## [**https://www.youtube.com/watch?v=U1XYlxWka4g**](https://www.youtube.com/watch?v=U1XYlxWka4g)

Firefox Privacy Setup:

Settings:

General tab:

Uncheck check spelling as you type

Check always ask for downloads

check for malware on an untrusted storage device by opening it in a linux distro on a USB

<https://www.youtube.com/channel/UC2Mq09_FBWckT1WmcraWr-g/videos?view=0&sort=p&flow=grid>

192.168.1.31

<https://www.toptal.com/raspberry-pi/how-to-turn-your-raspberry-pi-into-a-development-server>

## 

## **How to create an unhacked machine, for the ultra paranoid**

## Build your own air gapped machine. Transfer files to it through a flash drive, after formatting the flash drive and scanning all files you transfer for malware. Use this machine to store your most personal files. Journal, plans for world domination, compromising video and pictures, other secure information (passwords, credit card numbers, safe codes, etc). Add a hard drive backup that has never been plugged into a machine that has an internet connection. Don’t even add a NIC to the machine. It’s the only way to guarantee nobody is getting in. Keep the machine under a physical lock and key, which is unlocked only by you. Encrypt the machine and memorize the code. Do not write it down anywhere, the only place the password should live is inside your head. Unless they can read your mind, they cannot decrypt it. A bloated OS creates multiple potential points of failure in your security. Ideally you would create your own OS or run a skeleton version of an OS, only installing the essential programs you would need to work on the data you store on this machine.

verify Digital Signatures of programs

<https://keepassxc.org/verifying-signatures/>

Windows 7 is no longer receiving security support after Jan 2020. Research the risks involved with Win 7 and the need to upgrade to a more secure OS.

## 

## **Hacking and Pentesting:**

You need clear written permission to conduct ethical hacking activities

## A bloated OS creates multiple potential points of failure in your security. Ideally you would create your own OS or run a skeleton version of an OS, only installing the essential programs you would need to work on the data you store on this machine.

**Goals:**

* take an ethical hacking/pentesting course

**The 5 phases of hacking:**

* recon / info gathering: active vs passive
* Scanning & enumeration: Nmap, Nessus, Nikto
* gaining access
* maintaining access
* covering tracks

**Passive recon:**

Location information:  
Satellite images

Drone recon

Building layout (badge readers, break areas, security, fencing)

Job information:  
Employees (name, title, phone number manager)

Pictures (badge photos, desk photos, computer photos, etc)

RFID cloner (boss cloner)

web/host:

Target validation: WHOIS, nslookup, dnsrecon

Finding subdomains: google fu, dig, nmap, sublist3r, bluto, crt.sh

Fingerprinting: nmap, wappalyzer, whatweb, builtwith, netcat

Data breaches: haveibeeenpwned and other similar lists

OSINT tools

Hunter.io

1.4 billion cleartext credentials analysis nlp

**Research these common packet analyzers:**

cain and abel – recovers passwords

NarusInsight – monitors all internet traffic

Sniff – monitors a network for interesting traffic

Ettercap – intercepts traffic on network segment

Tcpdump – runs from the command line

## **Cybersecurity Research:**

Learn how to protect the assets you manage

How to avoid being recorded on your mobile devices and laptops

Research airbagged machines

Chanology

Research social engineering

Pwn2Own competition

4 chan

Integer overflow

Willybot cryptocurrency trading bot

APT advanced persistent threat

Hal Turner FBI informant

Gregg housh

Adrian chen

Brian mettenbrik

Low orbit ion cannon

Gabriella Coleman

Pokeanon

Joshua corman

Steven levy

Julian Assange

Wiki leaks

Richard thieme

Telecomix

Wired threat level

Hbgary

George Holtz

Lulsec

Sabu

Black hat con

Lopht

Funkill anonymous

stressors

You pay someone with lots of bots boat overload a server with requests

Binary executable

Plex code

Hacking democracy 2006

Telecommunications engineering

Lawful intercept

Isolate the malware

James bamford

Deep sec Vienna November 2016 james bamford talk

Votaphone Greece malware in 2004

Stacks and trees

Cross site scripting

Certificate authority

Man in the middle attacks

Superfish scam

Password cracking dictionary

Memory exploits

Tracking cookies and ghostly

Research encryption

How long does it actually take to decrypt something?

