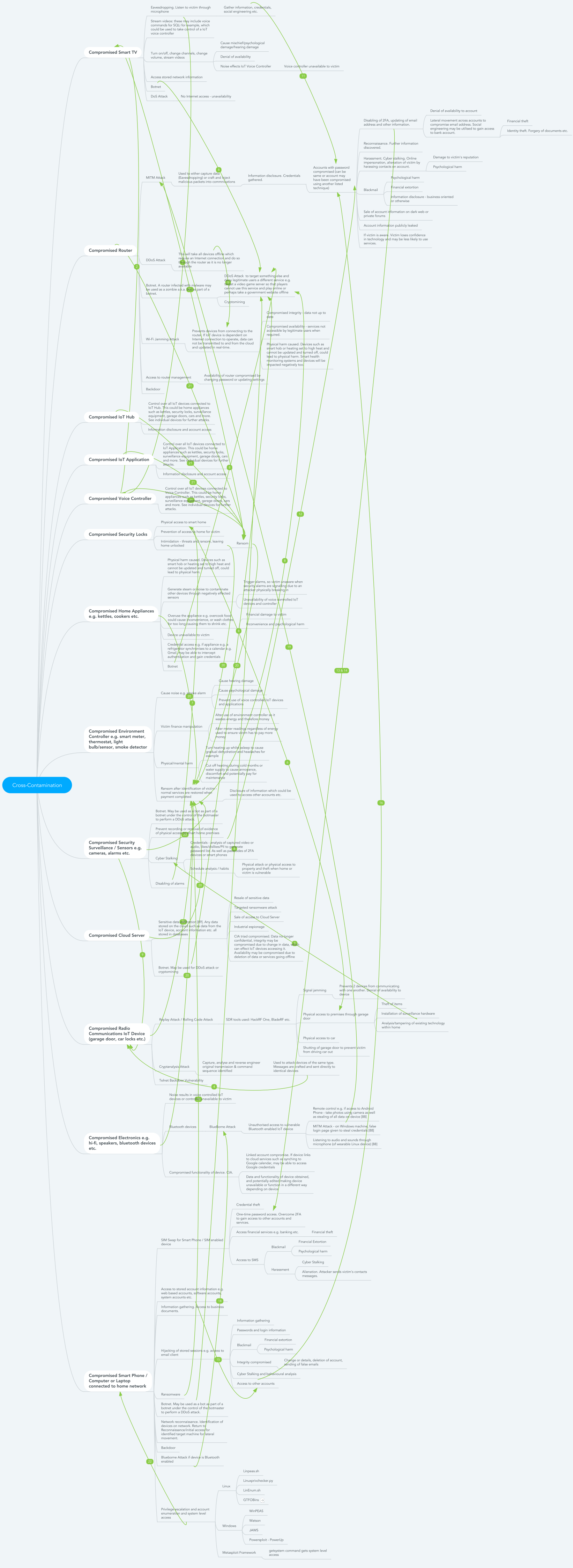

- Cross-Contamination
  - Compromised Smart TV
    - Eavesdropping. Listen to victim through microphone
      - Gather information, credentials, social engineering etc.
    - Stream videos: these may include voice commands for SQLi for example, which could be used to take control of a IoT voice controller
    - Turn on/off, change channels, change volume, stream videos
      - Cause mischief/psychological damage/hearing damage
      - Denial of availability
      - Noise effects IoT Voice Controller
        - Voice controller unavailable to victim
    - Access stored network information
    - Botnet
    - DoS Attack
      - No Internet access - unavailability
  - Compromised Router
    - MITM Attack
      - Used to either capture data (Eavesdropping) or craft and inject malicious packets into commnications
        - Information disclosure. Credentials gathered.
          - Accounts with password compromised (can be same or account may have been compromised using another listed technique)
            - Disabling of 2FA, updating of email address and other information.
              - Denial of availability to account
              - Lateral movement across accounts to compromise email address. Social engineering may be utilised to gain access to bank account.
                - Financial theft
                - Identity theft. Forgery of documents etc.
            - Reconnaissance. Further information discovered.
            - Harassment. Cyber stalking. Online impersonation, alienation of victim by harassing contacts on account.
              - Damage to victim's reputation
              - Psychological harm
            - Blackmail
              - Psychological harm
              - Financial extortion
              - Information disclosure - business oriented or otherwise
            - Sale of account information on dark web or private forums
            - Account information publicly leaked
            - If victim is aware. Victim loses confidence in technology and may be less likely to use services.
    - DDoS Attack
      - This will take all devices offline which require an Internet connection and do so through the router as it is no longer available
    - Botnet. A router infected with malware may be used as a zombie a.k.a. bot as part of a botnet.
      - DDoS Attack to target something else and deny legitimate users a different service e.g. target a video game server so that players cannot use this service and play online or perhaps take a government website offline
      - Cryptomining
    - Wi-Fi Jamming Attack
      - Prevents devices from connecting to the router. If IoT device is dependent on Internet connection to operate, data can not be transmitted to and from the cloud and updated in real-time.
        - Compromised integrity - data not up to date
        - Compromised availability - services not accessible by legitimate users when required.
        - Physical harm caused. Devices such as smart hob or heating set to high heat and cannot be updated and turned off, could lead to physical harm. Smart health monitoring systems and devices will be impacted negatively too.
    - Access to router management
      - Availability of router compromised by changing password or updating settings
    - Backdoor
  - Compromised IoT Hub
    - Control over all IoT devices connected to IoT Hub. This could be home appliances such as kettles, security locks, surveillance equipment, garage doors, cars and more. See individual devices for further attacks.
    - Information disclosure and account access
  - Compromised IoT Application
