David Thomsen
Eth Hack

- Password Guessing
  - After 2 step scan
  - Usernames/emails
  - Server IP's
  - Open Ports
  - Services running
  - Physical security vulnerabilities
  - Procedure/process/training vulns
  - Domain names
  - Finding possible exploitation spots
- Gaining a Foothold
  - Depending on the results:
  - Vulnerabilities that can be exploited remotely and provide system access
  - Physical access to systems (if in scope)
  - Endpoint malware
- Credentials
  - Phishing
  - Brute-forcing
  - Malware
  - Guess (worth a shot)
  - **Defaults for services (Source)**
- Goals of Password Guessing
  - See if you can get a few usernames and any passwords w minimal effort
  - Look for default and common passwords with account information
  - Testing completed in hours/days
- Password Guessing Techniques
  - **What is needed?**
  - List of usernames as well as naming conventions (i.e. first.last@xxx firstinitial.lastname@xxx, etc.)
  - List of possible passwords
  - List of authenticated services to test against
- Username Lists
  - Recon and scanning
    - LDAP and other Dirs
    - Website info
    - Email addresses
  - Wordlists
- Password Lists
  - Dictionary are available for download
  - Crawling websites to gather words/usernames for a particular org.
  - CEWL is a Kali tool for Lists

- Processes that takes wordlists and “mangle: them for password variation
  - **RSMangler is the Kali tool**
- Possible examples
  - Leet speak: G@nd@lfTh3Gr3y
  - Add numbers: Canada1
  - Append/prepend years: 2019Patriots
  - Mix case: PaTrIoTs
  - Special characters: Ch@mpl@1n!21
  - Combine words: bobadmin
  - Review organizations password policy if available
- Services?
  - RDP and SSH are great for access
  - But often heavily monitored
  - DCs/timeouts
  - Subject to Automatic locking
- Other services to use
  - FTP
  - SMTP
  - Simple web authentication
  - SMB and other file services
  - LDAP and other directory services
- Kali Tools
  - Ncrack
  - Medusa
  - Hydra