Is it possible to encrypt something in a way that makes it impossible, at least for a little while, to decrypt?

What does online privacy mean?

Why don’t people care about privacy online?

bugging rooms and surveillance equipment

Digital locks

Home alarm systems (vivint)

Most secure linux flavor

Windows security flaws

browse internet from virtualbox

Research all the ways social media tracks us

How do ad agencies use our browsing patterns to sell us shit?

Big tech and censorship

Removing mics and blocking cameras on mobile devices

You have to learn how to take apart mobile devices

Jailbreaking an iphone

How to live without social media

What are the functions of social media? What do they provide you with? Why do people think social media is necessary? Do surveys

how to become completely anonymous online

Twitter research

Can mobile devices become untraceable?

Research tech jobs

**What your IP address says about you**

**Research the best VPN**

**Conventions:**

**Defcon**

**Zero Day con**

Security approach: compartmentalization

The cybersecurity market

Security analyst jobs

Research Threat Modeling

**An overview of the current security landscape and the major players**

How to become unhackable and untrackable

Basic security best practices

* Passwords
* Phishing
* most common ways people are hacked

**Basic Password Security (2FA)**

**Browser Security, Cookies and other tracking**

**Mobile Security**

**Protecting Against Social Engineering & Avoiding Scams (phishing)**

**Crash course to the Darknet**

**Signal:** is it actually safe?

Diceware

FAA 702

**AES (alias Rijndael) or Twofish encryption algorithm using a 256 bit key.**

Cybersecurity blogs

How to prevent phishing

Research the digital nomad lifestyle

Cloudflare: hosting without censorship

Research imsi catchers

Finspy mobile

Research Kindle books

Interacting with technology security best practices

Ransomware

Nsa leak

gdpr

wpa2 can be cracked

cybersecurity on Medium

Shadow brokers

North Korea cyber organisation known as the Lazarus Group

The patriot act and the NSA

Research edward snowden

Bit nation

The cypherpunks in 1988

Tracking cookies (persistent cookies)

Check out samy kamkar website

Stuxnet spyware

Pbkdb2

Targeted siemens plcs

PLCs:computer attached to state infrastructure

How to search and browse for anything you want without fear.

Zero day exploit

Digital certificates

HTTPS and SSL

If I steal your cookies, i can pretend to be you on a website.

How to make sure than when you click on a link or send data, it is not scripted

If you want to protect from any government or entity you have to protect yourself from all

secureset.com/academy

Jeff Moss founder of defcon

UART based hacks: interacts with debug ports on board

one wire for transmit (TX0, one for receive (RX, and one wire for ground

different voltage levels: 1.8v, 3.3v, 5v

on the staples connect -uboot you can short out the NAND pins 29/30 to ground after powering on, which corrupts the uboot environment

EMMC sd card like, connect and modify storage directly

Command injection-related bugs

Firing up burp proxy

**Artificial scarcity DoS**

other application DoS possibilities:

disrupt an ecommerce business selling a sought-after product (video games/consoles, iphone, etc)

login denial of service

solving captchas: done in 3 days

OCR, a low cost attack on a microsoft captcha, a low cost automated attack on yahoo captchas

jeff yan and ahmad salah el ahmad school of computing science

mechanical turk “the turk”

pc stripper helps spam to spread

solving and creating captchas with free porn

solving captchas for cash: ha.ckers.org

recover someone else’s password: hijack a sprint user’s account with just a cell phone number

flawed security lets sprint account get easily hijacked

email preferred over secret questions

Pineapple - mobile hacking

application service providers (ASPs)

offer hosting for banks that can be hacked and exploited across dozens of credit unions

the system:

an asp provides hosting for banks, credit unions and other financial services companies. Banking application have three important url parameters: client\_id, band\_id & acct\_id

breaking the bank (vulnerabilities in numeric processing within financial applications)

woman admits fleecing shopping network of more than $412k

**affiliate scams**

online merchants and advertisers enlist the services of affiliate networks to drive traffic in exchange for a share of generated revenue

creating a network of sites that generates ad revenue

cookie stuffing

nothing besides pesky affiliate networks terms of service requires the user to actually click a link to be cookied with an affiliate id

