# Cyber Attack

# Cyber Attack

- Definition of Attack:
  - An action that violates a cyber pillar

- Three Basic Phases of an Attack:
  - Reconnaissance
    - Searching for the information to actually get in. (Firewall information, services, etc.)
  - Infiltration
    - Gain the access needed to achieve the goal
  - Exfiltrate & Maintain Access
    - Obtain the goal
    - Hide the evidence
    - Maintain access

# Cyber Attack

- Denial of Service Attack (DOS / DDOS)
  - Denying a system's availability vice infiltration
  - Usually carried out from the outside
  - Imagine overloading a service with 100's of thousands / millions of requests

# Cyber Attack

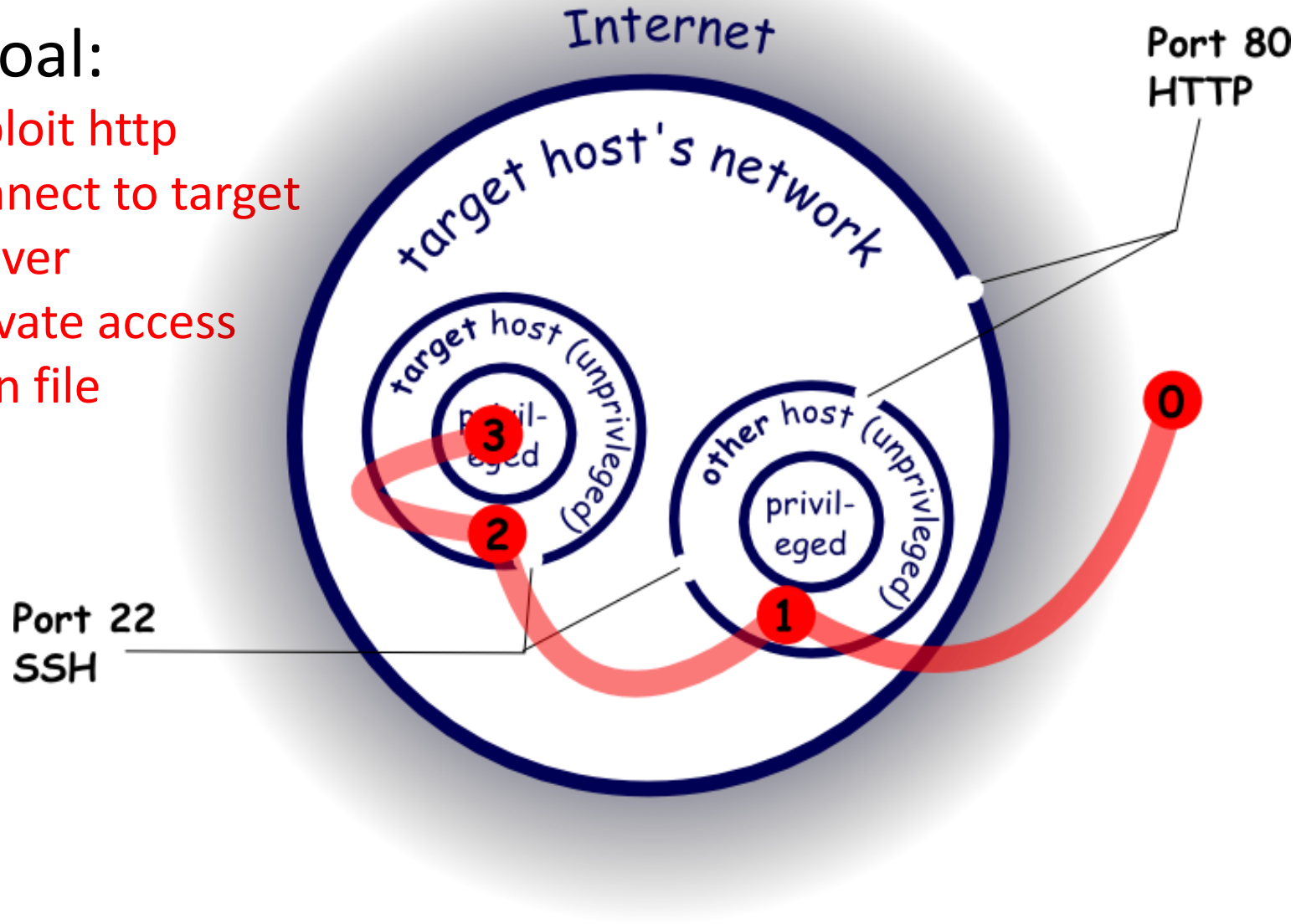
- Infiltration Phase
  - –Goal is to obtain access to systems, modify or obtain information, or perform follow-on actions.
  - –Requires a sequence of steps using knowledge obtained during recon phase.
    - Starting with open ports
    - Finding vulnerabilities in running services/software
    - Exploit vulnerabilities to gain access
    - Steal confidential information/manipulate data
    - Pivoting to attack other hosts on network

