praetorian

Fortune 500 Red Team Initial Access

Why not just ask for it?

Obligatory whoami

- AJ Hammond, PNPT, CRTO, OSCP, BSCP
- Senior Offensive Security Engineer, Red Team @ praetorian
- B.S. Computer Science, University of Mount Union, 2022
- Golf, fly fishing, esports, Magic: The Gathering, not seeing Star Wars, racing
- Twitter: @4JMAN
- GitHub: @ajm4n
- LinkedIn: /in/aj-hammond/
- Signal: @ajman.54

Agenda

- Effective OSINT
- Effective Pretexting
- Psychology of Vishing
- Case studies / war stories
- Mitigation strategies
- Questions

Effective OSINT

- Identify Targets
  - B2B Sales Platforms (LinkedIn Sales Nav, Apollo, Ludus, etc.)
  - Company websites (leadership bios, press releases, staff directories)
  - Google dorking (site:company.com “contact” OR “team” OR “tel”)
- Intention is to find as many relevant phone numbers and job titles as possible

- Target Selection
  - Find targets that match your ruse
    - If you’re going to be impersonating an IT Helpdesk operator, don’t choose others in IT
    - If you’re going to be impersonating an executive, don’t choose direct reports
  - Find “low hanging fruit” targets
    - New hires
    - Interns
    - Non-technical folks
- Keep it simple. Develop a wide-spanning target list, including a variety of departments and job titles.

Effective ORGINT

- Identify Technologies
  - Glassdoor (Internal lingo, departments, complaints)
  - Job postings (relevant tools, vendors, internal systems)
  - Shodan (RDP ports, VPNs)
- Overall, you're trying to understand the company's structure and tech stack
  - This can aid heavily in your ruse development – ex. If organization is using Cisco VPN

- Target Selection
  - Disperse targets where possible
    - Different departments, different offices, etc
    - Receptionists and salespeople are usually eager to assist, and frequently answer "random" phone calls from unknown parties

Every call doesn’t need to net a shell!

- It’s important for operators to realize that not every ‘successful’ call has to end in access
- More times than not, your initial calls will be entirely fact finding
- Any information that is new should be considered a win.

- Real world example: Fortune 50 company
  - Target had browsed to our payload delivery mechanism but could not download our .zip compressed payload
  - ”I try to download but it’s saying Bluecoat could not verify this file and has blocked the download”
    - We didn’t know about that, so we didn’t factor that into ruse development
    - Back to the drawing board…

Effective Pretexting

- **Credibility**
  - Aligns with the target's environment (job role, org structure, tech stack)
  - Uses realistic tone, terminology, and urgency levels
- **Specificity**
  - Leverages names, systems, or details acquired via OSINT *(e.g., "I see you're on the sales team under [boss's name]…")*
- **Plausibility**
  - Has a logical reason to exist (e.g., IT check, finance follow-up, vendor renewal)
  - Avoids overly dramatic or inconsistent scenarios
- **Authority or Familiarity**
  - Implies power *(e.g., "Security Team," "CFO Office")*
  - Implies closeness or insider connection *(e.g., "from onboarding," "from Compliance")*
- **Urgency Without Alarm**
  - Adds time pressure *(e.g., "We're finalizing access changes now…")*
  - Encourages fast action without inducing panic

Effective Pretexting

- For simplicity's sake, let's use the IT Helpdesk ruse, and explore how we can use this to achieve different goals
- You are posing as an internal IT Helpdesk operator, with the goal of gaining some form of initial access
  - Dropping and detonating a payload to receive a command-and-control beacon
  - Targeting CI/CD solutions to achieve pipeline compromise
  - Targeting cloud personal access tokens to achieve a cloud-based foothold
- What technologies does the target organization utilize?
  - GitHub vs GitLab
  - Google Cloud vs Azure vs AWS (or all three)
  - Entra ID vs Okta
  - Cisco AnyConnect vs Palo Alto GlobalProtect

