Core Services

Phillip Babey

Recap

- Linux
  - cat /etc/everything
- Windows
  - Computer\HKEY_LOCAL_MACHINE\oh_my_god_there_are_so_many_keys
- Networking
  - FIN? More like power machine broke
- What next?

What is a Service?

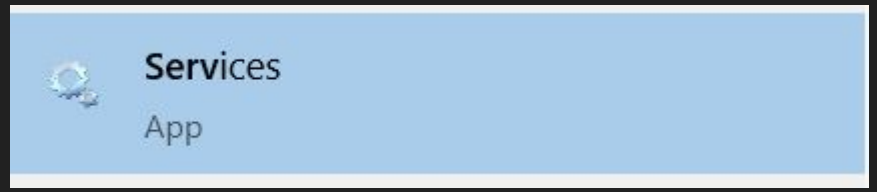
- In Linux when we refer to services (daemons), we are talking about a
  - Process
    - That runs independent of a logon
      - And *often* listens on a port
        - Like tcp/22
- In Windows Services are operate closely the same to unix services
- There usually can only be a single instance of a service

How Linux does the daemon

- Services are controlled by an init process
  - This is the first process started on system boot
    - All other processes are children of it
      - PID 1
  - Typically systemd unless your on alpine or some unknown fruit named
- Systemd syntax:
  - systemctl <verb> <service> [options]
    - Verbs:
      - start
      - stop
      - enable
      - disable
      - Status
    - systemctl --type=service

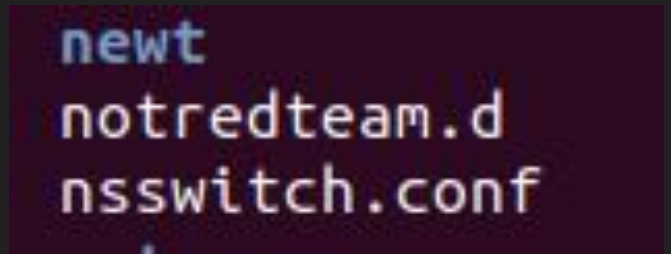
Windows?

- Similar to Linux, there is one service that rules them all
  - services.exe - The Service Control Manager (SCM)
- Every service reports to the SCM
  - Must also adhere to its standards
- “Enjoy ur GUI xD” - some linux nerds
  - You can interact with services through the command line
  - sc <option>
    - sc query <service name>
    - sc start <service name>
    - sc stop <service name>
    - sc qc <service name>
  - Or just use this ---------->