Blakhatworld.com

seoblackhat.com/forum

gfy.com

Whitehat sentinel:

unlimited assessments. Customer controlled and expert managed – the ability to scan websites no matter how big or how often they change

coverage – authenticated scans to identify technical vulnerabilities and custom testing to uncover business logical flaws

virtually eliminate false positives – operations team verifies results and assigns the appropriate severity and threat rating

development and qa – whitehat satellite appliance allows us to service intranet accessible systems remotely

improvement and refinement – real-world scans enable fast and efficient updates

hacking types

cross-site scripting

information leakage

content spoofing

predictable resource location

sql injection

insufficient authentication / authorization

abuse of functionality

http response splitting

directory indexing

Buffer overflows

affiliates start posting their code on Ssl pages

Dns rebranding, gifar, flash malware

sec vs the estonian spiders

ukrainian hacker makes a killing in stock market fraud

ukrainian hacker may get to keep profits

mac terminal commands

jeremiahgrossman.blogspot.com

treyford.wordpress.com

Ethan Zuckerman / geekcore

what is teensy

The free network foundation in brooklyn

Dropping usb devices: small binary less persistent reverse shell, a small payload that spawns a reverse shell without triggering AV

ARP: address resolution protocol, used on LAN

The network stack on your OS

How to change your MAC address so you are untrackable

# 

Reddit research:

* Crypto investing
* Psychedelics
* Darknet
* Cybersecurity
* Hacking

electronics repair (hardware tech)

blinking twelve problem

the failures of Web of trust

signal betrays your phone number?

Pidgin and initiating OTR

identity based encryption

GnuPG

S/MIME

OpenAI, democratization of AI

emergent AI

* Google sound search?
* Research all the capabilities of an android phone

[**https://www.ietf.org/**](https://www.ietf.org/)

[**http://ww**](http://ww/)[**w.ietf.org/rfc/rfc2396.txt**](http://www.ietf.org/rfc/rfc2396.txt)

encrypting 7-zip files

twitter cybersecurity accounts to follow (Joseph Cox)

security differences between a rooted and unrooted device

Enigmail Thunderbird plugin, problems with key management

pgp, gpg and X.509-style PKI

typosquatting

normalization and IDNA and PRECIS and label generation rules

RISC V completely "solves" the Spectre problem.

OTR + XMPP is from a usability perspective a raging dumpster fire. XMPP

has a piss poor support for people changing from device during a

conversation, OTR even less so.

<https://www.gwern.net/index>

user interface design for effective security remains an open problem

Signal uses TOFU + GSM checking, but that has two vulnerabilities:

- if your target does not use Signal, you can impersonate him by exploiting SS7

or similar hack (however, SS7 manipulation is not exactly easy)

- changing of phone without restoring the original key means a warning that the

key has changed, so you now have to do the fingerprint checking again

Yes, web-of-trust is a failed concept. What I usually do if I can't get a

fingerprint from other channel, is to google for it and check google cache

whether a person put it on their webpage (then check whois, etc). Keybase.io is

a tool that can make this work, but it's not as well known.

**Mailpile:**

A free software Gmail-type replacement with PGP encryption built in is

approaching its 1.0 release after nearly 6 years of work:

https://www.mailpile.is/

They also just hired some devs to finish up the Mac and Windows

packaging: https://twitter.com/MailpileTeam/status/973594524730699776

Among a lot of other amazing things, Mailpile has implemented encrypted

subject headers via Memory Hole:

https://twitter.com/HerraBRE/status/831636607543427072

https://github.com/mailpile/Mailpile/issues/156#issuecomment-279998595

https://github.com/autocrypt/memoryhole

Mailpile has some good blog posts about PGP:

https://www.mailpile.is/blog/2014-10-07\_Some\_Thoughts\_on\_GnuPG.html

https://www.mailpile.is/blog/2015-02-26\_Revisiting\_the\_GnuPG\_discussion.html

https://www.mailpile.is/blog/2016-12-13\_Too\_Cool\_for\_PGP.html

That last blog post is a response to anti-GPG posts like this one:

<https://moxie.org/blog/gpg-and-me/>

Signal on Android is \*not\* 100% free software because it does not build

without these nonfree libraries:

https://github.com/signalapp/Signal-Android/blob/master/build.gradle#L67-L69

The play-services maven repo also would need to be removed from Signal,

but no one has figured out how to do that and still get it to build:

https://gitlab.com/fdroid/fdroiddata/merge\_requests/1229#note\_4151671

It'd be great if Signal or some independent contributors could address

this issue and provide a way to have an APK that is 100% free software,

but I'm not holding my breath. Please contribute to this if you can!

