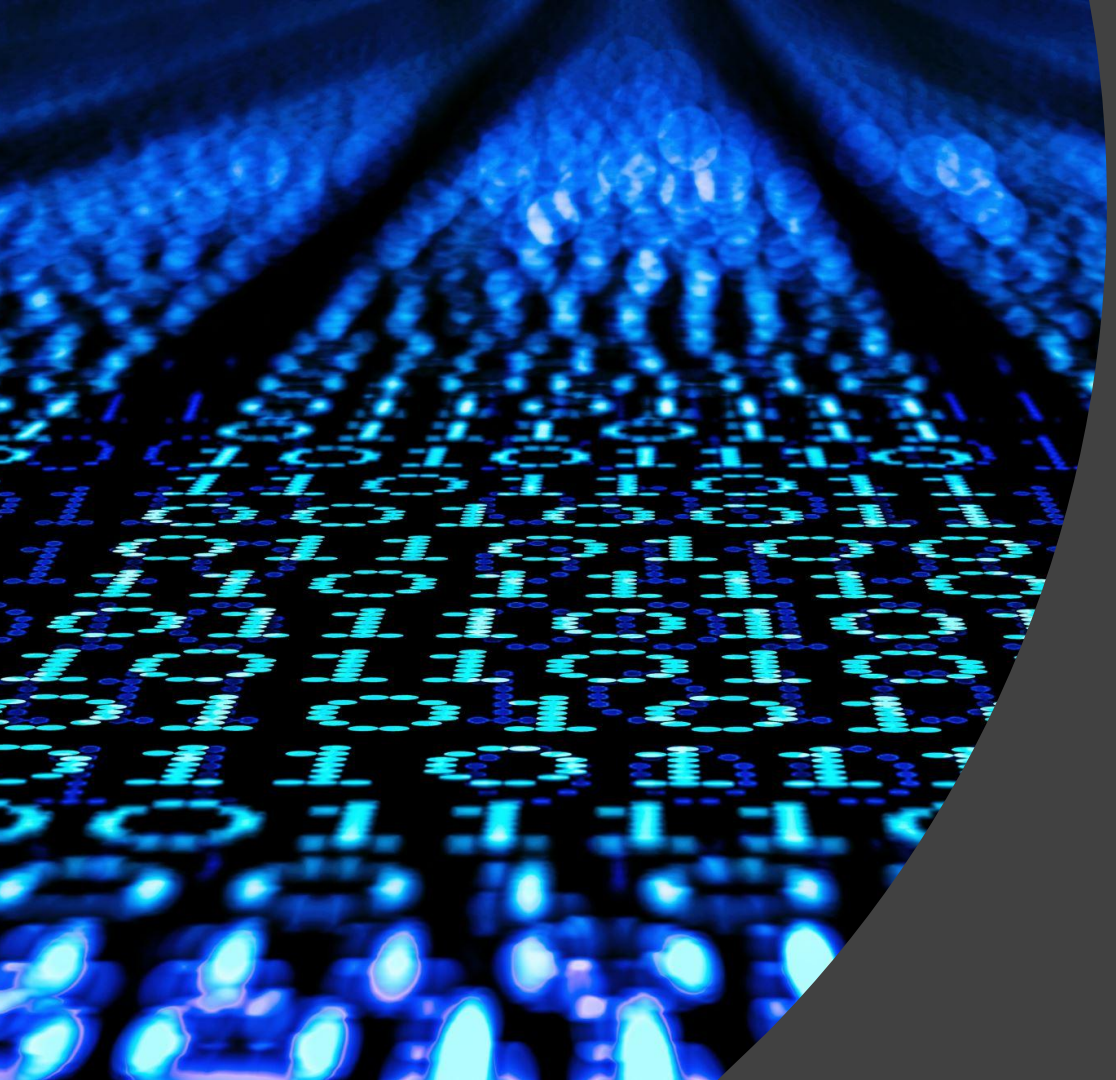
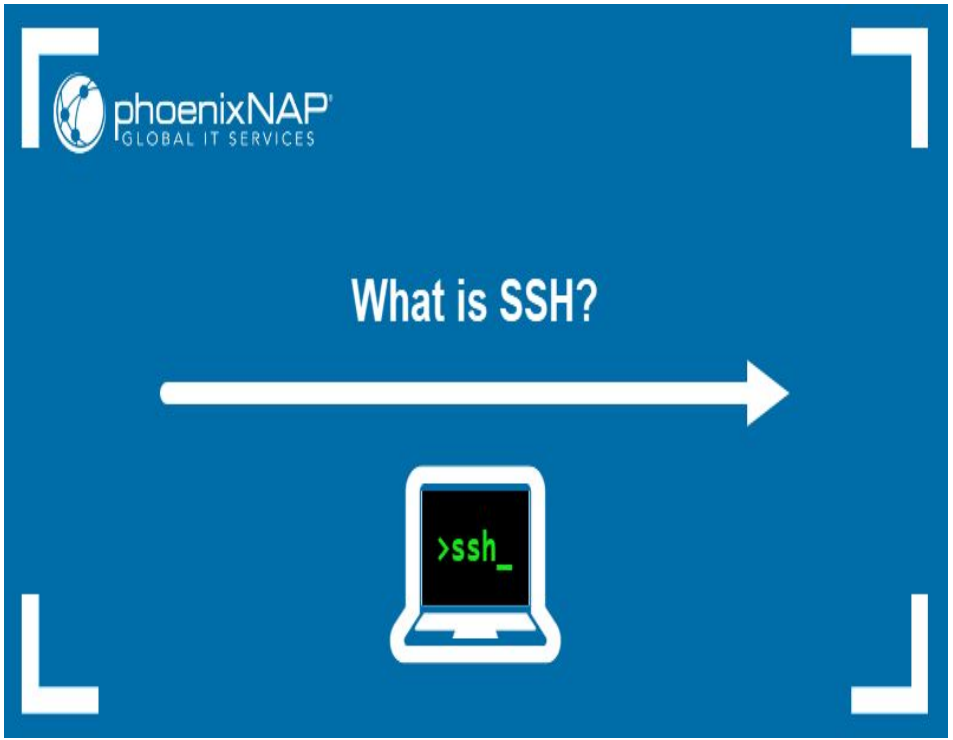