# Cyber Attack

- Imagine that our goal was to access a specific users file
  - File: secret.txt
  - User: bob
  - Server Layout:
    - A web server:
      - Port 80 – Open to the world
      - Port 22 – Open within the target network
    - Target Computer:
      - Port 22 – Open within the target network
- How do we proceed?

# Cyber Attack

- The goal:
  - ❑ 1. exploit http
  - ❑ 2. connect to target server
  - ❑ 3. Elevate access
  - ❑ Obtain file



# Cyber Attack

- But how do we do this.
  - For the webserver, we could have tried a buffer overflow attack
  - For the target machine, we may have had to guess a username / password
  - Once on the target machine, we needed to escalate privileges.

# Cyber Attack

- Remote code execution
  - We want our code (program) to run on their system.
  - Our goal is to get a shell on their box.
  - We have seen how hard it is to handle ill-formatted inputs, in fact this is a very common vector into a system.

# Cyber Attack

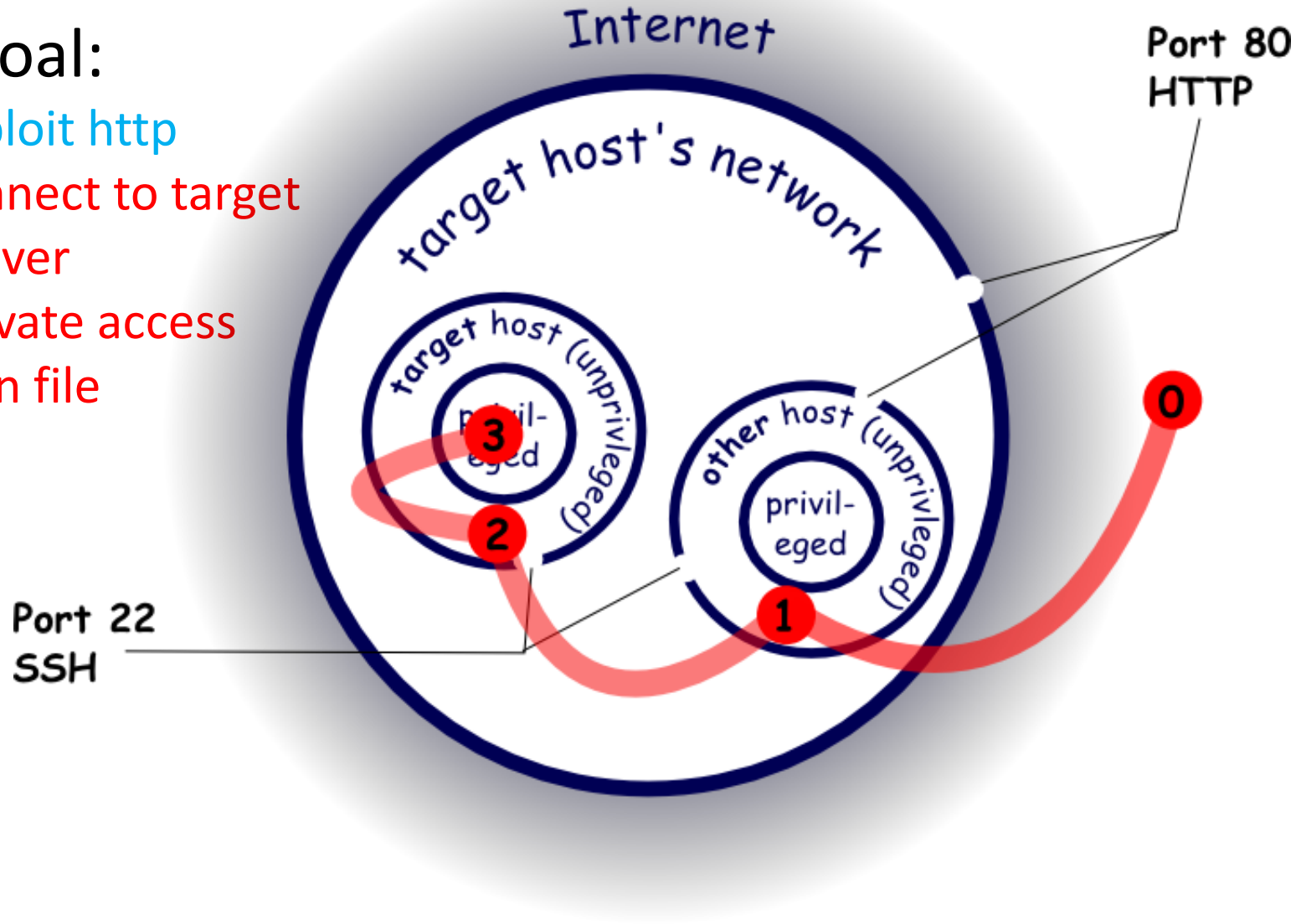
- Remote code execution
  - –Some bugs cause a crash or infinite loop
    - DOS Attack
  - –Some bugs allow you to send a piece of code, that then is executed on the system
    - **Remote code execution**
  - –In fact there is a web page just for Apache Web Server Vulnerabilities. (here)
  - –There is also a site that you can look up Common Vulnerabilities and Exposures for just about any software. (here)

# Cyber Attacks

- Buffer overflow example
  - –A common bug
  - –A program attempts to write the information received into a buffer (but the buffer isn't big enough) so it goes past it's own boundaries.
  - –Here is an example (demo)

# Cyber Attack

- The goal:
  - ✓ 1. exploit http
  - ❑ 2. connect to target server
  - ❑ 3. Elevate access
  - ❑ Obtain file

