Offensive technologies
Fall 2017

Lecture 1 - Intrusion

Fabio Massacci

Course Objective

- Offensive (IT) technologies are
  - a permanent characteristics of a technological society.
  - Due to the very same "features" that make our society advanced.
- The purpose of the course is to give students
  - an hands-on approach to understand the main technological drivers behind security attacks
  - A etter understanding of attacks so that we could better identify methods to defend ourselves
- Offensive technologies are a dangerous tools → "with great powers come great responsibility"

Ethical Issues

Reminder

Ethical Acceptance

- You are bound by the terms and conditions of this course
  - You try offensive technologies **only** in the lab
  - You are **not allowed** to disclose information about any individual that you find during the analysis
  - Your final deliverable, as approved by the professor is **the only public deliverable** you are allowed to disclose to third parties
- Any use outside the agreed framework of the course may be penally relevant (i.e. a crime)
  - Everything is **isolated** from rest of infrastructure → you must deliberately exfiltrate material → cannot claim that "happened by mistake"
  - The same considerations apply if you give material to other students who have not signed the agreement → aiding and abetting = same penal responsibility as if you did it yourself.

What Prosecutors can do

- You did some "innocent prank"
  - plus tweeted "I'm going to destroy America and dig up Marilyn Monroe"
- They can give you slap on the wrist
  - Assuming your "prank" was really "innocent"…
- They can also give you really but really really hard times,
  - Charging "Aggravated Theft" or "Assault with danger to people" or
  - "Organized Crime" or/and
    - Exchanged email with somebody
  - "Collusion with foreign powers" or/and
    - This somebody is not of the right nationality
  - "Terrorism"
    - Possibly planning disruptive actions
- A good lawyer can take you out of jail BUT in the meanwhile
  - They send you to a security prison without bail
- Don't think "This can happen in Uzbekistan but not <here>"
  - Where <here> in { US, IT, FR, DE, etc. etc. }

Why they are going to do it?

- True discussion with a (former) Judge from Italian Supreme Court
  - **IF** a prosecutor want to investigate a computer crime (e.g. your "prank") s/he needs access to emails/internet traces etc.e tc.
  - **BUT** email is protected (this is not North Korea after all)
  - **UNLESS** there is a very serious crime going on
  - **SO** prosecutor claims "this is a very serious crime (eg Organized Crime)"
  - **THEN** judge grants access to your emails (they write to Google and Google gives them everything about your life)
  - **OBVIOUSLY** during the trial all accusations will fail as you have just done a prank (anyhow need to pay a good lawyer, technical counsel)
  - **HENCE** Prosecutor conscience is clean: no innocent people will finally be injustly condemned whilst he can investigate the bad guys
- Side Effects…
  - **WISELY** "charges of serious crimes" go hand in hand with measures limiting offenders (eg you won't let a mafios go around and kill more people)
  - **BUT NOW** you are charged with the same crimes of the dangerous mafioso…
  - **SO** police sends you in a security prison without bail as potential offender...

You don't believe it, do you?

I'm going to destroy America and dig up Marilyn Monroe': British pair arrested in U.S. on terror charges over Twitter joke

y RICHARD HARTLEY-PARKINSON
PDATED: 13:08 GMT, 31 January 2012

Share

View comm

wo British tourists were barred from entering America after joking on witter that they were going to 'destroy America' and 'dig up Marilyn lonroe'.

eigh Van Bryan, 26, was handcuffed and kept under armed guard in ell with Mexican drug dealers for 12 hours after landing in Los Angel ith pal Emily Bunting.

he Department of Homeland Security flagged him as a potential thre hen he posted an excited tweet to his pals about his forthcoming trip lollywood which read: 'Free this week, for quick gossip/prep before I nd destroy America?'

- Leigh, from Coventry, and Emily, 24, from Birmingham, were then quizzed for five hours at LAX before they were handcuffed and put into a van with illegal immigrants and locked up overnight.
  - "When we arrived at the prison I was shoved in a cell on my own but after an hour two huge Mexican men covered in tattoos came in and started asking me who I was.
  - 'They told me they'd been arrested for taking cocaine over the border.
  - 'When the food arrived on the tray they took it all and just left me with a carton of apple juice.'"
- They spent 12 hours in separate holding cells before being driven back to the airport where they were put on a plane home via Paris.

