Find who owns the IP
 <u>http://serversniff.net/asreport.php</u>
- IP+Network Owner+Host Name+Google = identity?



Mitigation

💣 Registry Editor					×
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>H</u> elp					
🗄 🛄 swwd	^	Name	Туре	Data	^
🗈 🛄 sym_hi		💩 (Default)	REG_SZ	(value not set)	
⊞ <mark></mark> sym_u3		AddressType	REG_DWORD	0×00000000 (0)	
		all DefaultGateway	REG_MULTI_SZ		
⊞ 🛄 symc8xx ⊕- 🛅 sysaudio		💩 DefaultGateway	REG_MULTI_SZ		
		🔀 DhcpClassIdBin	REG_BINARY	(zero-length binary v	
			REG_SZ	192.168.1.145	=
🖃 📄 Topip		DhcpServer	REG_SZ	192.168.1.1	
Enum) DhcpSubnetMask	REG_SZ	255.255.255.0	
🛄 Linkage		ஸ்Domain	REG_SZ		
🖨 🧰 Parameters		EnableDeadGWD	REG_DWORD	0×00000001 (1)	
🗈 🦲 Adapters			REG_DWORD	0×00000001 (1)	
DNSRegisteredAdapters			REG_MULTI_SZ	0.0.0.0	
		MIPAutoconfigurati	REG_SZ	0.0.0.0	
		Diperturbation International I	—	255.255.0.0	
A023AF6D-ED25-4E		IPAutoconfigurati	—	0×00000000 (0)	
CC83E30D-13FC-4F		Billease	REG_DWORD	0×00015180 (86400)	
D7AC76C3-2E35-4F			REG_DWORD	0x4830d51b (12111)	
= (EFFEF000 2000 11	~	聞LeaseTerminates	REG_DWORD	0x4832269b (12112	~
< >		<		>	

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{CC83E30D-

ers\l

http://Irongeek.com

Other apps? (Skype, IM, IRC, etc)

- Test your apps (in my case Pidgin)
- What servers does it contact, and what does it send?

М	icroso	ft - W	'iresh	ark																	_ [l ×
Eile	Edit	⊻iew	Go	⊆a	pture	Analy	ze 😫	Statistic	ts Te	lephon <u>y</u>	Tools	Help	5									
	1	0	e í)			×	2	₽	୍	Þ 🔿		Ŧ	⊉		Ð	0.0	2] 🌌	¥	•	•
Filter	r: <mark>!(ip</mark>	.addr=	=192	.168.	1.13 88	(udp.p	oort==	=12668	3)				•	Expression	i Clea	r Ap	ply					
No.		Time			Source				D	estinatio	n			Protoc: 🔺	Info							
_					192.1				-	6.73.				DISTCO								
1	.042	12.2	62.03	19	86.73	.16.	201		1	92.16	8.1.1	.3		DISTCO								
	207				192.1				1	92.16	8.1.1	-		DNS			query					
Z	867	31.8	9824	42 :	192.1	68.1	L.13		1	92.16	8.1.1	-		DNS	Stan	dand	query	A W	w.rev	erbn	ation.	C
4	474	37.9	771	85 🔅	192.1	68.1	L.13		1	92.16	8.1.1	-		DNS							lias.c	:0
5	209	42.3	111	57 🗄	192.1	68.1	L.13		1	92.16	8.1.1	-		DNS	Stan	dand	query	A ir	r⊂.min	tirc	.net	
	718				192.1					92.16				DNS							neswar	
3	003	32.4	027	38 :	192.1	68.1	1.1		1	92.16	8.1.1	.3		DNS	Stan	dand	query	nesp	onse	CNAM	E farm	12
	002				192.1				1	92.16	8.1.1	.3		DNS							E reve	
	322 -				192.1					92.16				DNS							.59.25	
	i208 -				192.1				1	92.16	8.1.1	-		DNS			query					
5	i320 -	42.7	101:		192.1				1	92.16	8.1.1	.3		DNS							E chat	
6	6734 -	49.8	284	79 :	192.1	68.1	L.13		1	92.16	8.1.1	-		DNS			query				org	
3	442	33.8	500	73 🔅	192.1	68.1	L.13		1	92.16	8.1.1	-		DNS	Stan	dand	query	Ar.	openx	.net		
1	.589	19.3	774	44 🔅	192.1	68.1	L.13		1	92.16	8.1.1	-		DNS	Stan	dand	query	A 51	L.4pub	lish	ers.co	m
1	610	19.7	898	44 🔅	192.1	68.1	1.1		1	92.16	8.1.1	.3		DNS	Stan	dand	query	nesp	onse	A 8.3	15.7.1	.2
Z	870	31.9	102	55 🔅	192.1	68.1	L.13		1	92.16	8.1.1	-		DNS	Stan	dand	query	A ab	<.phob	os.a	pple.c	0
	829	31.7	561	60 🔅	192.1	68.1	1.1		1	92.16	8.1.1	.3		DNS	Stan	dand	query	nesp	onse	CNAM	E COMM	iu 🔳
4																						۶.
E E	rame	520	8: 3	76 ł	ivtes	on '	wire	60	8 hi	ts).	76 by	/t es	can	tured (608 h ⁻	itsì						
														d), Dst			i cc:a	7:31	(00:2	1:29	:cc:a7	.=
)st: 19								•
4																						•
0000	0 00) 21	29	<i>cc</i>	a7 31	00	1.2	70	30 21	5 3 d	08.00	4.5	00		1 n/	. =	c					_
0010					00 00) a8				.>9								
0020	0 01	01	fb	e0	00 35	ōō	2a	42	cc 2'	F 82	01 00	00	01			7						
0030					00 00		69			3 66	72 65	65	6e		irc	.fre	en					
0040	D 6†	- 64	65	03	6e 65	74	00	00	01 0	0 01				ode.n	et	••						-
F	ile: "C:	Users	\adria	n\App	oData\Lo	ocal\Te	emp\w	ire	Packel	s: 1058	7 Displa	yed: 8:	151 Ma	irked: 0 Dro	opped: 0		Profile	: Defau	lt			



