MODULE 00 FIELD EXERCISE

Self-Targeting: Map Your Exposure, Then Close It

TASK: Collect what an adversary could obtain about you without a warrant, reduce it, and confirm the reduction.

CONDITION: Given your own phone, laptop, home network, and online accounts, an internet connection, and a two-week window for mailed and emailed replies. You work only against your own identity, devices, and home.

STANDARD: Baseline exposure documented across four vectors (data held, identity brokers, home and RF, browser fingerprint) and scored. The listed hardening actions and opt-outs completed and dated. The re-measured score brought below baseline on the fingerprint and the identifiable-device count, and the adversary summary written.

> SAFETY FIRST
>
> Only run these tools on your own accounts, devices, and home network, never anyone else's. Some tasks need your real SSN or date of birth. Only enter those on the exact sites listed here, because look-alike sites are built to steal them.

PHASE 1 · RECON: MAP YOUR EXPOSURE

Task 1 · Pull what the platforms hold

1. Google: go to `takeout.google.com`, click Deselect all, check only the products you want, click Next step, and have it emailed to you as a .zip. Open it and look through your location history, searches, and ad profile.
2. Apple: at `privacy.apple.com`, open Get a copy of your data, check the categories you want, pick a file size, click Continue, then Complete request.
3. Meta: go to Settings > Accounts Center > Your information and permissions > Download your information > Download or transfer information. Pick your account, click Next, choose Available information, and Meta emails you when it is ready.
4. Score: how many of the data categories surprised you? Write that count in the Data held row, Baseline.

Task 2 · Pull your financial and identity files

1. Credit: at `annualcreditreport.com`, the only official site, pull all three bureaus using your name, date of birth, SSN, and current and previous address. It is free every week.
2. LexisNexis: ask for your full file at `consumer.risk.lexisnexis.com/request`. They mail you back a link; if nothing shows up within 10 days, call 888-497-0011.
3. Acxiom: go to `acxiom.com/privacy/us/consumer-instructions`, follow it to the portal, and ask for your access report.
4. Score: count the old addresses, relatives, or contacts listed that you never gave them. Write it in the Identity brokers row, Baseline.

Task 3 · Request your carrier record

1. Open your carrier's data-request tool: Verizon Privacy Dashboard `verizon.com/privacy/your-data`, AT&T Choices and Controls `about.att.com/privacy/choices-and-controls.html`, or T-Mobile `t-mobile.com/privacy-center/personal-data-request`.
2. Ask for the Access or Right to Know request, not a marketing opt-out, and verify your identity. The report comes back later, not on the spot.
3. Score: when it comes back, add the years of location or call history it covers to the Identity brokers row.

Task 4 · Audit your network and find your home on the map

1. Find your router's address: on Windows, run `ipconfig` and read the Default Gateway; on a Mac, go to System Settings > Network > Details > TCP/IP > Router. It is usually `192.168.1.1`.
2. Type that address into a browser, log in with the username and password on the router's sticker, and open the Connected Devices or DHCP Clients list.
3. For any device you do not recognize, look up the first three pairs of its MAC address (the OUI) at `maclookup.app` to see who made it. If the second character of the MAC is 2, 6, A, or E, the address is randomized and the lookup will not help, so spot the device by toggling its Wi-Fi off and on, and rename it in the router once you know what it is.
4. Look up your router's BSSID (its Wi-Fi MAC) at `wigle.net`. If it is there, your home is already pinned on a global map of scanned networks. Add `_nomap` to the end of your network name to ask mappers to leave it off.
5. Score: count the devices you still cannot identify. Write it in the Home and RF row, Baseline.

Task 5 · Scan what you broadcast

1. Install a free Bluetooth scanner, nRF Connect for Mobile (Nordic Semiconductor) or LightBlue (Punch Through), and start a scan.
2. Check the signal strength (RSSI, in dBm): the closer to 0, the nearer the device. To find one, watch its number and walk around; it climbs as you get closer and peaks when you are on top of it. Treat it as hotter or colder, not a distance in feet.
3. To find the maker, read the Company ID in the Manufacturer Data (Apple's is `0x004C`), not the address. Phones, AirPods, watches, and laptops use random addresses that keep changing, so looking up the vendor by address will not work.
4. To tell which entry is which device, turn that device off and watch which line disappears or drops out.
5. If you carry a Faraday bag, prove it works: pair the phone to a Bluetooth speaker and start audio, then seal the phone in the bag. If the audio stops, the bag blocks the signal.
6. Score: count the devices broadcasting around you. Add it to the Home and RF row.

Task 6 · Census the mics, cameras, and trackers

1. For anything you are unsure about, find its model number (on the back, or in Settings > About) and search the maker's spec page for camera, microphone, far-field, or voice. The spec page settles it.
2. Look it over: shine a flashlight across the edges, since a camera lens flashes back a bright glint and mics show up as tiny pinholes. On a TV the mic is usually in the remote (the voice button), not the screen. Learn the odd ones: the Nest Hub Max has a camera but the regular Nest Hub does not; the Ecobee Premium and Voice Control have a mic but the Enhanced and lite do not; the PS5 controller mic is on out of the box.
3. See what is active right now: on a Mac, an orange dot means a mic is on and green means a camera; on Windows, check Settings > Privacy and security > Camera and Microphone.
4. Check for trackers that are not yours: on iPhone, Find My > Items > Items Detected With You; on Android, Settings > Safety and emergency > Unknown tracker alerts > Scan now.
5. Score: count the mics and cameras. Add it to the Home and RF row.