Why OffTechs are here to stay

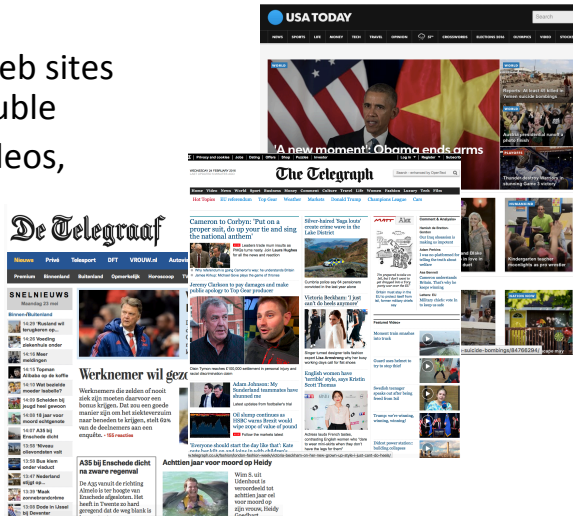
Four questions to better understand the modern context

Do you trust these organisations?

- S-TRUST Authentication and Encryption Root
  - Deutscher Sparkassen Verlag GmbH, Stuttgart, Baden-Wuerttemberg (DE)
- NetLock Kozjegyzoi Tanusitvanykiado
  - Tanusitvanykiadok, NetLock Halozatbiztonsagi Kft., Budapest, Hungary
- TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı
  - Bilgiletişim ve Bilişim Güvenliği Hizmetleri A.Ş. ANKARA, Turkey
- CA 沃通根证书
  - WoSign CA Limited, China
- To guarantee that a website is really what it claims to be?

So, what's that?

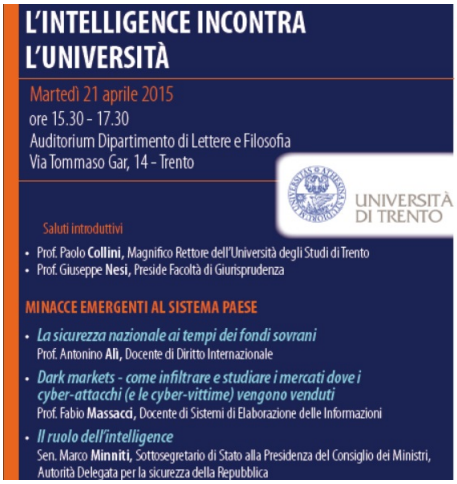
- It is just some web sites without any trouble
- just pictures, videos, and text



What's this?

- ONE webpage
  - Plenty of ads
- Process
  - We DON'T look at the ads
  - Only click on mail
- And download the program of the infosec conference

What's this?


L'INTELLIGENCE INCONTRA L'UNIVERSITÀ

Martedì 21 aprile 2015
ore 15.30 - 17.30
Auditorium Dipartimento di Lettere e Filosofia
Via Tommaso Gar, 14 - Trento

UNIVERSITÀ DEGLI STUDI DI TRENTO

Saluti introduttivi

- Prof. Paolo **Collini**, Magnifico Rettore dell'Università degli Studi di Trento
- Prof. Giuseppe **Nesi**, Preside Facoltà di Giurisprudenza

MINACCE EMERGENTI AL SISTEMA PAESE

- *La sicurezza nazionale ai tempi dei fondi sovrani*
  Prof. Antonino **Alì**, Docente di Diritto Internazionale
- *Dark markets - come infiltrare e studiare i mercati dove i cyber-attacchi (e le cyber-vittime) vengono venduti*
  Prof. Fabio **Massacci**, Docente di Sistemi di Elaborazione delle Informazioni
- *Il ruolo dell'intelligence*
  Sen. Marco **Minniti**, Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri, Autorità Delegata per la sicurezza della Repubblica

INTELLIGENCE LIVE

- ONE PDF file, essentially an image
- What happens if we open it?
  - Nothing
  - Acrobat Reader shows the image on the monitor

What's this?

