RECONNAISSANCE

Jarrett Lane

WHAT IS RECONNAISSANCE?

- Reconnaissance is the beginning phase of an attack, pentest, or CTF challenge where information is gathered about a target
- The more you know about the target, you will be able to come up with more attacks and find more possible vulnerabilities
- You can also even find possible defenses, so you know what you need to evade and how to go about the attack
- This isn't just for hacking; this can be for any type of coordinated action against a target

TYPES OF RECONNAISSANCE

- Active
  - Gather information by interacting with the target
  - Risky but more effective
  - Non-technical: Social engineering in order to get more info
  - Technical: Port scanning, sending requests that trigger informative responses, enumerating known services, etc.
- Passive
  - Gather information without directly interacting with the target
  - Stealthier but less effective
  - Non-technical: OSINT, research
  - Technical: Network monitoring, web scraping, basic DNS/IP information

WHAT DO ATTACKERS WANT TO KNOW

- It depends on what their goal is
- If they want to go for more social engineering, they care more about data like employee names, partners/suppliers, personal details about employees, etc. This can help them do something like create a believable phishing email
- If they are more interested in hacking, they want to know which services are used in a company's infrastructure, which protocols can they interact with, which operating system is being used, which version of a particular service or asset is something, what protections are in place, etc. This can help them find vulnerabilities and plan out how to go about the attack

HOW DO ATTACKERS GET THIS INFORMATION

- Attackers have many tools and strategies for preforming reconnaissance
- Some methods are manual while others are automatic
- Doing something manually or automatically has pros and cons to each, it's best to keep a balance of both
- Attackers use multiple methods; they don't rust rely one thing
- I will mention common tools and methods for enumeration, just remember these are common approaches not all, and also these methods are also used together a lot

OSINT

- Open-Source Intelligence is the process of finding any publicly available information about something
- You would be surprised at how much information is out there
- This can be highly effective in something like phishing or social engineering
- On the technical side, this can lead to supply chain attacks or watering hole attacks
- Always be careful saying too much on social media, especially if you work at a private company that deals with very important projects
- OSINT can be directed at a company, individual (ex: CEO), group, and much more

RESEARCH

- This kind of goes off of OSINT
- Once you have some starting information, research and go deeper on it (pause)
- You found out the CEO of the company? Great, what can you gather about him?
- This is important on the technical side too: You found an open port on one of their servers? Great, how can you exploit the service on that port, what version is it, etc.
- It is important to go deeper on what is relevant
- Maybe you will need to learn something new in order to get a better understanding of the data you found, research into it

SOCIAL ENGINEERING

- Not all social engineering is about tricking people into clicking things
- "What are further ways to contact you?" "Need IT help, tell us your operating system."
- Think twice before sharing certain information that may seem harmless, even your birthday can (and will) be used against you (maybe to see if that’s your password)
- In general, don't share more information than is necessary, even if the person isn't malicious, ask yourself "Is there a good reason for them to know this?" or "Could saying this be risky?"
- Social engineering is everywhere and takes many forms, and attackers commonly extract information from the unsuspecting

SCANNERS

- Scanners are a way to gather information about an infrastructure or a running service
- Scanners can be tuned to look for many different types of things
- With networks, scanners look for open connections, running services, set configurations, reachable devices, and more
- With apps, scanners look for common vulnerabilities, strange behavior, outdated software, configurations, and more
- There are many open-source scanners available, such as NMAP
- There are also premade scanners and scripts that can be found on github, some of these can get pretty niche
- If you are good at coding/scripting, you can make your own scanner

AI

- It sounds obvious but AI is used in enumeration all the time, especially in things like OSINT
- Anyone can go online to a chatbot right now and ask "Tell me everything you can find about this company"
- AI may not always be accurate but for the most part it does a scary good job
- AI can also help an attacker develop a plan based off of information gathered from the enumeration stage
- There are people out there who know how to write very detailed and specific queries to get AI to run in a specific way

WEB SCRAPERS

- Web scrapers are scripts that parse web data in order to extract specific information
- An example is parsing a company's linkedin page to extract every unique employee name found, or all forms of contact information on that page
- Some web scrapers are made to constantly run and gather as much data from the web as possible
- These are automatic, which are good for quickly getting information, but may lack important context and details that can be useful

DNS ANALYSIS

- A domain is a hierarchical name that identifies a realm of administrative control or ownership on the internet (ex: floridapoly.edu)
- DNS (Domain name service) translates names and IP addresses, ex: example.com ==> 1.2.3.4 or 1.2.3.4 ==> example.com
- Not just for websites, can be any network device
- DNS records can tell more than just address translations, they give information about mail services, and general information about the domain overall
- Find accessible IPs, devices, host names, services, subdomains, etc.
- This can tell you a lot about the infrastructure of an organization

DNS RECORDS QUICK OVERVIEW

- A: What is the IPv4 address of this name
- AAAA: What is the IPv6 address of this name
- CNAME: A nickname for another domain name
- MX: Which mail servers get mail for this domain
- NS: Which name server actually holds records for a domain (not just in a cache)
- PTR: Opposite of DNS, IP addresses translate to names
- SOA: Administrative info about a DNS zone
- SRV: Location of servers that run specific services (includes protocol, port number, and host name)
- TXT: Random and arbitrary notes/information, can be used with SPF & DKIM

ERROR MESSAGES

- Sometimes, error messages can tell us a lot
- With specific services, you can purposely send bad input, and the resulting error message will tell you a lot about the application
- This can expose lots of data, and an attacker can further find out more based off of the error
- This also can expose configurations, software versions/dependencies, other running services, and so much more
- In SQLi vulnerabilities, error messages are extremely valuable
- Never overlook these

BRUTE FORCE/FUZZ

- Remember: brute force looks for valid input, fuzzing looks for unexpected responses
- Brute forcing can reveal things like valid subdomains, open ports, passwords, etc.
- Fuzzing can reveal things like error messages, valid subdomains, weird application behavior, etc.
- This can be very effective but it is also very noisy
- There are many tools for this, or you can script one

ENUMERATION ISN'T A ONE-TIME THING

- If you break into a system, now you need to find out MORE
- Lateral movement is when an attacker breaks in, but wants to move throughout the network
- When an attacker is in, they need to find out more information about the system in order to shape their next steps
- When an attacker is in a system, they may try to enumerate the mapping of a network, network hierarchies, naming conventions, operating systems, and general important information
- Privilege escalation is another goal of an attacker, once they are in, they want more power to actually do things
- Once in a system, an attacker wants to know more about the computer so they can find a vector for privilege escalation

HOW TO USE THIS INFORMATION

- Always remember the context of the information you find
- Sort through the data and expand upon what sticks out
- Don't just use one strategy, enumeration is a multilayered process, for example find the contact for an organizations IT department by web scraping, then socially engineer the department to get more information
- Think of different paths that can be taken when analyzing the data
- Research even more on the data you find
- Parse the data in order to effectively sort through it

LAB

- https://example.com/
- Tell me everything you can find about this domain
- Do both active and passive reconnaissance
- At the end tell me everything you found
- DO NOT DO ANY TYPE OF ATTACK

REFERENCES

- https://abdelmlaksaid.medium.com/passive-vs-active-reconnaissance-in-ethical-hacking-b5fe1ffc8bb2
- https://www.recordedfuture.com/threat-intelligence-101/tools-and-techniques/dns-enumeration
- https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/lateral-movement/