    - Control over all IoT devices connected to IoT Application. This could be home appliances such as kettles, security locks, surveillance equipment, garage doors, cars and more. See individual devices for further attacks.
    - Information disclosure and account access
  - Compromised Voice Controller
    - Control over all IoT devices connected to Voice Controller. This could be home appliances such as kettles, security locks, surveillance equipment, garage doors, cars and more. See individual devices for further attacks.
  - Compromised Security Locks
    - Physical access to smart home
    - Prevention of access to home for victim
    - Intimidation - threats and ransom, leaving home unlocked
      - Ransom
  - Compromised Home Appliances e.g. kettles, cookers etc.
    - Physical harm caused. Devices such as smart hob or heating set to high heat and cannot be updated and turned off, could lead to physical harm.
    - Generate steam or noise to contaminate other devices through negatively effected sensors
      - Trigger alarms, so victim unaware when security alarms are signalling due to an attacker physically breaking in
      - Unavailability of voice controlled IoT devices and controller
    - Overuse the appliance e.g. overcook food could cause inconvenience, or wash clothes for too long causing them to shrink etc.
      - Financial damage to victim
      - Inconvenience and psychological harm
    - Device unavailable to victim
    - Credential access e.g. if appliance e.g. a refrigerator synchronises to a calendar e.g. Gmail, may be able to intercept authentication and gain credentials
    - Botnet
  - Compromised Environment Controller e.g. smart meter, thermostat, light bulb/sensor, smoke detector
    - Cause noise e.g. smoke alarm
      - Cause hearing damage
      - Cause psychological damage
      - Prevent use of voice controlled IoT devices and applications
    - Victim finance manipulation
      - Alter use of environment controller so it wastes energy and therefore money
      - Alter meter readings regardless of energy used to ensure victim has to pay more money
    - Physical/mental harm
      - Turn heating up whilst asleep to cause gradual dehydration and headaches for example
      - Cut off heating during cold months or water supply to cause annoyance, discomfort and potentially pay for maintenance
    - Ransom after identification of victim - normal services are restored when payment completed
      - Disclosure of information which could be used to access other accounts etc.
  - Compromised Security Surveillance / Sensors e.g. cameras, alarms etc.
    - Botnet. May be used as a bot as part of a botnet under the control of the botmaster to perform a DDoS attack.
    - Prevent recording or removal of evidence of physical access to smart home premises
    - Cyber Stalking
      - Credentials - analysis of captured video or audio, likes/dislikes/PII to generate password list. As well as passcodes of 2FA devices or smart phones
      - Schedule analysis / habits
        - Physical attack or physical access to property and theft when home or victim is vulnerable
    - Disabling of alarms
  - Compromised Cloud Server
    - Sensitive data exfiltration [89]. Any data stored on the cloud such as data from the IoT device, account information etc. all stored in databases
      - Resale of sensitive data
      - Targeted ransomware attack
      - Sale of access to Cloud Server
      - Industrial espionage
      - CIA triad compromised. Data no longer confidential, integrity may be compromised due to change in data, which can effect IoT devices accessing it. Availability may be compromised due to deletion of data or services going offline