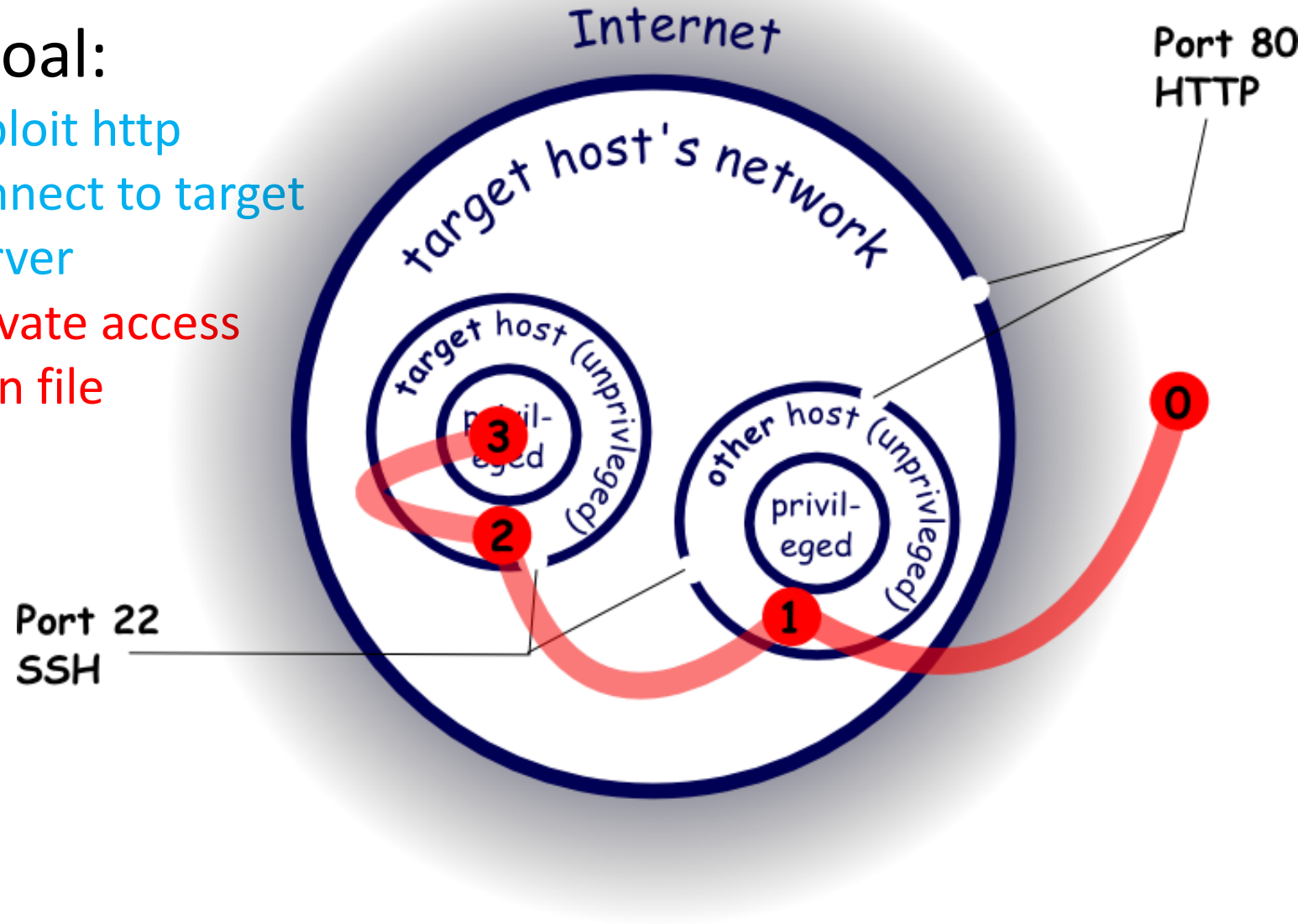


# Cyber Attack

- We now need a username/password!
- We have a few options:
  - Websites that host the information
  - Violence and Threats
  - Trickery (Phishing / misdirection)
  - Unchanged default passwords
  - Predictable Passwords
  - Passwords sent in the clear.

# Cyber Attack

- The goal:
  - ✓ 1. exploit http
  - ✓ 2. connect to target server
  - ❑ 3. Elevate access
  - ❑ Obtain file