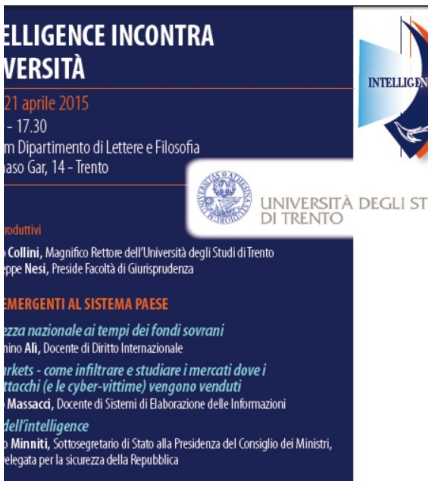
- A photocopier
- A printer
- You send a file, and it prints

What *really is* this? Just like that!

Xerox computer to just print a file:
Intel Celeron - 733 MHZ – 128MB

NASA computer to land Apollo 16 to the Moon
AGC – 1 MHz – 4KB RAM

What *really* is this?



- That's a **program** containing
  - at least 1682 instructions
- What happens when we open it?
  - All instructions are executed
  - Not necessarily true that the result is displayed
- PDF language is Turing Complete
  - **ANY** function can be written in PDF language
  - Opening a PDF file can seamlessly display an image and simultaneously solve Fermat's little theorem

What *really* is this?

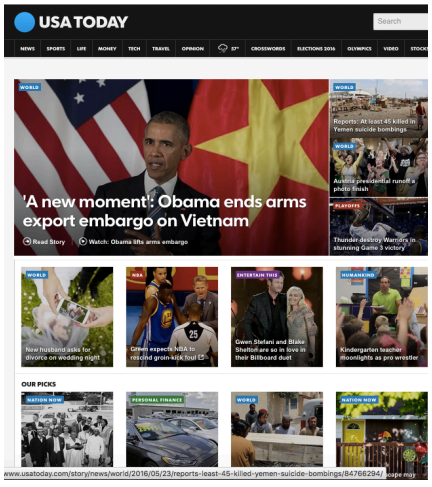
- When we type www.libero.it on the browser, YOUR computer will:
- Execute
  - 186 local functions
  - 15 functions from ***external*** sites
- Aggregate static contents from
  - 676 websites of which
  - 370 external websites
  - 193 may be just images
- Aggregate dynamic content from
  - 8 advertisers (at least)
- Are all of these actions "good" ones?

Cyberlife is never what it seems - UK

- What it REALLY is
- ~~It is ONE web site without any trouble just picture and text~~
- 12 web trackers for advertising
- 72 javascript snips **executed by your browser while you load it**
- More than 100 references to different sites, some of them executing code
  - http://player.ooyala.com
  - http://widget.cloud.opta.net
  - Some of them dynamically created on the fly e.g. by b.scorecardresearch.com
- >100 errors/warnings in processing
- How can you tell what's good what's bad?

Cyberlife is never what it seems - US

- What it REALLY is
- ~~It is ONE web site without any trouble just picture and text~~
- 8 web trackers for advertising
- 122 javascript snips **executed by your browser <u>before</u> you see anything**
- More than 500 references to external sites, many executing code
  - Garretn-cdn.com
  - Brightcove.com
  - Tags.tiqcdn.com
- >164 errors/warnings processing web page
- How can you tell good from bad?
- And I didn't load Flash, sorry …

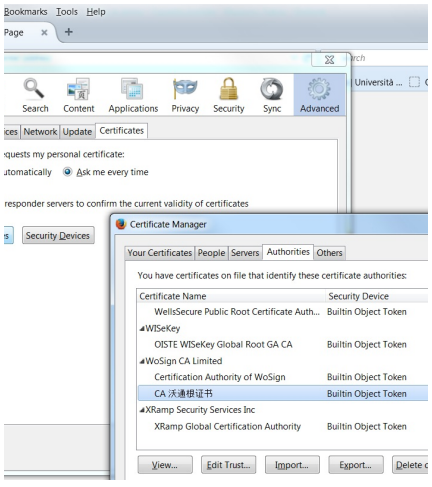


Cyberlife is never what it seems - NL

- What it REALLY is
- ~~It is ONE web site without any trouble just picture and text~~
- 13 web trackers for advertising
- 207 javascript snips **executed by your browser before you see anything!**
- > 200 references to different sites, some of them executing code
  - Easypoll
  - Hotjar
  - Tiq
- >100 errors/warnings in processing the web page
- How can you tell good vs bad?
- And they wanted me to disable the adblocker! Sorry mates…

Who trusts these? Everybody.