Effective Pretexting

- **Azure Device Trust Enrollment**
  - *Scenario*: “We’re updating compliance baselines — your device needs to re-enroll using a secure device code. I’ll read you a code to enter at microsoft.com/devicelogin.”
  - *Target*: **Azure / Entra ID**
  - *Objective*: Capture PRT via Device Code to establish Entra ID foothold
- **GitHub Key Mismatch**
  - *Scenario*: “We’re seeing token sync issues for your GitHub or GitLab account — I need you to generate a new personal access token and paste it here to rebind to your SSO identity.”
  - *Target*: **GitHub / GitLab**
  - *Objective*: Harvest PAT for repo access or pipeline insertion
- **New VPN Profile Rollout**
  - *Scenario*: “IT is rolling out a new VPN profile for better load distribution. Let me walk you through importing the config into GlobalProtect — it’s quick.”
  - *Target*: **Palo Alto GlobalProtect / Cisco AnyConnect VPN**
  - *Objective*: Drop malicious VPN config or implant for C2 channel

Dos

- **Use natural, conversational tone**
  Mirror the target's communication style; stay confident but not robotic.
- **Build rapport subtly**
  Use small talk or internal lingo to avoid skepticism.
- **Embed your ask in a process**
  Make requests sound like a step in a known or expected workflow.
- **Adjust in real time**
  Adapt your pretext based on responses or resistance cues. Confirm on success or redirect on failure.

Don'ts

- **Don't rush the target**
  Pressure without context raises suspicion. Urgency should feel procedural.
- **Don't overuse jargon or act too technical**
  Sounds suspicious or fake. Match the target's level of expertise.
- **Don't give too much detail too fast**
  Overexplaining sounds rehearsed and inauthentic.
- **Don't demand sensitive info directly**
  Guide the target to offer it as part of a "normal" task.
- **Don't break character**
  Stay in role even if challenged or redirected. Every reaction is data.

The Psychology of Vishing: Professional Lying

- Saying something like *“I’m looking at a ticket you put in — your Lenovo laptop with serial number [random numbers]…”* creates an illusion of insider access.
- Even though the detail isn’t correct or real, it triggers:
  - *Cognitive confirmation*: The target tries to remember the ticket or assume it’s real.
  - *Anchoring bias*: Specifics (like a 10-character serial) sound official and are rarely challenged.
- Most of the time, their computers are running slow anyway - and who doesn’t love a call from IT saying you’re going to have a faster/fixed computer?
- If they don’t have a ticket, say it was autogenerated, and pivot to the remainder of the pretext where feasible

The Psychology of Vishing: ”Is now a good time?”

- I always start my vishing calls with the following:

  “Hi [Target], it’s [Fake name] calling you from the [Organization] IT Helpdesk, am I catching you at a good time?”

- Using the target’s first name immediately signals **familiarity** and **directed communication**, which:
  - Grabs attention and **breaks autopilot thinking**
  - Makes the target feel **seen** and **accounted for**
  - Reduces defenses; it sounds like someone who knows them, even vaguely
  - *The Name Bias* - people are more likely to trust and respond when their name is used.

- Invoking an internal team like IT Helpdesk:
  - **Legitimizes the call** - most employees have interacted with IT before
  - Places the attacker in a **non-threatening but authoritative role**
  - Explains why the caller would have the target’s contact info
  - *Authority Bias* - people tend to comply with perceived authority figures, especially in structured organizations.

The Psychology of Vishing: ”Is now a good time?”

- **“...Is now a good time?”** soft question:
  - **Puts the target in control** - disarms suspicion by offering a choice
  - **Lowers resistance** - a manipulative politeness move
  - Encourages **mental reciprocity** - since you asked, they “owe” you their attention
  - *The Foot-in-the-Door Technique* - small agreements (like saying “yes” to continuing the call) make future compliance more likely.

  - What happens if they say no?

The Psychology of Vishing: The Callback

- When a target says "No, now isn't a good time," you're given a **low-resistance path to re-engage** - and it can often be even more effective than the initial cold call.
  - *Commitment/Consistency Bias* - People are more likely to comply if they've agreed to something small (a callback time).
  - *Trust Reinforcement* - You respected their schedule, which builds credibility.
  - *Lowered Defenses* - The second call is **expected**, so it bypasses the suspicion of an unsolicited first call.
- In my experience, I have **near-100% success** when callbacks are used.
  - By the time of the follow-up:
    - The target feels like **you're a known quantity** and has essentially "invited you in"
    - They're mentally **primed to be helpful**
    - Your request is **now seen as procedural**, not intrusive
- Even targets who were skeptical at first tend to **comply on the second interaction** because it feels scheduled, normal, and expected.