- DNS shows info, even if the connection is encrypted
- Unencrypted, the protocol may give a ton of stuff away to a sniffer

📶 Follow TCP Stream	<u> </u>
rStream Content	
<pre>:asimov.freenode.net NOTICE * :*** Looking up your hostname USER adrian skynet irc.freenode.net :purple NICK Irongeek :asimov.freenode.net NOTICE * :*** Checking Ident :asimov.freenode.net NOTICE * :*** Found your hostname :asimov.freenode.net NOTICE * :*** No Ident response :asimov.freenode.net 001 Irongeek :welcome to the freenode Internet Relay Chat Network Irongeek :asimov.freenode.net 002 Irongeek :Welcome to the freenode.net[174.143.119.91/6667], runni version ircd-seven-1.0.3 :asimov.freenode.net 003 Irongeek :This server was created Wed Jun 30 2010 at 20:01:02 CDT :asimov.freenode.net 004 Irongeek asimov.freenode.net ircd-seven-1.0.3 DOQRSZaghilopswz CFILMPQbcefgijklmnopgrstvz bkloveqjfI :asimov.freenode.net 005 Irongeek CHANTYPES=# EXCEPTS INVEX CHANMODES=eIbq,k,flj,CFLMPQcgimnprs CHANLIMIT=#:120 PREFIX=(ov)@+ MAXLIST=bqeI:100 MODES=4 NETWORK=freenode KNOCK STATUSMSG=@+ CALLERID=g :are supported by this server :asimov.freenode.net 005 Irongeek SAFELIST ELIST=U CASEMAPPING=rfc1459 CHARSET=ascii NICKLEN=16 CHANNELLEN=50 TOPICLEN=390 ETRACE CPRIVMSG CNOTICE DEAF=D MONITOR=100 :are supported by this server :asimov.freenode.net 005 Irongeek FNC Find Save As Print Entire conversation (7104 bytes)</pre>	tz rver
Help Filter Out This Stream	⊆lose

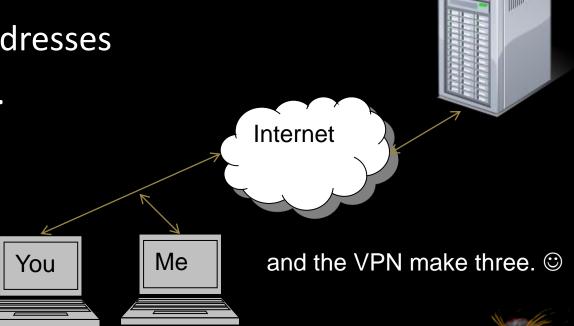
Mitigation

- Awareness
- Don't use those apps when you want to stay low profile
- Sniff to see what your apps give away



More thing that need looking into

- VPN follow home (fun to try at a hacker con ⁽²⁾)
- UPnP/Bonjour
- Phone home addresses
- So much more...



Thanks to d4ncingd4n, Bill Swearingen, Jim Halfpenny and Michael Dickey for suggestions http://Irongeek.com

Clean Room PC/VM

Simply stated:

An attacker should not use the same box for normal use, as for attack.

- Harden up the box as best as you can using what tips have been given
- Full Clean Room PC > Clean Room Boot Partition > Clean Room VM
- Make yourself some dual boot systems!!!



Great tools

- Wireshark <u>http://www.wireshark.org/</u>
- NetworkMinor <u>http://networkminer.sourceforge.net/</u>
- BackTrack Linux <u>http://www.backtrack-linux.org/</u>



Events

- DerbyCon 2011, Louisville Ky <u>http://derbycon.com/</u>
- Louisville Infosec
 <u>http://www.louisvilleinfosec.com/</u>

 Skydogcon/Hack3rcon/Phreaknic/Notacon/Outerz0ne http://www.skydogcon.com/ http://www.hack3rcon.org/ http://phreaknic.info http://phreaknic.info http://notacon.org/ http://www.outerz0ne.org/



QUESTIONS?

42