- S-TRUST Authentication and Encryption Root
  - Deutscher Sparkassen Verlag GmbH, Stuttgart, Baden-Wuerttemberg (DE)
- NetLock Kozjegyzoi Tanusitvanykiado
  - Tanusitvanykiadok, NetLock Halozatbiztonsagi Kft., Budapest, Hungary
- TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı
  - Bilgİlletişim ve Bilişim Güvenliği Hizmetleri A.Ş. ANKARA, Turkey
- 沃通根证书
  - WoSign CA Limited, China



Are they reliable?

- Read
  - Axel Arnbak, Hadi Asghari, Michel Van Eeten, and Nico Van Eijk "Security Collapse in the HTTPS Market". Communications of the ACM 57, no. 10 (2014): 47-55.
  - http://queue.acm.org/detail.cfm?id=2673311
- Or Listen to
  - https://www.youtube.com/watch?v=uTWqV47QZZw#action=share

Why are OffTech There to Stay?

- Our systems are Beyond-over-provisioned for the tasks we use them
  - The right image is a parent, with the driving license for a Fiat 500, bringing kids to the elementary school two blocks down the road by taxing a Airbus A340
- Being very complex systems it is possible that they have bugs
  - Remember Rice's theorem
- And there always be some people who will make their personal priority to make such bugs happen in other's people computers.

Offensive Approaches

Targeted Attack

- Reconnaissance
- Scanning surface
- Gaining access
  - Somebody let you in
  - Break through
- Maintaining access
- Covering tracks

Untargeted Attack

- …
- Distributing traps
- Gaining access
  - Somebody let you in
  - Break through
- Maintaining access
- Covering tracks

Targeted Attacks

Reconnaissance and Scanning

Phase 1: Reconnaissance

- Learn Information about intended target:
  - How its network is organized
  - Any specifics about OS and applications running
  - Any potential information about users
- Physical Gathering
  - Very human intensive, high risk of being caught, valuable
- Social Web Gathering
  - Human intensive, no risk of being caught, potentially valuable
- Technical Web Gathering
  - Fully automated, some traces maybe left in logs, technical value depends on target

"Physical" Reconnaissance

- Social engineering
  - Call employees and ask details → Instruct the employees not to divulge sensitive information on the phone
    - Sometimes very difficult as your business purpose may be actually to give information (eg Apple's help desk attack)
- Physical break-in
  - Tailgating → Insist on using badges for access, everyone must have a badge, lock sensitive equipment
  - Shoulder surfing, cleaning lady attacks → Clean desk policy
  - How about wireless access?
- Dumpster diving
  - or collect receipt left by previous customer → Shred important documents

"Social Web" Reconnaissance

- Search organization's web site
  - Employee may post something sensitive (thinking it is transient or not accessible)
  - Beware of mailers logs and transient links (search engines might pick them up)
- Search various mailing list archives and interest groups
  - Employees may not post info on themselves as employee but private information might be clue
- Search Web to find all documents mentioning company X
  - Find out what is posted about you

Internet is Forever

- Context:
  - Prof Fabio and Dept Assistant Mirta are looking for CS alumni to invite to the Alumni Event (2017/09/27). Searched the internet with Alice' Name
- Dialogue for Fabio and Mirta to see
  - Alice: I can do everything darling... You know I'm on school trip to X in march? See, if you went to university in X instead of Y… [smile]
    - (DD Month YY at hours H:MM)
  - Bob: these guys bouncing back these things to me, tse… I'm fine where I am darling!!!u_u
  - Alice: pff... -.-" cool down my sweet husband! Is is so funny to tease you !!=) come on, now I'm going to bed!!!!!!!!! Night night! ...big kiss!
  - Bob: night [smile] a hard hard kiss [heart]
    - DD Month YY at hours HH:MM+10minutes
- What do we know now?
  - BobYears can be a good password candidate,
  - Can we send Alice an image with name "School_Trip_X_March_YY.jpg" from a eg a friend's name mispelled? Would this be a credibile email?