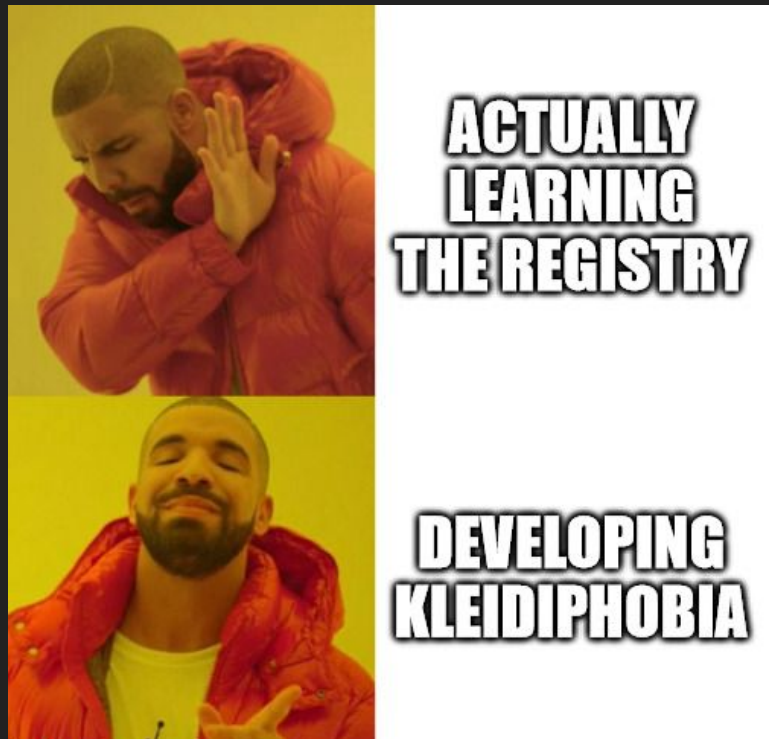
Linux Config Files

- You picked Linux because you want to have control over your system
  - This means you need to know where the configuration files are
- /etc/<service>/
  - 9/10 times this is where the configuration files are
  - The config file is usually called <service>.conf
  - Sometimes you will see a .d appended to the service name
    - This is to denote that it is a daemon
- Ex.
  - /etc/nginx/
  - /etc/sshd/
  - /etc/scoring.sh (totally not redteam @Choi)
  - Nor is this ----------->



Windows Config Files

- Registry
  - HKLM/SYSTEM/CurrentControlSet/Services
    - Contains a lot of service configuration options
- Services.msc
  - A lot easier to work with. Most of your service config changes should be done through here
  - Registry machine hard.

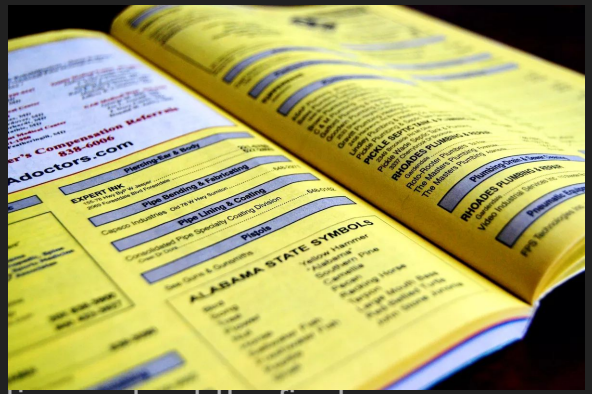


Core Services

- DNS
  - Domain Name Service
- SSH
  - Secure Shell
- FTP
  - File Transfer Protocol
- SMTP
  - Simple Mail Transfer Protocol
- RDP
  - Remote Desktop Protocol
- DHCP
  - Dynamic Host Configuration Protocol

- MYSQL
  - Database
- Other Databases
  - Mongo, Cassandra, Postgres
- Apache/nginx
  - Web
- Samba/SMB
  - Remote file shares
- *The T word*
  - Telnet
    - Just no

DNS: The Phonebook of the Internet

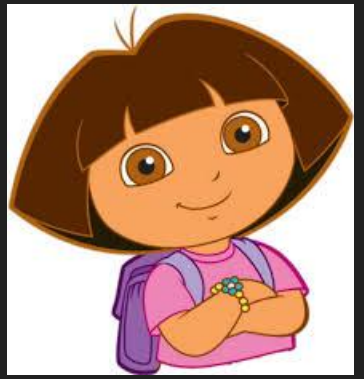


- DNS: Port 53/udp AND 53/tcp
  - Hierarchy of servers that resolve names into IP addresses
    - Can you remember grandma's phone number?
      - How about 192.64.119.183?
  - Recursive and iterative
    - Recursive servers will do all the work for you, ask a question and get the final answer
    - Iterative will tell you who the next person you should ask is
  - Many different types of records:
    - SOA - Start Of Authority (Which DNS server is authoritative for this domain)
    - A or AAAA - Alias (name -> IP)
    - MX - Mail (IP of domain's mail server)
    - CNAME - Canonical Name (name -> name)
    - …(there are several more, look them up)

SSH

- Get comfortable with the config files:
  - PermitRootLogin
    - Please don’t, or at least without-password
  - X11Forwarding
    - GUI over SSH…
  - Banner
    - Greeting message
  - AuthorizedKeysFile
    - Which keys are allowed to connect
  - PubKeyAuthentication
    - Can clients use public keys?