LibreSignal has the exact same problems and so it isn't Libre and should

stop using Libre in the name because that is super confusing:

https://github.com/xmikos/fdroiddata/issues/43 https://fdroid.eutopia.cz/

Signal for GNU+Linux has a number of issues with it as well, some of

which are outlined here: <https://labs.riseup.net/code/issues/15200>

XMPP+OMEMO is way better than XMPP+OTR: https://conversations.im/omemo/

You can find clients with OMEMO support here: https://omemo.top/

You have to make sure you're using an XMPP server with the proper XEPs

installed. Use this chart if you need help finding one:

<https://conversations.im/compliance/>

NeoPG is a modern drop-in replacement for GnuPG 2: https://neopg.io/

A presentation on NeoPG can be viewed at around minute 47 here:

[https://media.ccc.de/v/34c3-9258-lightning\_talks\_day\_4#t=2855](https://media.ccc.de/v/34c3-9258-lightning_talks_day_4" \l "t=2855)

Briar is a new kid on the block which looks promising:

https://briarproject.org

<https://media.ccc.de/v/34c3-8937-briar>

Ricochet doesn't seem to be updated often enough, but is worth

mentioning as a possible email replacement:

https://github.com/ricochet-im/ricochet <https://ricochet.im/>

A GPG alternative: <https://github.com/stealth/opmsg>

decrypts easy hashes

<https://hashkiller.co.uk/md5-decrypter.aspx>

secure MIME: authentication, integrity and digital signatures

Tracking cookies (persistent cookies)

Check out samy kamkar website

Zero day exploits

Digital certificates

If I steal your cookies, I can pretend to be you on a website.

[Wigle.net](http://wigle.net/)

homeland security EINSTEIN program meant to identify cyber attacks in real time

Man in the middle: MITM

secureset.com/academy

How to change your MAC address so you are untrackable

layered defense: firewalls, ids, ips, and anti malware

vulnerabilities provide attack vectors

Research imsi catchers

Finspy mobile

The patriot act and the NSA

Research edward snowden

Bit nation

The cypherpunks in 1988

configuration errors

unpatched systems

human error

software flaws

More aggressive attacks: trojan horses, rootkits & spyware. Many involve social engineering

polymorphic malware

instant messaging, IRC and p2p requires installing custom software, makes machine vulnerable

End user license agreements allow companies and people to use your computer in ways that you did not intend.

Wireless networks: 802.11 standard (WIFI) is insecure by nature

most modern vehicles can be hacked, hackers infiltrate computer control systems and manufacturers are exploring vulnerabilities

avoid connecting to untrusted networks that you do not control

malware and phishing attacks, credit card fraud,

protect yourself: change passwords often and don’t use the same password twice

Social engineering: physical attack vectors, gaining unauthorized access to a facility, cutting fiber optic backbone, breaking into secure spaces and equipment

ASLR

Thoroughly explore tails documentation

**Threat model:** profiles attackers and their type of attacks,

**Attack vectors** specify particular techniques targeted towards specific threats

**Security architects** need to create solutions that keep systems secure

Social engineering is best. People are always the easiest vulnerability to exploit.

Drop a bunch of flash drives in a public place

Kali linux rootkit

“Can I use your phone? Mine is dead and I need to call my mom”

Learn the technical specifics behind hacking 4g / wifi spots

Veracrypt

**Operation nightdragon**

Stuxnet spyware

* Targeted siemens plcs
* PLCs:computer attached to state infrastructure

secure access to buildings and rooms

audit services, users and administrators

secure backup media

disable drives

protect industrial printers

**data mining printers**

malware: umbrella term for malicious software

virus, worms, trojan horses, ransomware and spyware, delivered via scripts in programs and active content such as gifs and images, spreadsheets

viruses and worms: self replicates and infects multiple systems

reconnaissance attacks are sneaky and passive

denial of service attack

session initiation protocol, sets up, maintains and ends session for protocols such as voip and im

a SIP flood

**hacker:** first used in MIT in 1990, usually has a negative connotation

Black hat: the bad guys, a “cracker”. Objective is to cause harm by engaging in criminal activities. They operate on the dark web.