    - Botnet. May be used for DDoS attack or cryptomining
  - Compromised Radio Communications IoT Device (garage door, car locks etc.)
    - Replay Attack / Rolling Code Attack
      - SDR tools used: HackRF One, BladeRF etc.
        - Signal jamming
          - Prevents 2 devices from communicating with one another. Denial of availability to device
        - Physical access to premises through garage door
          - Theft of items
          - Installation of surveillance hardware
          - Analysis/tampering of existing technology within home
        - Physical access to car
        - Shutting of garage door to prevent victim from driving car out
    - Cryptanalysis Attack
      - Capture, analyse and reverse engineer original transmission & command sequence identified
        - Used to attack devices of the same type. Messages are crafted and sent directly to identical devices
    - Telnet Backdoor Vulnerability
  - Compromised Electronics e.g. hi-fi, speakers, bluetooth devices etc.
    - Noise results in voice controlled IoT devices or controller unavailable to victim
    - Bluetooth devices
      - BlueBorne Attack
        - Unauthorised access to vulnerable Bluetooth enabled IoT device
          - Remote control e.g. if access to Android Phone - take photos using camera as well as stealing of all data on device [88]
          - MITM Attack - on Windows machine, false login page given to steal credentials [88]
          - Listening to audio and sounds through microphone (of wearable Linux device) [88]
    - Compromised functionality of device. CIA.
      - Linked account compromise. If device links to cloud services such as synching to Google calendar, may be able to access Google credentials
      - Data and functionality of device obtained, and potentially edited making device unavailable or function in a different way depending on device
  - Compromised Smart Phone / Computer or Laptop connected to home network
    - SIM Swap for Smart Phone / SIM enabled device
      - Credential theft
      - One-time password access. Overcome 2FA to gain access to other accounts and services.
      - Access financial services e.g. banking etc.
        - Financial theft
      - Access to SMS
        - Blackmail
          - Financial Extortion
          - Psychological harm
        - Harassment
          - Cyber Stalking
          - Alienation. Attacker sends victim's contacts messages.
    - Access to stored account information e.g. web based accounts, software accounts, system accounts etc.
    - Information gathering. Access to business documents.
    - Hijacking of stored sessions e.g. access to email client
      - Information gathering
      - Passwords and login information
      - Blackmail
        - Financial extortion
        - Psychological harm
      - Integrity compromised
        - Change or details, deletion of account, sending of false emails
      - Cyber Stalking and behavioural analysis
      - Access to other accounts
    - Ransomware
    - Botnet. May be used as a bot as part of a botnet under the control of the botmaster to perform a DDoS attack.
    - Network reconnaissance. Identification of devices on network. Return to Reconnaissance/initial access for identified target machine for lateral movement.
    - Backdoor
    - Blueborne Attack if device is Bluetooth enabled
    - Privilege escalation and account enumeration and system level access
      - Linux
        - Linpeas.sh
        - Linuxprivchecker.py
        - LinEnum.sh
        - GTFOBins
      - Windows
        - WinPEAS
        - Watson
        - JAWS
        - Powersploit - PowerUp
      - Metasploit Framework
        - getsystem command gets system level access

