## Web Application

* Cross-Site Scripting (XSS)
  + Reflected
  + Persistent
* Cross-Site Request Forgery (CSRF)
* SQL injection
* File uploads
  + Only allows needed file types
    - Checked server-side
    - Can’t be spoofed
* Server-Side Request Forgery
* File paths / referenced files
  + Local File Inclusion
  + Remote File Inclusion
* Unsecured Cookies
  + HTTPOnly
  + Secure
  + X-XSS Protection
  + X-Content Type: nosniff
  + X-Frame-Options: SAMEORIGIN
    - Clickjacking
* Account login
  + Default credentials
  + User Enumeration
* Encryption / Cleartext
  + Using plaintext protocols
  + Login in cleartext
* Externally Accessible Admin Portals
* XML External Entity (XXE)
* Directory Listing
* Forceful Browsing - OTP bypass (?)
* Password Complexity
* Broken Password Reset
* Account Lockout
* EOL Software
* SSL errors
* IIS Shortname Disclosure
* Verbose Error Messages / Enticement Information
  + Default IIS
* Sensitive Information Disclosure
* Internal IP Disclosure
* Sensitive information stored in cookies
* Session timeout
* Session hijacking
* Source code disclosure
* Open redirect
* Insecure HTTP methods
  + TRACE
  + CONNECT
  + PUT
  + DELETE
* Unconfigured web servers
* Authentication over GET
* Default credentials

## Network Services

* Databases!
  + Default creds
  + Ability to execute commands via database
  + Sensitive data stored improperly
    - Social security numbers
    - Passwords
    - PCI
* File access / FTP
  + Config files w/ sensitive data
  + Backups w/ sensitive data
  + Command history (e.g. powershell audit logs)
* Limited access services (should not be open to all)
  + Redis, Memcache
* EOL Software
* Potentially Unwanted Services (ex. Crypto Mining)
* Enticement Information
* Anonymous FTP
* SSH User Enumeration
* DNS enumeration
  + AXFR zone transfer
* SMTP open relay
  + Able to send mail w/o authentication
* Access Controls (In general)
* Firewall Rule not best practice
  + CLOSED | FILTERED
* SMB Null Share
* Clear text protocols
  + Telnet
  + FTP
* Basic Auth
* ICMP ping through firewall

## Windows Domain

* RPC enumeration
  + Users
  + Groups
  + Password Policy
* Anonymous shares (SMB)
  + What can we read
  + What can we write
* ZeroLogon (CVE-2020-1472)
* Exchange Web Services - EWS
* Domain backups
* LDAP unauthenticated binds

## API

* Available endpoints
* Available methods
* Documentation
* Hardcoded keys
* API path traversal
* Code Injections
* Improper Access Controls on Methods
  + Role-based access controls (ie. administrator access)
  + Attribute based access controls (ie. user account number guessing)
* Authentication methods
  + Is an API key actually validated?
  + Can API keys be derived from known information?
* Are older versions of the API still queryable?

## Post-Exploitation

* Correct sudo permissions - “sudo -L”
* SSH keys (can’t read them)
* Vulnerable kernel version