White hat: ethical hackers who have the support of government and industry, contracted by employers and security companies. Trained to test and break into systems

Ethical hackers look for vulnerabilities in a system and report them to strengthen their security

Grey hat: they may try to gain access to a system without permission but not with malice. They will notify a target that their system is vulnerable.

Hackers take advantage of common mistakes. Attacks can occur from outsiders and insiders. You should defend using a layered approach at multiple locations. Attacks may not need advanced techniques for success.

Three defense pillars:

technical controls: should detect and protect, centralized correlation, tuned to provide early detection

Firewall: hardware and software based mechanism that is based on a set of rules for access control and activex filtering.

research activex

Next-gen firewall: they provide firewall, intrusion prevention, antivirus, data loss prevention and protection while reducing complexity.

Spam filters, packet shapers and honeypots

Network isolation using VLANS

encryption and access control

**TOGAF – ITIL -COBIT**

A set of well defined standards that follow business needs

Security plan > policies > procedures: the template is found at NIST

What assets need to be protected? Who has access to these assets? What is the potential for damage? What protection mechanisms are already in use?

CVE and US-CERT reveals latest vulnerabilities

OWASP: organization aimed at increasing awareness of information security

Top vulnerabilities:

SQL injections: used in relational databases

broken authentication and session management: a session should “time out” after inactivity

cross site scripting: inserts malicious code in the form of a client side scripting

XSS safeguards: white list input validation on all user input

content security policy CSP HTTP response header

defines what resources are allowed to load and locks if anything else is given

content security policy: ensure content is only from the site’s domain

**Understand the services shepherd shield provides**

**Research other security apps like it**

**Scanning someone else’s system is considered a hostile act.**

Scanning tools: retina community, nesus, qualys free scan & microsoft baseline security analyzer

Remove sim card from the phone and check to make sure it is not being monitored, get yourself a burner and use to call people if necessary

Wireshark

Charles (web debugging proxy)

NightHawk (ARP/ND spoofing and password sniffing)

Arpy (ARP spoofing)

Dsniff (password sniffing)

Kali Linux (penetration testing)

Network intrusion

Sniffing

Man-in-the-middle

Cybersecurity Certs:

* Systems Security Certified Practitioner, International Information Systems Security Certification Consortium
* Certified Information Systems Security Professional
* Cyber Training 365: Certified Security Analyst Training Course

Most common way companies and people get hacked: phishing

**Authentication** is the process by which a computer determines who it is interacting with it

IDS/IPS, penetration and vulnerability testing

DLP, anti-virus and anti-malware

TCP/IP, computer networking, routing and switching

Firewall and intrusion detection/prevention protocols

Network protocols and packet analysis tools

Security Information and Event Management (SIEM)

Security access is assessed through these 2 questions:

Who are you? / What should you have access to?

All forms of authentication can be overridden, so it’s best to use 2 or more authentication methods, two factor or multi factor authentication

**Access control:** Permissions list (ACL)

* Read permissions
* Write permissions
* Execute permissions

No read up, no write down ACL model: bell lapadula model

* Other models: chinese wall model & biba model

Security kernel, trusted computing base: a minimal set of operating system software that is as close to provably secure as possible. The biggest challenge is determining what goes into it

Go to [Defcon](https://www.defcon.org/) in August (hacking conference)

Password entropy: the amount of information held in a password

* Hackers will test your password and email against HUNDREDS of sites

[How to encrypt and send a file that has an expiration date](https://www.addictivetips.com/windows-tips/quick-crypt-encrypt-files-and-set-schedule-a-delete-date-for-them/)

**Cyber Security Certifications:**

* CompTIA A+, Network+, Security+ & Linux+
* CompTIA Advanced Security Practitioner (CASP)
* CompTIA CSA+
* Microsoft MCSA
* Cisco CCENT & CCNA
* Certified Ethical Hacker (CEH)

[The information security forum](https://www.securityforum.org/)

[Canary Tokens](https://www.stationx.net/canarytokens/)

SABSA stands for the Sherwood Applied Business Security Architecture, and is a leading methodology for developing business operational risk and opportunity-based architectures. It provides a framework for developing risk driven enterprise information security and information assurance architectures. It also helps deliver security infrastructure solutions that support critical business initiatives.