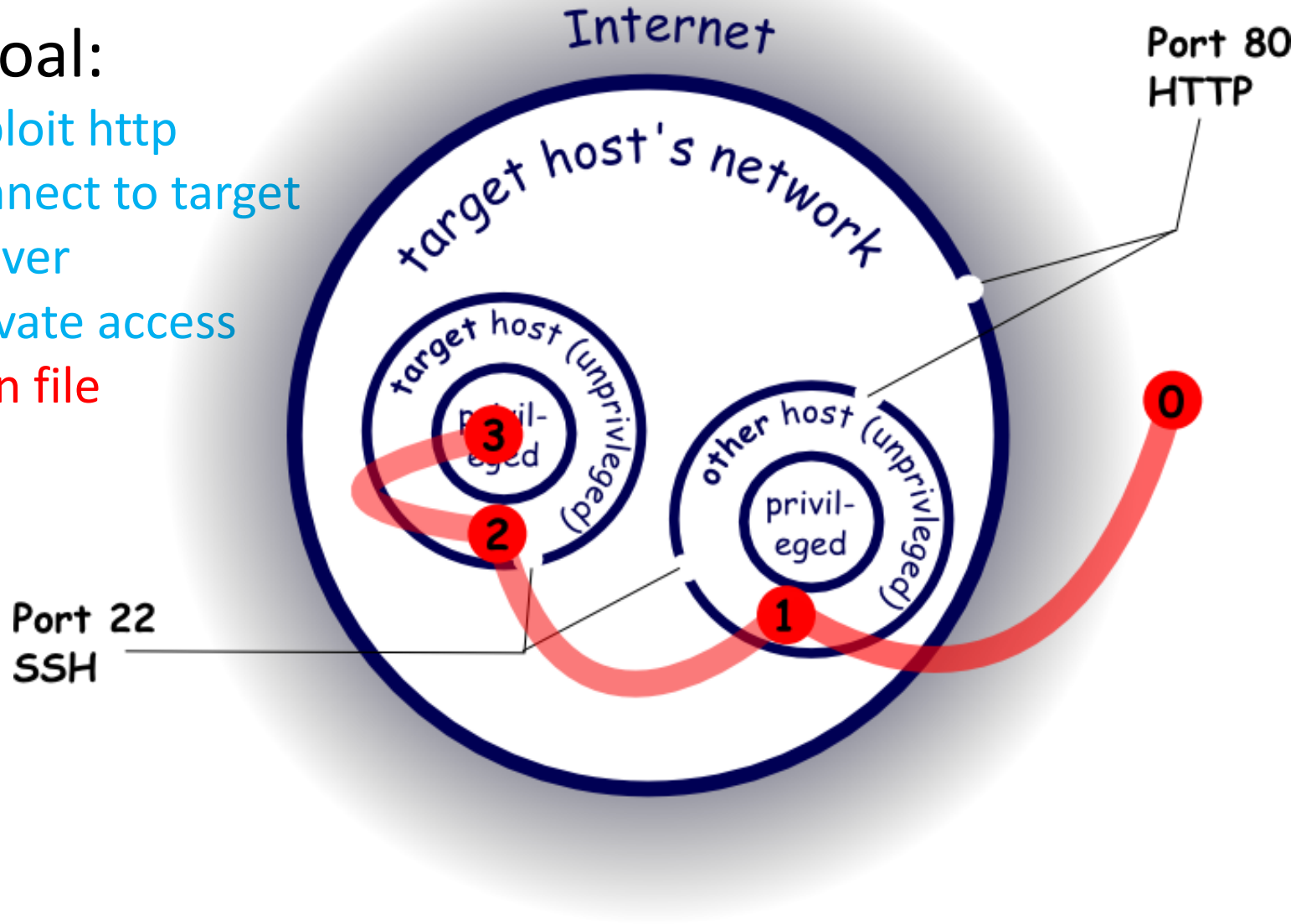


# Cyber Attack

- We now need to escalate our access within the target machine. (escalate privileges)
  - Need to become the target user or admin
  - Brute force attack the password file
  - Dictionary attack the password file
  - Rainbow table attack the password file
  - Try to hijack a running process.
    - Preferably a higher permission service.