"Technical" Gathering

- Look at the plumbing of the internet
  - Whois/ARIN
  - DNS
- Look at the plumbing of the company
  - Scan the network
  - Probe the firewall (firewalking)
  - Probe the individual machines

Whois and ARIN Databases

- When an organization acquires domain name it provides information to a registrar
- Public registrar files contain:
  - Registered domain names
  - Domain name servers
  - Contact people names, phone numbers, E-mail addresses
  - http://www.networksolutions.com/whois/
- ARIN database
  - Range of IP addresses
  - http://whois.arin.net/ui/

Domain Name System

- What does DNS do?
- How does DNS work?
- Types of information an attacker can gather:
  - Range of addresses used
  - Address of a mail server
  - Address of a web server
  - OS information
  - Comments
- Several type of queries (A, CH, HS, MX, SRV, etc.)

Interrogating DNS – Zone Transfer

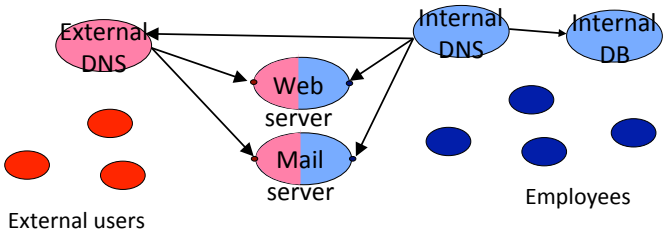
```
$ nslookup
Default server:evil.attacker.com
Address: 10.11.12.13
      server 1.2.3.4
Default server:dns.victimsite.com
Address: 1.2.3.4
      set type=any
      ls –d victimsite.com
system1    1DINA  1.2.2.1
           1DINHINFO “Solaris 2.6 Mailserver”
           1DINMX 10 mail1
web        1DINA 1.2.11.27
           1DINHINFO “NT4www”
```

Sample Strategy

- whois massacci.org
- whois unisi.it
- dig @corallo.unisi.it www.dii.unisi.it any
- dig @corallo.unisi.it CH www.dii.unisi.it version.bind TXT

Protecting DNS

- Provide only necessary information
  - No OS info and no comments
- Restrict zone transfers
  - Allow only a few necessary hosts
- Use split-horizon DNS



At The End Of Reconnaissance

- Attacker has
  - a list of IP addresses assigned to the target network
  - some administrative information about the target network
  - Names of individuals!
  - few "live" addresses
  - some idea about functionalities of target computers
- Tools
  - integrate Whois, ARIN, DNS interrogation and many more services:
  - Applications
  - Web-based portals
    - http://www.network-tools.com

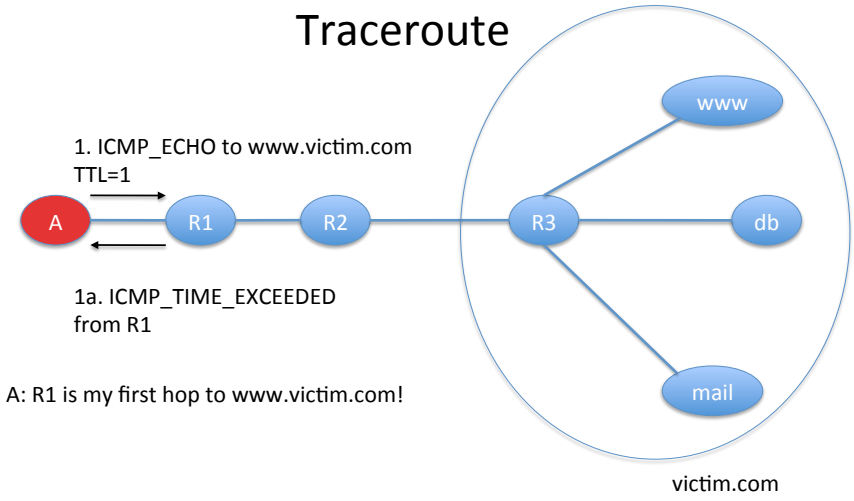
Phase 2: Scanning

- Detecting information useful for break-in
  - Live machines
  - Network topology
  - Firewall configuration
  - Applications and OS types
  - Vulnerabilities