[Enterprise Security Architecture: A Business-Driven Approach](https://www.amazon.com/Enterprise-Security-Architecture-Business-Driven-Approach-ebook/dp/B00UVAQ75G/ref=mt_kindle?_encoding=UTF8&me=)

[Guidelines for information security management](https://www.iso.org/standard/56742.html)

**Reconnaissance:** You will have to learn to think like an enemy in order to gain an outside perspective on the security level of your network

Open Source Intelligence: OSI

Whaling: phishing attack against a VIP

Phishing Attack

Spearheading:

xkcd password strength

No typed passphrase is immune to a keylogger

Active scanning:

* Network scanning / mapping
* Os scanning / fingerprinting
* Web app vulnerability scanning

We need to capture packets that hold important information as they move from node to node.

Capturing packets:

* Wired network
* Network tap
* hub (devices much like switches)

Wireless network

* Promiscuous or monitor mode

Capture the handshake that occurs with wpa2 to determine password

OSINT source include google, internet registries, domain names & social media sites

Devices in promiscuous or monitor mode can ‘listen’ to other devices around them

**The toolkit for reconnaissance:**

* **NMAP:** Command line: man nmap
* Ifconfig

**Goals & Learning Objectives:**

* Master the fundamental building blocks of security & privacy
* Understand the online threat and vulnerability landscape
* Perform threat modeling and risk assessments
* Determine personal threats and adversaries
* Master encryption
* Understand Windows, MacOS, Linux security & privacy features
* Be able to mitigate social engineering attacks
* Use isolation and compartmentalization effectively

**Checksum**

## **Government Surveillance Research:**

June 1st, 2015: Patriot Act Provisions Expired

Government programs: mystic, muscular, xkey-score, & prism,

patriot Act Section 215: Controversial provision that was renewed

The library records provision

Requires businesses to “hand over any tangible things for an investigation to protect against international terrorism”

What are the government's capabilities: edward snowden in 2013

The government can eavesdrop on any phone call and track you online

Research Julian Assange

People in the NSA and other security agencies using government surveillance services for their own nefarious purposes.

Domestic surveillance and foreign surveillance.

Executive order Eo12333

SIGINT system

Research William Binney

Stellar wind program

There is no court oversight for these programs.

Bluffdale, Utah. The NSA’s largest repository of data

keith Alexander, congressional hearing in 2012

2006, MARK Klein NSA and AT&T class action lawsuit

Jewel V. NSA

Gen. Clapper congressional hearing, full

SSO Special services operations

CNN: millions of american’s phone records seized

Report: US Tracking Verizon Calls

Glenn Greenwald, Guardian, Snowden story

This court order allows the government to track anyone and everyone, regardless of their association with anti-government groups or criminal records

Look at the Wikileaks documents

Washington post article & the guardian, the NSA and FBI are directly tapping into servers of large tech companies.

TEMPORA

Research all the Nsa surveillance bases that exist around the world.

Laura Poitras

Prism: collection directly from the servers of: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.

Upstream: Collection of communications on fiber optic cables and infrastructure as data flows through them.

Stellar Wind Washington Post

The five eyes governments

Thomas Drake, NSA whistleblower

The 4 major tech players: they have access to all your data

google

facebook

amazon

apple

## **History of hacking:**

Hacking was born in 1971: captain crunch “blue box phone phreaking”

1980: the PHIRM published guides on breaching systems

1986: how to get anything on anybody book

1989: hacking bank of america’s home banking system

1988: robert morris, launched a worm on ARPANET

1993: first defcon

2000: “I love you virus”. An email attachment that when opened was sent to everyone in the recipient’s email contact list