Cybersecurity

Password Attacks

Storing Passwords

- Passwords should never be stored in plaintext
  - Also known as unencrypted
- For example:
  - A plaintext/unencrypted password could be **p@ssw0rd1@3$5^**
  - Windows will hash this password and store it as:

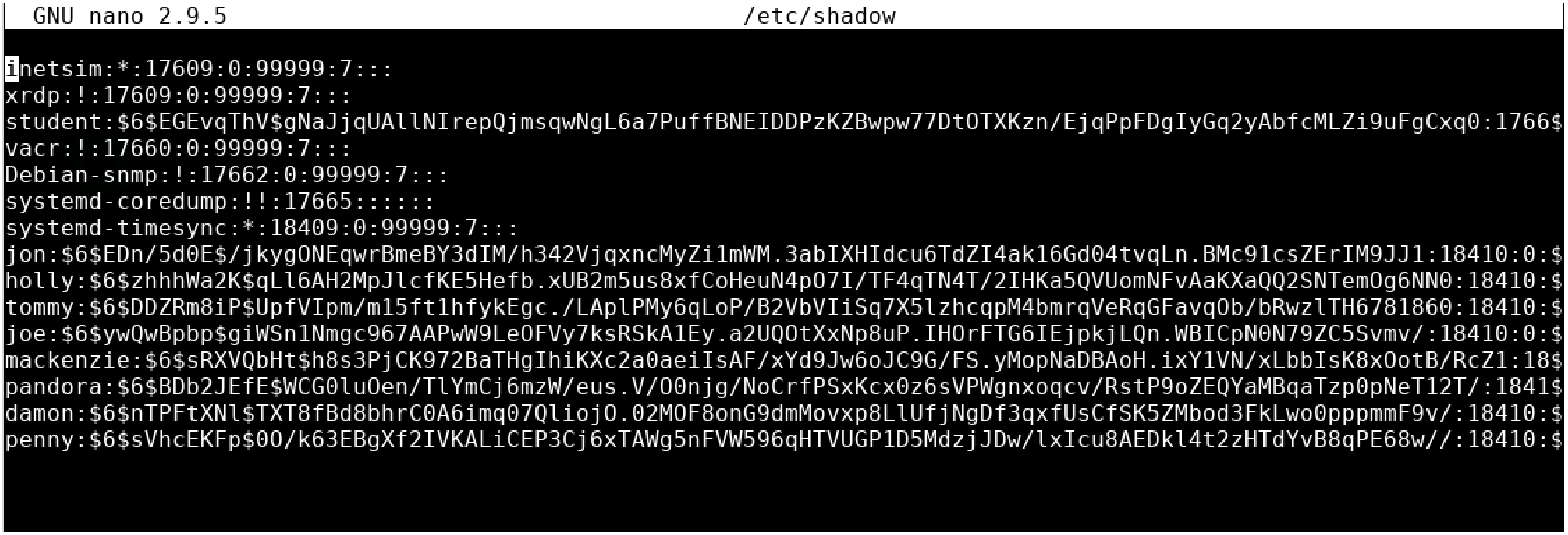
4578A81E395F749BBA1D41B320F8AFFA

  - Linux will hash this password and store it as:

**542F3706AF4A262E59A8161D7F4ED679E671E7A
B2CA5B49F08308651AC9E0822E544C30C072B60
FC204EAEAC118C7A875F90BBD2435CB9982D1F
93AFC2F54061**

The Password File

- Each OS stores passwords differently
  - Example: Linux /etc/shadow file



```
  GNU nano 2.9.5                                        /etc/shadow

inetsim:*:17609:0:99999:7:::
xrdp:!:17609:0:99999:7:::
student:$6$EGEvqThV$gNaJjqUAllNIrepQjmsqwNgL6a7PuffBNEIDDPzKZBwpw77DtOTXKzn/EjqPpFDgIyGq2yAbfcMLZi9uFgCxq0:1766$
vacr:!:17660:0:99999:7:::
Debian-snmp:!:17662:0:99999:7:::
systemd-coredump:!!:17665::::::
systemd-timesync:*:18409:0:99999:7:::
jon:$6$EDn/5d0E$/jkygONEqwrBmeBY3dIM/h342VjqxncMyZi1mWM.3abIXHIdcu6TdZI4ak16Gd04tvqLn.BMc91csZErIM9JJ1:18410:0:$
holly:$6$zhhhWa2K$qLl6AH2MpJlcfKE5Hefb.xUB2m5us8xfCoHeuN4pO7I/TF4qTN4T/2IHKa5QVUomNFvAaKXaQQ2SNTemOg6NN0:18410:$
tommy:$6$DDZRm8iP$UpfVIpm/m15ft1hfykEgc./LAplPMy6qLoP/B2VbVIiSq7X5lzhcqpM4bmrqVeRqGFavqOb/bRwzlTH6781860:18410:$
joe:$6$ywQwBpbp$giWSn1Nmgc967AAPwW9LeOFVy7ksRSkA1Ey.a2UQOtXxNp8uP.IHOrFTG6IEjpkjLQn.WBICpN0N79ZC5Svmv/:18410:0:$
mackenzie:$6$sRXVQbHt$h8s3PjCK972BaTHgIhiKXc2a0aeiIsAF/xYd9Jw6oJC9G/FS.yMopNaDBAoH.ixY1VN/xLbbIsK8xOotB/RcZ1:18$
pandora:$6$BDb2JEfE$WCG0luOen/TlYmCj6mzW/eus.V/O0njg/NoCrfPSxKcx0z6sVPWgnxoqcv/RstP9oZEQYaMBqaTzp0pNeT12T/:1841$
damon:$6$nTPFtXNl$TXT8fBd8bhrC0A6imq07QliojO.02MOF8onG9dmMovxp8LlUfjNgDf3qxfUsCfSK5ZMbod3FkLwo0pppmmF9v/:18410:$
penny:$6$sVhcEKFp$0O/k63EBgXf2IVKALiCEP3Cj6xTAWg5nFVW596qHTVUGP1D5MdzjJDw/lxIcu8AEDkl4t2zHTdYvB8qPE68w//:18410:$
```

Brute Force Attack

- Brute force = try all possible combinations and permutations until the right guess works
- Like trying to guess a number by sequentially trying
  every number starting at 0… 1… 2…
- Very slow
- Many systems will lock you out after X failed attempts
- Doing this offline will not lock you out
  - Requires password file with usernames and hashes

Dictionary Attacks

- Most passwords are comprised of common words
- If using brute force attack, try dictionary attack first. Be sure it isn't easy-to-guess like single word from dictionary
- Wordlists are available online
  - Made up of cracked/leaked password files from old cyberattacks
  - Each year, articles pop up of "Most common passwords of 20__."
- Only good against simplistic passwords
  - Every organization has *someone* that uses a weak password!

Spraying Attacks

- Attempting random passwords
- Very ineffective
- Malicious actor hoping to get lucky
- If they know the person likes Disney, they might try the following passwords:
  - MickeyMouse
  - DonaldDuck
  - Mickey123
  - M1nn1eM0use
  - B3ll3

Rainbow Tables

- Pre-calculated series of hashes using known hashing algorithms
- Commonly used for cracking passwords
  - Find the matching hash
  - Look up the input text that gave the result
  - Voila! There’s the password/input string
- Rainbow table built for each application
  - No one table for all uses

Defense

- Use strong passwords
  - Longer and more character types
- Limit number of incorrect attempts
- Protect the password hashes!
- Do not reuse old passwords
- Change passwords frequently