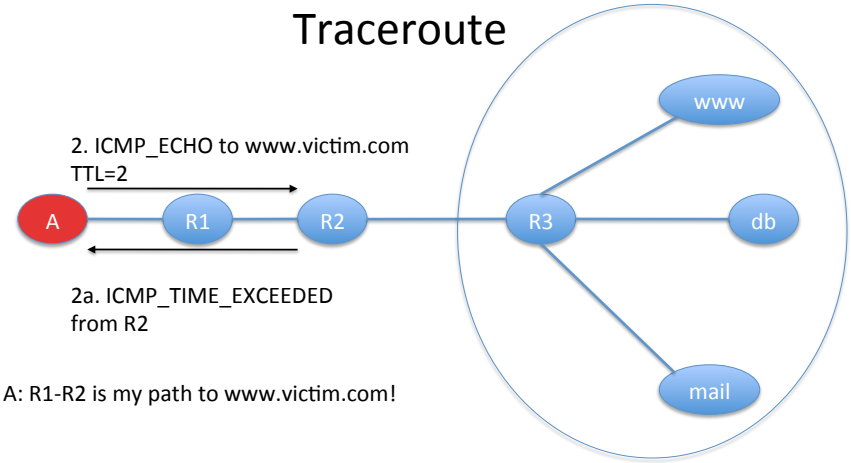
Network Mapping

- Finding live hosts
  - Ping sweep
  - TCP SYN sweep
- Map network topology
  - Traceroute
    - Sends out ICMP or UDP packets with increasing TTL
    - Gets back ICMP_TIME_EXCEEDED message from intermediate routers

Traceroute



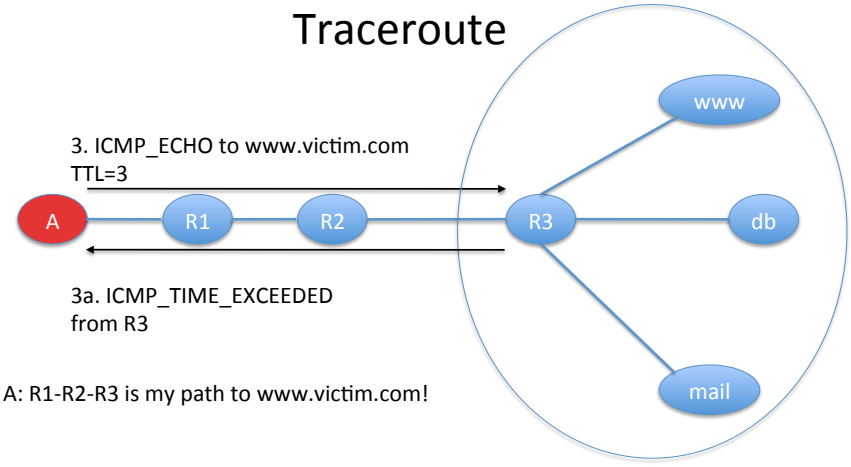
Traceroute



2a. ICMP_TIME_EXCEEDED
from R2

A: R1-R2 is my path to www.victim.com!