DHCP



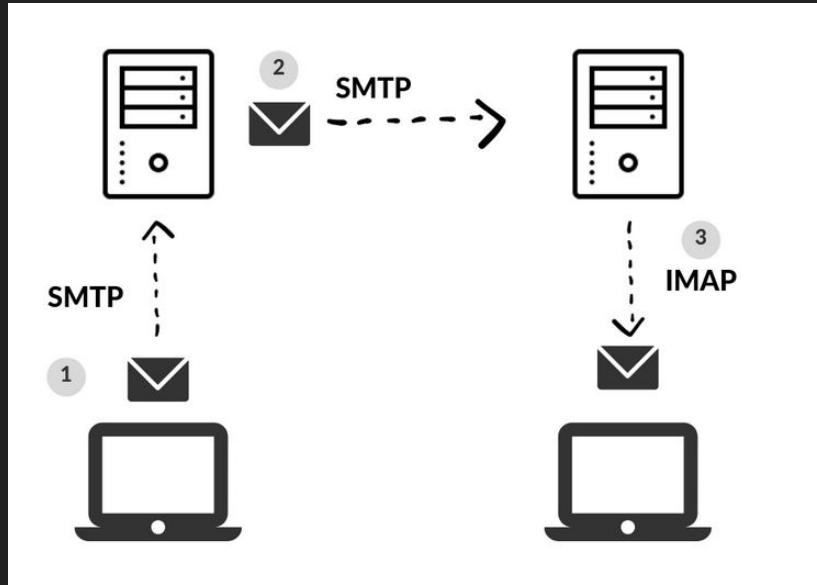
- Dynamic Host Configuration Protocol
- Assigns IP addresses to hosts on a network
  - Dynamically
- Can also send configurations such as DNS servers
- DORA process
  - Discover - Client sends a broadcast trying to find a server
  - Offer - Server issues an offer for an IP address in its pool
  - Request - The client requests that IP
  - Acknowledge - The server acknowledges, and includes more info like netmask and gateway
- Net services spends half a semester on DHCP
  - Other half is DNS

FTP

- Port 21/tcp
- By itself not secure
  - Everything is plaintext…
- You should really use SFTP
  - SSH + FTP
- Some common FTP misconfigurations
  - Anonymous login enabled
  - Chown on upload
    - Changes the owner when a file is uploaded
  - Chmod on upload
    - Change file permissions on upload
      - Like make it executable

Mail

- Simple Mail Transfer Protocol
- SMTP= 25/tcp
  - Used for **sending** emails
- Pop3 = 110/tcp
  - Used for **receiving** but from one client
  - A.k.a deletes your email after you store it locally
- Imap = 143/tcp
  - Used for **receiving** but from multiple clients
- Common Servers
  - postfix (SMTP) and dovecot for linux
  - MS Exchange for windows (pls no hmail_



VNC/X11/RDP

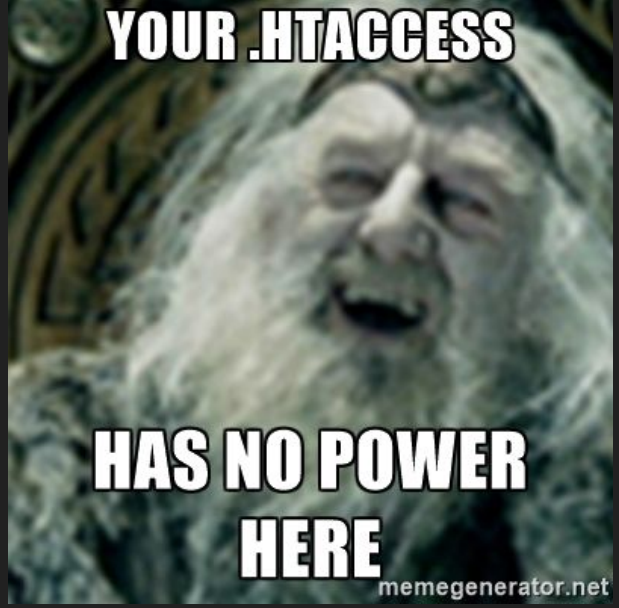
- Port 5900, 6000, 3389
- Remotely manage another computer using a desktop environment.
- VNC can be used without authentication.
- VNC: vncviewer <IP address>
- RDP can have weak passwords logins that are acceptable to a brute-force.
- RDP: rdesktop <IP address> (for linux)
- X11: ssh -X superadmin@192.168.1.1