Cross-Contamination

1. Compromised Smart TV

1.1. Eavesdropping. Listen to victim through microphone

1.1.1. Gather information, credentials, social engineering etc.

1.2. Stream videos: these may include voice commands for SQLi for example, which could be used to take control of a IoT voice controller

1.3. Turn on/off, change channels, change volume, stream videos

1.3.1. Cause mischief/psychological damage/hearing damage

1.3.2. Denial of availability

1.3.3. Noise effects IoT Voice Controller

1.3.3.1. Voice controller unavailable to victim

1.4. Access stored network information

1.5. Botnet

1.6. DoS Attack

1.6.1. No Internet access - unavailability

2. Compromised Router

2.1. MITM Attack

2.1.1. Used to either capture data (Eavesdropping) or craft and inject malicious packets into commnications

2.1.1.1. Information disclosure. Credentials gathered.

2.1.1.1.1. Accounts with password compromised (can be same or account may have been compromised using another listed technique)

2.1.1.1.1.1. Disabling of 2FA, updating of email address and other information.

2.1.1.1.1.1.1. Denial of availability to account

2.1.1.1.1.1.2. Lateral movement across accounts to compromise email address. Social engineering may be utilised to gain access to bank account.

2.1.1.1.1.1.2.1. Financial theft

2.1.1.1.1.1.2.2. Identity theft. Forgery of documents etc.

2.1.1.1.1.2. Reconnaissance. Further information discovered.

2.1.1.1.1.3. Harassment. Cyber stalking. Online impersonation, alienation of victim by harassing contacts on account.

2.1.1.1.1.3.1. Damage to victim's reputation

2.1.1.1.1.3.2. Psychological harm

2.1.1.1.1.4. Blackmail

2.1.1.1.1.4.1. Psychological harm

2.1.1.1.1.4.2. Financial extortion

2.1.1.1.1.4.3. Information disclosure - business oriented or otherwise

2.1.1.1.1.5. Sale of account information on dark web or private forums

2.1.1.1.1.6. Account information publicly leaked

2.1.1.1.1.7. If victim is aware. Victim loses confidence in technology and may be less likely to use services.

2.2. DDoS Attack

2.2.1. This will take all devices offline which require an Internet connection and do so through the router as it is no longer available

2.3. Botnet. A router infected with malware may be used as a zombie a.k.a. bot as part of a botnet.

2.3.1. DDoS Attack to target something else and deny legitimate users a different service e.g. target a video game server so that players cannot use this service and play online or perhaps take a government website offline

2.3.2. Cryptomining

2.4. Wi-Fi Jamming Attack

2.4.1. Prevents devices from connecting to the router. If IoT device is dependent on Internet connection to operate, data can not be transmitted to and from the cloud and updated in real-time.

2.4.1.1. Compromised integrity - data not up to date

2.4.1.2. Compromised availability - services not accessible by legitimate users when required.

2.4.1.3. Physical harm caused. Devices such as smart hob or heating set to high heat and cannot be updated and turned off, could lead to physical harm. Smart health monitoring systems and devices will be impacted negatively too.

2.5. Access to router management

2.5.1. Availability of router compromised by changing password or updating settings

2.6. Backdoor

3. Compromised IoT Hub

3.1. Control over all IoT devices connected to IoT Hub. This could be home appliances such as kettles, security locks, surveillance equipment, garage doors, cars and more. See individual devices for further attacks.

3.2. Information disclosure and account access

4. Compromised IoT Application

4.1. Control over all IoT devices connected to IoT Application. This could be home appliances such as kettles, security locks, surveillance equipment, garage doors, cars and more. See individual devices for further attacks.

4.2. Information disclosure and account access

5. Compromised Voice Controller

5.1. Control over all IoT devices connected to Voice Controller. This could be home appliances such as kettles, security locks, surveillance equipment, garage doors, cars and more. See individual devices for further attacks.

6. Compromised Security Locks

6.1. Physical access to smart home

6.2. Prevention of access to home for victim

6.3. Intimidation - threats and ransom, leaving home unlocked

6.3.1. Ransom

7. Compromised Home Appliances e.g. kettles, cookers etc.

7.1. Physical harm caused. Devices such as smart hob or heating set to high heat and cannot be updated and turned off, could lead to physical harm.

7.2. Generate steam or noise to contaminate other devices through negatively effected sensors

7.2.1. Trigger alarms, so victim unaware when security alarms are signalling due to an attacker physically breaking in

7.2.2. Unavailability of voice controlled IoT devices and controller

7.3. Overuse the appliance e.g. overcook food could cause inconvenience, or wash clothes for too long causing them to shrink etc.

7.3.1. Financial damage to victim

7.3.2. Inconvenience and psychological harm

7.4. Device unavailable to victim

7.5. Credential access e.g. if appliance e.g. a refrigerator synchronises to a calendar e.g. Gmail, may be able to intercept authentication and gain credentials

7.6. Botnet

8. Compromised Environment Controller e.g. smart meter, thermostat, light bulb/sensor, smoke detector

8.1. Cause noise e.g. smoke alarm

8.1.1. Cause hearing damage

8.1.2. Cause psychological damage

8.1.3. Prevent use of voice controlled IoT devices and applications

8.2. Victim finance manipulation

8.2.1. Alter use of environment controller so it wastes energy and therefore money

8.2.2. Alter meter readings regardless of energy used to ensure victim has to pay more money

8.3. Physical/mental harm

8.3.1. Turn heating up whilst asleep to cause gradual dehydration and headaches for example

8.3.2. Cut off heating during cold months or water supply to cause annoyance, discomfort and potentially pay for maintenance

8.4. Ransom after identification of victim - normal services are restored when payment completed

8.4.1. Disclosure of information which could be used to access other accounts etc.

9. Compromised Security Surveillance / Sensors e.g. cameras, alarms etc.

9.1. Botnet. May be used as a bot as part of a botnet under the control of the botmaster to perform a DDoS attack.

9.2. Prevent recording or removal of evidence of physical access to smart home premises

9.3. Cyber Stalking

9.3.1. Credentials - analysis of captured video or audio, likes/dislikes/PII to generate password list. As well as passcodes of 2FA devices or smart phones