Case Study: Fortune 500 Banking

- Full scope red team
- Highly advanced SOC, IR, and Blue team
  - No Red Team has ever gotten a beacon to call back
- Objectives:
  - Get in, somehow. We opted to deliver a payload we were _sure_ would get past [EDR Vendor who must not be named] (they hate me)
- Pretext: IT Helpdesk – Device Synchronization

  ”Hi there [target]! I’m Matt from the [organization] IT Helpdesk. I’m looking at a ticket here that says you’ve been experiencing some laptop issues?”
- Target had a ticket in already for printer issues… go figure!
- “Great, yeah, this will also fix that problem, do you have a few moments to walk through this with me? This won’t take more than five minutes – what happened was your workstation has fallen out of sync with Active Directory, and IT has been internally working on a solution that we’re rolling out.”

Case Study: Fortune 500 Banking

- Walked them through browsing to the payload delivery website…
  - The payload wouldn't even download.
  - "Bluecoat has blocked this download and I don't have the permission to scan it"
- Pivot time! "Okay, no problem. Can we try one more thing, and if that doesn't work, I'll have to give you a call back tomorrow around the same time?"
- Generated a Microsoft Azure device code, instructed them to enter it at Microsoft.com/devicelogin
  - Of course, this didn't work. It was blocked at the org level.
- "Okay – let me call you back tomorrow, same time?"
- Had to regroup internally to see what was going on, and cook up some potential bypasses

Case Study: Fortune 500 Banking

- The solution? HTTP Smuggling
- Instead of downloading the data through the browser, let’s just stream it to their device
- Called back, instructed target through navigating to the ”Secure Download Portal” utilizing HTTP Smuggling
- Worked like a charm!

Case Study: Fortune 500 Medical

- Full scope red team
- Highly advanced SOC, IR, and Blue team
- Objectives: Get in
- Device Code SMShing had netted us Entra ID data
  - Names
  - Phone numbers
  - Departments
  - **Serial numbers**
  - **Entra group memberships**
- We were triaged and evicted from Entra ID shortly after RoadRecon did its thing and grabbed data
- Let’s at least put that data to good use…

Case Study: Fortune 500 Medical

- “Hey there, this is Matt from the [organization] IT Helpdesk, is now a good time?”
- ”I’m calling regarding this ticket for your Lenovo laptop with serial number [actual serial number]
- User looked under her laptop, verified that it was indeed their serial number
- I could have told her to throw their laptop out the window and they would have. That’s all it took.
- Installed a C2 implant on their machine
- It died, I called them back when it died to re-run the implant, and they did
- Called them back to get another Entra PRT, received another Entra PRT

Remediation and Prevention Strategies

- **Ban ad hoc credential sharing over the phone**
  - Formalize that IT will never ask for credentials, MFA codes, or device enrollment via phone without a ticketed process.
- **Teach soft-skill red flags**

  Train users to spot:
  - Urgency with no paper trail
  - Name-dropping without clear context
  - Inconsistent or evasive explanations
- **Reinforce "Verify, then comply" culture**
  - Normalize the behavior of politely rejecting or verifying suspicious requests - even from seemingly internal sources.
- **Limit phone-based auth where possible**
  - Favor app-based MFA with device binding as opposed to SMS-based MFA

Remediation and Prevention Strategies

- **Enable anomaly detection tools**
  - Use UEBA (User and Entity Behavior Analytics) to flag unusual logins, token use, or cloud access.
- **Establish an escalation path for suspected social engineering**
  - Employees must know *how and where* to report suspicious calls immediately.
- **Record and analyze patterns**
  - Track recurring pretexts or impersonation patterns to strengthen detection rules and training content.
- Add a **mandatory internal IT Helpdesk greeting** that includes a verification code or callback number.
- Use **caller ID masking** rules to flag unknown internal-looking numbers.
- Tag all internal phone calls in UC platforms (like Zoom, Teams) with a visual “internal verified” indicator if possible.

praetorian

Questions?

Thank you for coming!

x.com/praetorianlabs

facebook.com/praetorianlabs

linkedin.com/company/praetorian

youtube.com/user/praetorianlabs

github.com/praetorian-inc