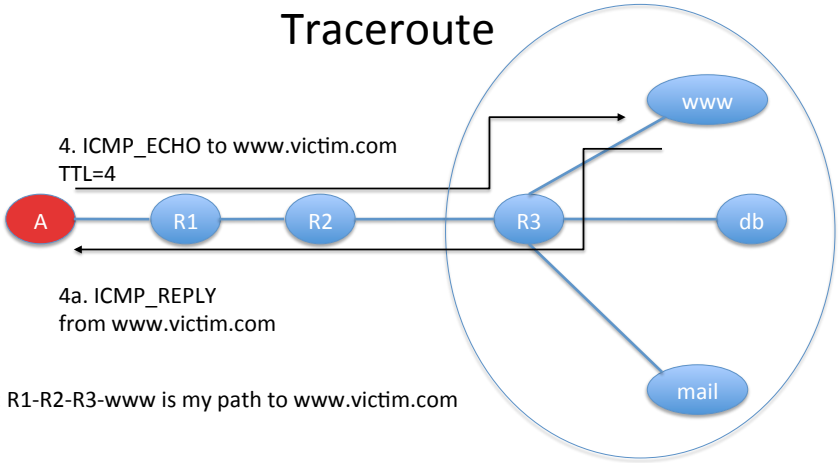
Traceroute



3a. ICMP_TIME_EXCEEDED
from R3

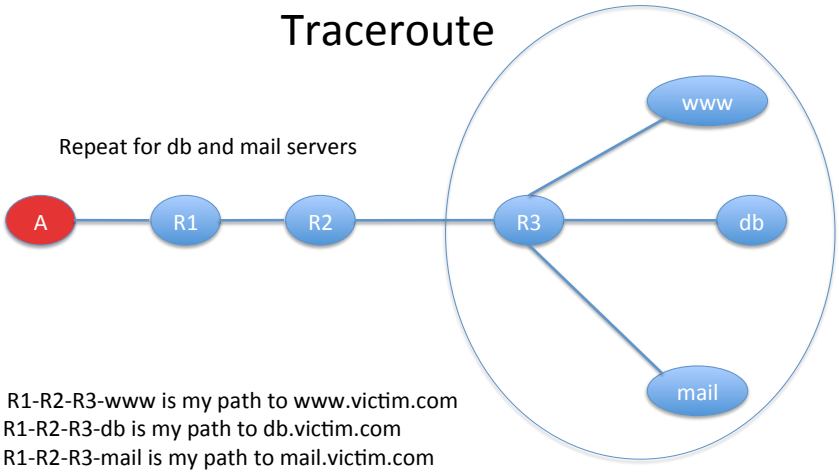
A: R1-R2-R3 is my path to www.victim.com!

Traceroute



A: R1-R2-R3-www is my path to www.victim.com

Traceroute



A: R1-R2-R3-www is my path to www.victim.com
R1-R2-R3-db is my path to db.victim.com
R1-R2-R3-mail is my path to mail.victim.com

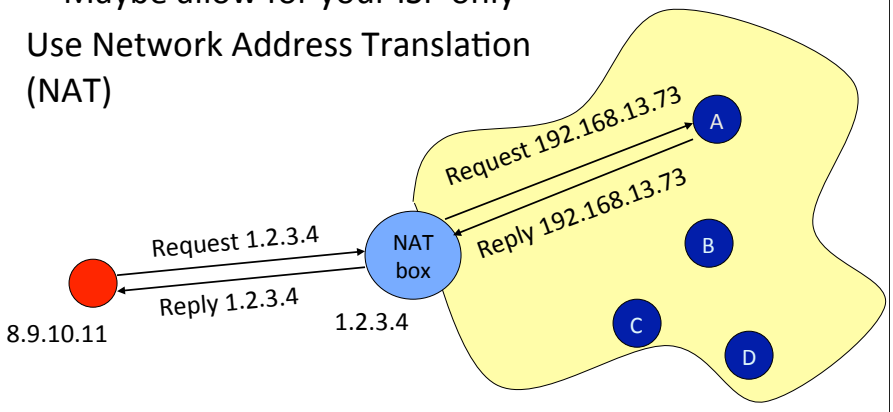
➔ Victim network is a star with R3 at the center

Network Mapping Tools

- Cheops
  - Linux application
  - http://cheops-ng.sourceforge.net/
  - Automatically performs ping sweep and network mapping and displays results in a GUI

Defenses Against Network Mapping And Scanning

- Filter out outgoing ICMP traffic
  - Maybe allow for your ISP only
- Use Network Address Translation (NAT)