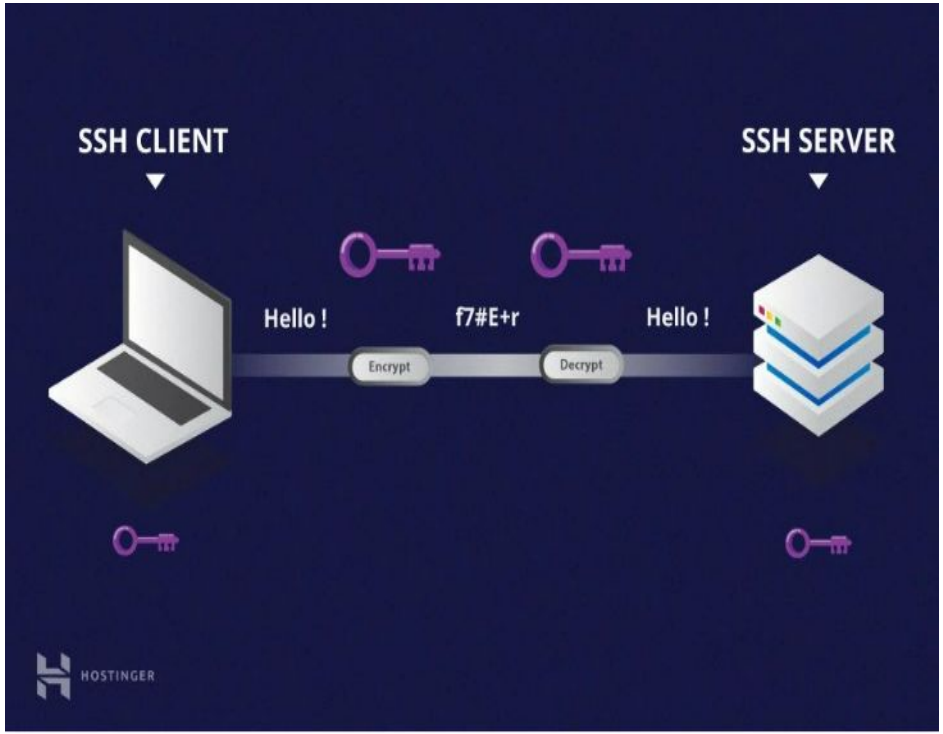
SSH

Colin Brindley, Andrew Feitl, Nick Survant, Zackary Tullar



SECURE SHELL (SSH)

- SSH (also know as secure socket shell):
  - Cryptographic Network Protocol
  - Operates network services securely over an unsecured network
  - Designed for Unix operating systems
  - Replaced Telnet
  - Main entry point for attackers

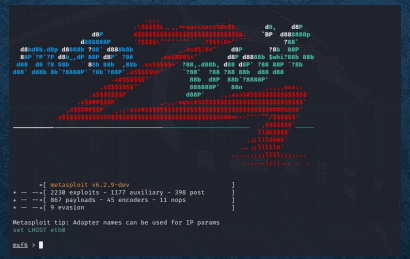


HOW IT'S USED

- SSH uses Symmetric Encryption, Asymmetric Encryption, and Hashing
- Symmetric keys are used for encrypting entire connection
- Asymmetric keys (public/private) are used for authenticating connection
- Hashing is used to protect data that is not meant to be reversed

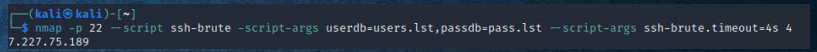
EXPLOITATION OF PROTECTED SSH

- There are a number of tools that can compromise SSH authentication steps
- Kali Linux can utilize a number of free, open-source programs made for this



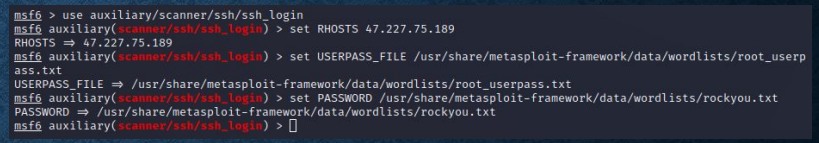
NMAP

- Network Mapper is a tool for probing networks
- With scripts, it can also be used to conduct brute force attacks
- Brute force can be used to establish unauthorized SSH connections



METASPLOIT

- Metasploit Framework is a pen testing application
- It has many built-in exploits that are updated as vulnerabilites are discovered
- Some of these can be used to compromise SSH



HYDRA

- HYDRA THC is a login cracking program
- It works to guess the correct username and password required
- Often used with other tools to generate wordlists for more accurate cracking than a generic list

```
Enter the service to attack (eg: ftp, ssh, http-post-form): hydra -L usr/share/wordlists.rockyou.txt -P /usr/share/
wordlists/rockyou.txt 47.227.75.189 -t 4 ssh
```

SOURCES

- https://en.wikipedia.org/wiki/Secure_Shell
- https://sysdig.com/blog/aws-secure-ssh-ec2-threats/
- https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process