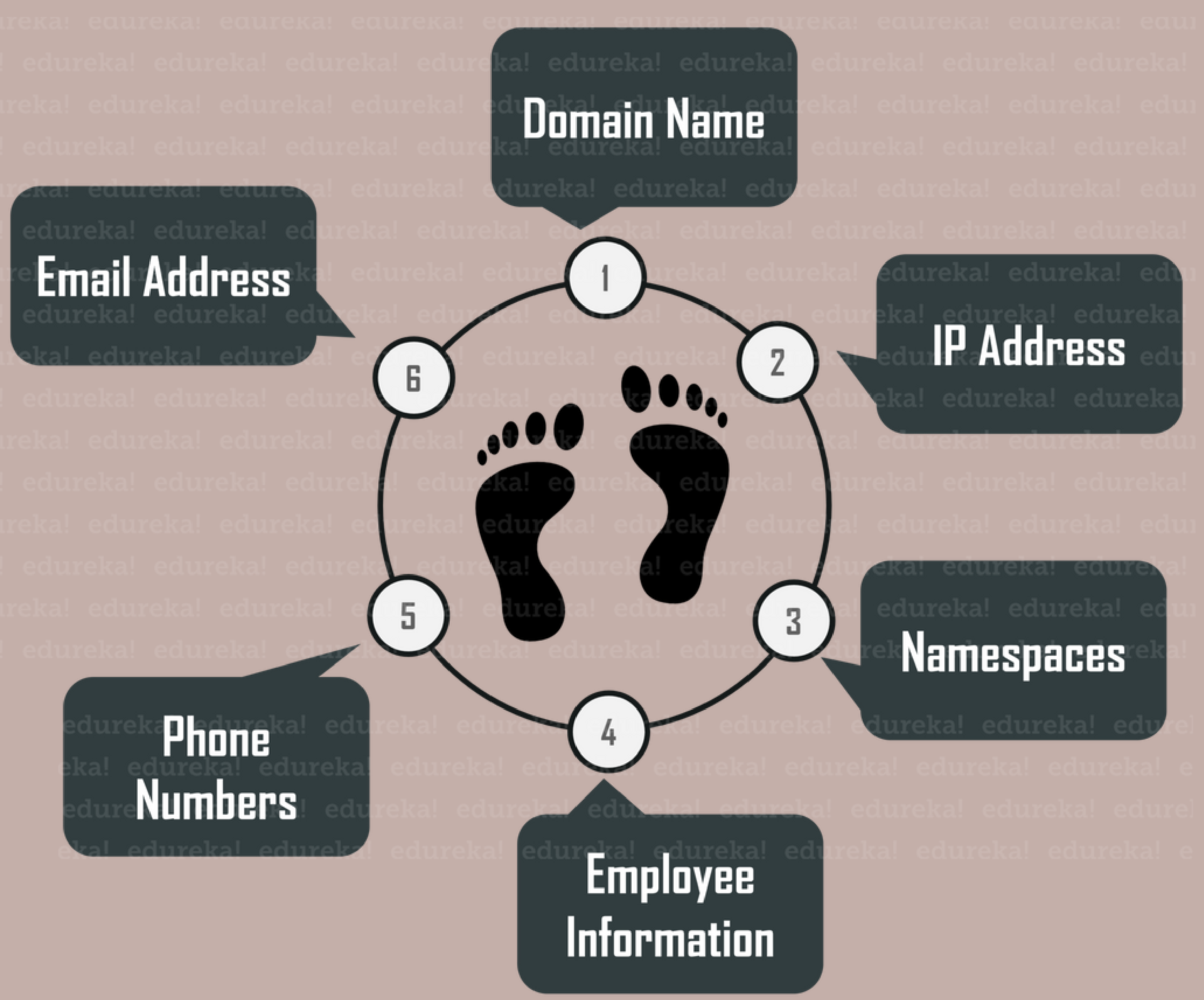
FOOTPRINTING

Footprinting is one of the most convenient ways for hackers to collect information about targets such as computer systems, devices, and networks. Using this method, hackers can unravel information on open ports of the target system, services running, and remote access probabilities. Footprintinh is the first step during which a hacker gather as much information as possible to find ways to enter a target system. For successful footprinting, the attacker needs to first check the visibility of the target and see how to gather related information on the internet through open sources. Through careful analysis, the attacker cermine the scope of potential entry points. The following information can be collected:

- Company name
- Domain names
- Business subsidiaries
- IP Addresses
- Business emails
- Network phone numbers
- Key employees

and so on.

How to perform footprinting?



The first step of footprinting is to determine what to attack to obtain the "footprint" of the target network which includes, but is not limited to the following:

- Hostnames
- Network address ranges
- Exposed hosts
- Exposed applications
- OS and its versions
- Application and its versions

and many more.

Apart from this, the attackers have to decide the scope of the target with regards to the entire organization or certain subsidiaries or locations. Based on the scope, they start to dig deep into the information like company web-pages, related organizations, employee details, contacts, e-mail addresses, currents events, locations, news, policies, disgruntled employees, mergers, acquisitions, or events to garner some clues, opportunities, and contacts for attackers.

FOOTPRINTING HELPS TO:

- **Know Security Posture – The data gathered will help us to get an overview of the security posture of the company such as details about the presence of a firewall, security configurations of applications etc.**
- **Reduce Attack Area – Can identify a specific range of systems and concentrate on particular targets only. This will greatly reduce the number of systems we are focussing on.**
- **Identify vulnerabilities – we can build an information database containing the vulnerabilities, threats, loopholes available in the system of the target organization.**
- **Draw Network map – helps to draw a network map of the networks in the target organization covering topology, trusted routers, presence of server and other information.**

OBJECTIVE OF FOOTPRINTING

- Network Footprinting: This is the process of collecting information related to a target network. Information like Domain name, subdomains, network blocks, IP addresses of reachable systems, IDSes running, Rouge websites/private websites, TCP & UDP services running, VPN points, networking protocols, ACL's, etc are collected.
- Collect System Information: The information related to the target system like user and group names, system banners, routing tables, SNMP information, system names etc are collected using various methods.
- Collect Organization's information : The information related to employee details, organization website, Location details, security policies implemented, the background of the organization may serve as an important piece of information for compromising the security of the target using direct or social engineering attacks.