How NATs Work

- For internal hosts to go out
  - B sends traffic to www.google.com
  - NAT modifies the IP header of this traffic
    - Source IP: B ➔NAT
    - Source port: B's chosen port Y ➔ random port X
  - NAT remembers that whatever comes for it on port X should go to B on port Y
  - Google replies, NAT modifies the IP header
    - Destination IP: NAT ➔B
    - Destination port: X ➔ Y

How NATs Work

- advertise your web server A at NAT's address (1.2.3.4 and port 80)
- NAT remembers that whatever comes for it on port 80 should go to A on port 80
  - External clients send traffic to 1.2.3.4:80
  - NAT modifies the IP header of this traffic
    - Destination IP: NAT \A
    - Destination port: NAT's port 80 \ A's service port 80
  - A replies, NAT modifies the IP header
    - Source IP: A\NAT
    - Source port: 80 \ 80

How NATs Work

- What if you have another Web server C
  - You advertise your web server A at NAT's address (1.2.3.4 and port 55) – not a standard Web server port so clients must know to talk to a diff. port
  - NAT remembers that whatever comes for it on port 55 should go to C on port 80
  - External clients send traffic to 1.2.3.4:55
  - NAT modifies the IP header of this traffic
    - Destination IP: NAT \C
    - Destination port: NAT's port 55\ C's service port 80
  - C replies, NAT modifies the IP header
    - Source IP: C\NAT, source port: 80 \ 55

Port Scanning

- Finding applications that listen on ports
- Send various packets:
  - Establish and tear down TCP connection
  - Half-open and tear down TCP connection
  - Send invalid TCP packets: FIN, Null, Xmas scan
  - Send TCP ACK packets – find firewall holes
  - Obscure the source – FTP bounce scans
  - UDP scans
  - Find RPC applications

Port Scanning

- Set source port and address
  - To allow packets to pass through the firewall
  - To hide your source address
- Use TCP fingerprinting to find out OS type
  - TCP standard does not specify how to handle invalid packets
  - Implementations differ a lot
- Tools: Nmap (http://nmap.org/)
  - Unix and Windows NT application and GUI
  - Various scan types + adjustable timing

Defenses Against Port Scanning

- IF you (As SysAdmin) can tamper with targets
  - Close all unused ports
  - Remove all unnecessary services
  - Filter out all unnecessary traffic
  - Find openings before the attackers do
  - Use smart filtering, based on client's IP
- If you cannot tamper with target
  - Put a firewall in between to drop all the unwanted connection

Firewall Flavors

- Packet filters
  - Stateless
    - Allow all traffic to port 80
  - Statefull
    - Allow all traffic to port 80 on established connections
- Proxies
  - Capture all traffic and reissue it with source IP of the firewall – normalizes traffic

Firewalk: Determining Firewall Rules

- Find out firewall rules for new connections
- We don't care about target machine, just about packet types that can get through the firewall
  - Find out distance to firewall using traceroute
  - Ping arbitrary destination setting TTL=distance+1
  - If you receive ICMP_TIME_EXCEEDED message, the ping went through

Defenses Against Firewalking

- Filter out outgoing ICMP traffic
- Use firewall proxies
  - This defense works because a proxy recreates each packet including the TTL field
  - The destination host would have to be set up to ignore messages that are not allowed

Vulnerability Scanning

- The attacker knows OS and applications installed on live hosts
  - She can now find for each combination
    - Vulnerability exploits
    - Common configuration errors
    - Default configuration
- Vulnerability scanning tool uses a database of known vulnerabilities to generate packets
- Vulnerability scanning is also used for sysadmin

Defenses Against Vulnerability Scanning

- Close your ports and keep systems patched
- Find your vulnerabilities before the attackers do
- Tools
  - SARA
    - http://www-arc.com/sara
  - SAINT
    - http://www.saintcorporation.com
  - Nessus
    - http://www.nessus.org

At The End Of Scanning Phase

- Attacker has
  - a list of "live" IP addresses
  - Open ports and applications at live machines
  - Some information about OS type and version of live machines
  - Some information about application versions at open ports
- Information
  - network topology
  - firewall configuration
  - Software vulnerabilities