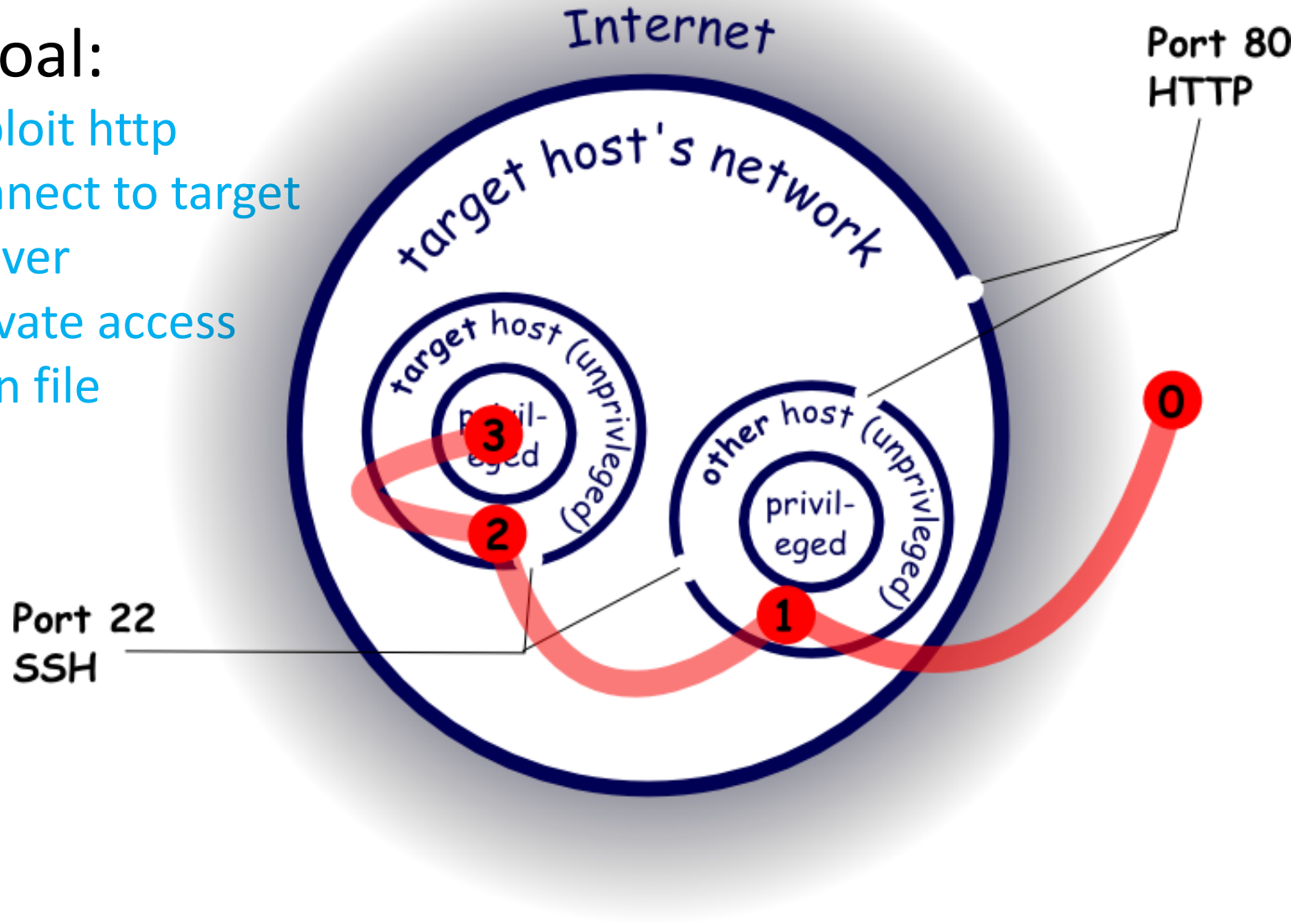
# Cyber Attack

- The goal:
  - ✓ 1. exploit http
  - ✓ 2. connect to target server
  - ✓ 3. Elevate access
  - ❑ Obtain file



# Cyber Attack

- The goal:
  - ✓ 1. exploit http
  - ✓ 2. connect to target server
  - ✓ 3. Elevate access
  - ✓ Obtain file



# Cyber Attack

- Summary:
  - The attack may need to hop from host to host to achieve the goal
  - We have to first find access within their network
  - Injection attacks – like what you have done to my message board are a vector
  - Default passwords – routers/switches often have default username/password combos.

# Wednesday – ATTACK!!!

- The plan will be for both teams to attack the other team during this lab.
- Team Leaders must review the lab instructions the night before