9.3.2. Schedule analysis / habits

9.3.2.1. Physical attack or physical access to property and theft when home or victim is vulnerable

9.4. Disabling of alarms

10. Compromised Cloud Server

10.1. Sensitive data exfiltration [89]. Any data stored on the cloud such as data from the IoT device, account information etc. all stored in databases

10.1.1. Resale of sensitive data

10.1.2. Targeted ransomware attack

10.1.3. Sale of access to Cloud Server

10.1.4. Industrial espionage

10.1.5. CIA triad compromised. Data no longer confidential, integrity may be compromised due to change in data, which can effect IoT devices accessing it. Availability may be compromised due to deletion of data or services going offline

10.2. Botnet. May be used for DDoS attack or cryptomining

11. Compromised Radio Communications IoT Device (garage door, car locks etc.)

11.1. Replay Attack / Rolling Code Attack

11.1.1. SDR tools used: HackRF One, BladeRF etc.

11.1.1.1. Signal jamming

11.1.1.1.1. Prevents 2 devices from communicating with one another. Denial of availability to device

11.1.1.2. Physical access to premises through garage door

11.1.1.2.1. Theft of items

11.1.1.2.2. Installation of surveillance hardware

11.1.1.2.3. Analysis/tampering of existing technology within home

11.1.1.3. Physical access to car

11.1.1.4. Shutting of garage door to prevent victim from driving car out

11.2. Cryptanalysis Attack

11.2.1. Capture, analyse and reverse engineer original transmission & command sequence identified

11.2.1.1. Used to attack devices of the same type. Messages are crafted and sent directly to identical devices

11.3. Telnet Backdoor Vulnerability

12. Compromised Electronics e.g. hi-fi, speakers, bluetooth devices etc.

12.1. Noise results in voice controlled IoT devices or controller unavailable to victim

12.2. Bluetooth devices

12.2.1. BlueBorne Attack

12.2.1.1. Unauthorised access to vulnerable Bluetooth enabled IoT device

12.2.1.1.1. Remote control e.g. if access to Android Phone - take photos using camera as well as stealing of all data on device [88]

12.2.1.1.2. MITM Attack - on Windows machine, false login page given to steal credentials [88]

12.2.1.1.3. Listening to audio and sounds through microphone (of wearable Linux device) [88]

12.3. Compromised functionality of device. CIA.

12.3.1. Linked account compromise. If device links to cloud services such as synching to Google calendar, may be able to access Google credentials

12.3.2. Data and functionality of device obtained, and potentially edited making device unavailable or function in a different way depending on device

13. Compromised Smart Phone / Computer or Laptop connected to home network

13.1. SIM Swap for Smart Phone / SIM enabled device

13.1.1. Credential theft

13.1.2. One-time password access. Overcome 2FA to gain access to other accounts and services.

13.1.3. Access financial services e.g. banking etc.

13.1.3.1. Financial theft

13.1.4. Access to SMS

13.1.4.1. Blackmail

13.1.4.1.1. Financial Extortion

13.1.4.1.2. Psychological harm

13.1.4.2. Harassment

13.1.4.2.1. Cyber Stalking

13.1.4.2.2. Alienation. Attacker sends victim's contacts messages.

13.2. Access to stored account information e.g. web based accounts, software accounts, system accounts etc.

13.3. Information gathering. Access to business documents.

13.4. Hijacking of stored sessions e.g. access to email client

13.4.1. Information gathering

13.4.2. Passwords and login information

13.4.3. Blackmail

13.4.3.1. Financial extortion

13.4.3.2. Psychological harm

13.4.4. Integrity compromised

13.4.4.1. Change or details, deletion of account, sending of false emails

13.4.5. Cyber Stalking and behavioural analysis

13.4.6. Access to other accounts

13.5. Ransomware

13.6. Botnet. May be used as a bot as part of a botnet under the control of the botmaster to perform a DDoS attack.

13.7. Network reconnaissance. Identification of devices on network. Return to Reconnaissance/initial access for identified target machine for lateral movement.

13.8. Backdoor

13.9. Blueborne Attack if device is Bluetooth enabled

13.10. Privilege escalation and account enumeration and system level access

13.10.1. Linux

13.10.1.1. Linpeas.sh

13.10.1.2. Linuxprivchecker.py

13.10.1.3. LinEnum.sh

13.10.1.4. GTFOBins

Link: https://gtfobins.github.io/

13.10.2. Windows

13.10.2.1. WinPEAS

13.10.2.2. Watson

13.10.2.3. JAWS

13.10.2.4. Powersploit - PowerUp

13.10.3. Metasploit Framework

13.10.3.1. getsystem command gets system level access