Databases

- Two of the most popular (there are lots):
  - MySQL: 3306/tcp
  - MongoDB: 27017/tcp
- Poor configurations
  - Not sanitizing input
    - SQL injection
      - More on this during web week (#5)
  - Weak/default/no passwords

Web

- Ports: 80/tcp (HTTP) and 443/tcp (HTTPS)
- We have an entire week devoted to web!
  - Week 10: Come back in like a fe wmonths
  - Also a whole semester @csec380
- Common problems:
  - Unsanitized inputs
    - XSS, SQLi
  - Permissioning
    - .ht files
  - File uploads
    - Web shells
      - If webserver is running as root
        - You win
- IIS is cool (Windows), also apache and nginx (linux)



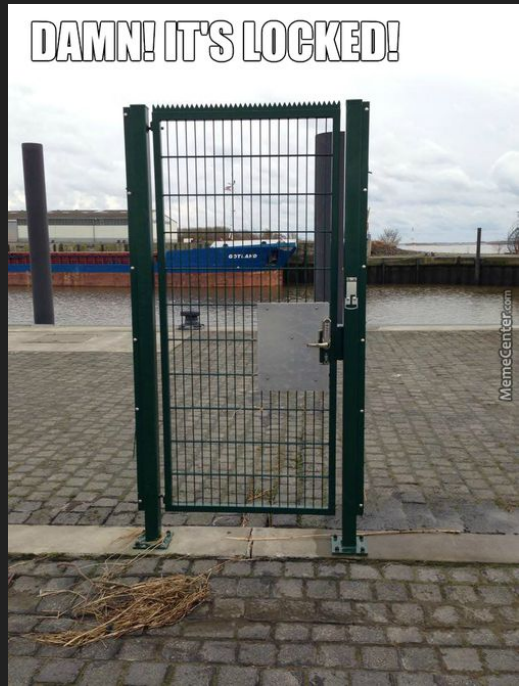
SMB

- Ports: 139,445,137,138
- Network shares for Linux and Windows.
- Samba and NFS by default do not require authentication.
- SMB shares require authentication but can be DISABLED.
  - Also: MS17-010 anyone?
- Open network shares can be use for data exfiltration.
- Samba:
  - mount -t cifs -o <username>,<password> //<remote directory> /<local directory>
- SMB:
  - smbclient -L <IP address> [-U <username>] [-P <password>]
- NFS:
  - mount <IP Address>:<remote directory> <local directory>

SMB2

Telnet

- Port 23/tcp
- How about no
- There is no encryption
  - All usernames and passwords sent in cleartext.
  - As seen in basically every class here
- Be aware networking devices may use it.
- Good for two things:
  - telnet towel.blinkenlights.nl
  - Sending email
    - Look this up



Detecting Services

- To take advantage of poor configurations, you need to know what is running
  - nmap -sV -Pn --top-ports <10-100> <target IP>
  - nmap -sV -p- <target IP>
- Use your favorite search engine to learn about the services you found
  - http://lmgtfy.com/?iie=1&q=mysql+metadata
- Once you have info on what's actually running then you can make a plan to exploit that, redteaming 101.