Task 7 · Measure your fingerprint (baseline)

1. In your everyday browser, go to `coveryourtracks.eff.org` and click Test Your Browser.
2. Score: write down the bits of identifying information it reports (lower is better) in the Browser fingerprint row, Baseline.

PHASE 2 · HARDEN AND CONFIRM: DRIVE THE SCORE DOWN

Task 8 · Close the account and device gaps

1. Go back and do any of the module's Do-It-Now steps you skipped: turn on disk encryption, passkeys, unique passwords, encrypted DNS, high-risk mode, and a short screen auto-lock.
2. Switch off any Wi-Fi and Bluetooth you are not using, and unplug or get rid of the unknown or unneeded devices you turned up in Tasks 4 to 6.
3. Thin your daily carry of RFID: contactless cards, transit cards, access badges, and a passport all answer scanners. Move the ones you do not need out of your pockets, or into an RFID-blocking wallet.
4. Score: count the unknown devices and the broadcasting devices again, and put both in the After column, Home and RF row.

Task 9 · File the broker opt-outs

1. Free, and open to everyone: stop prescreened credit and insurance offers at `optoutprescreen.com`, or call 888-567-8688. Opting out online lasts 5 years; the mailed form makes it permanent.
2. Opt out at each of the big brokers: Acxiom `acxiom.com/optout`, LexisNexis `optout.lexisnexis.com`, Epsilon `legal.epsilon.com/dsr`, Experian `consumerprivacy.experian.com`, TransUnion `transunion.com/consumer-privacy`, and Cotality, formerly CoreLogic, `cotality.com`, where most people can only remove a little.
3. For junk mail, register at `dmachoice.org/register.php`. It costs 8 dollars and lasts 10 years.
4. Write down each opt-out and its date in the cadence log. For a longer list of brokers, see `github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List`.

Task 10 · Re-measure your fingerprint

1. Install a browser that resists fingerprinting. Brave covers everyday use; for the strongest result, use Mullvad Browser together with a VPN, so you share a fingerprint and a pool of IP addresses with many other users, a crowd to blend in with.
2. Leave the new browser at its defaults. Privacy extensions and custom settings make your fingerprint stand out again.
3. Run `coveryourtracks.eff.org` again in that browser. The exposure check in module Unit 2 shows the same rows changing.
4. Score: write the new bits in the Browser fingerprint row, After, and compare to your baseline.

Task 11 · Total the score and set the cadence

1. Add up the Baseline column and the After column, and write the difference.
2. Write your adversary summary in the box below. You pass if your fingerprint bits and your device count both went down.
3. Set a calendar reminder to redo the opt-outs and the fingerprint test every 3 to 4 months, and write the first re-check date in the cadence log.

Task 12 · Adversary summary and field notes

In three sentences, describe yourself the way an adversary would: what they can still get on you, how they would get it, and which threat from your Module 00 threat model it lines up with. As the mailed and emailed reports come in over the next couple of weeks, log them here.

Exposure scorecard

Fill in Baseline during Phase 1 and After during Phase 2. Lower is better. You pass when your fingerprint bits and your device count both drop, and the total comes down.

Vector	What you count	Baseline	After
Data held	Data categories that surprised you		
Identity brokers	Old addresses, relatives, or contacts you never gave them, plus years of carrier history		
Home and RF	Devices you cannot name, plus devices broadcasting, plus always-on mics and cameras		
Browser fingerprint	Bits of identifying information from Cover Your Tracks		
TOTAL	Add up the four rows above		
DELTA	Baseline total minus After total (write it in the After box)		

#	Task	Where / Tool	Standard (done =)	Date	Finding
1	Platform data	Google / Apple / Meta	3 archives requested and opened		
2	Credit + broker files	annualcreditreport / LexisNexis / Acxiom	3 reports pulled; broker files requested		
3	Carrier record (CPNI)	carrier privacy portal	Access request filed		
4	Network audit + map check	router + maclookup.app + wigle.net	Unknowns identified; BSSID checked		
5	RF broadcast scan	nRF Connect / LightBlue	Broadcasting devices counted		
6	Mic/camera + tracker census	spec sheets; OS dashboard; Find My / Android	Total counted; tracker scan run		
7	Fingerprint (baseline)	coveryourtracks.eff.org	Bits recorded as baseline		
8	Harden device + accounts	module Units 3 to 5	Hardening actions completed		
9	Broker opt-outs	optoutprescreen + 6 brokers + DMAchoice	Opt-outs filed and dated		
10	Fingerprint (after)	new browser + coveryourtracks	After reading recorded and compared		
11	Score, summary, cadence	scorecard + threat model	Delta computed; summary written; re-check set		

Removal cadence log

Opt-outs do not stick: brokers pull your info back in from public records, so this is an ongoing job, not a one-time fix. Run the list again every 3 to 4 months and log each pass here.

Broker / list	Opted out (date)	Re-check due	Re-checked (date)	Still listed? (Y/N)