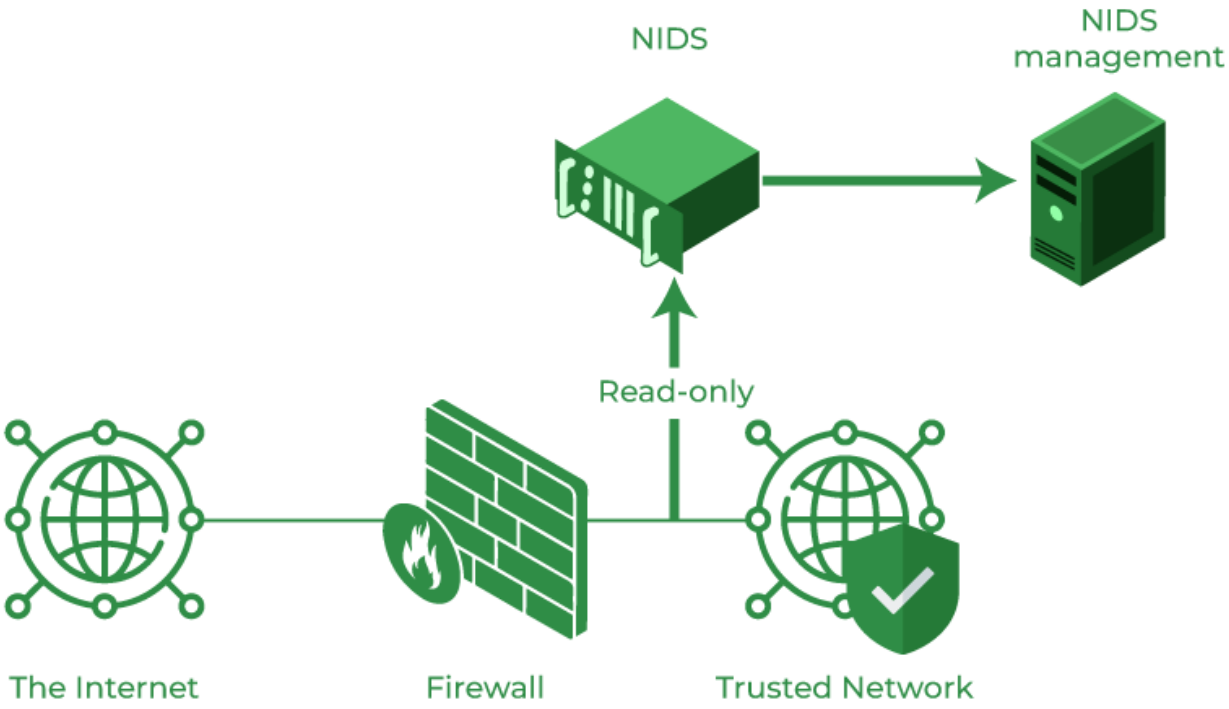
Network intrusion detection methods & how to evade them

Created by Mary McCready & Rohith Krishna Papani
CSE 548 - Advanced Network Security

Network Intrusion Detection System (NIDS) Overview



Types:

- Signature-based
- Stateful protocol analysis
- Behavioral-based
- Anomaly-based
- Heuristic-based

Image Source: https://www.geeksforgeeks.org/intrusion-detectio system-ids/

Signature vs. Anomaly-based detection

Signature-based NIDS

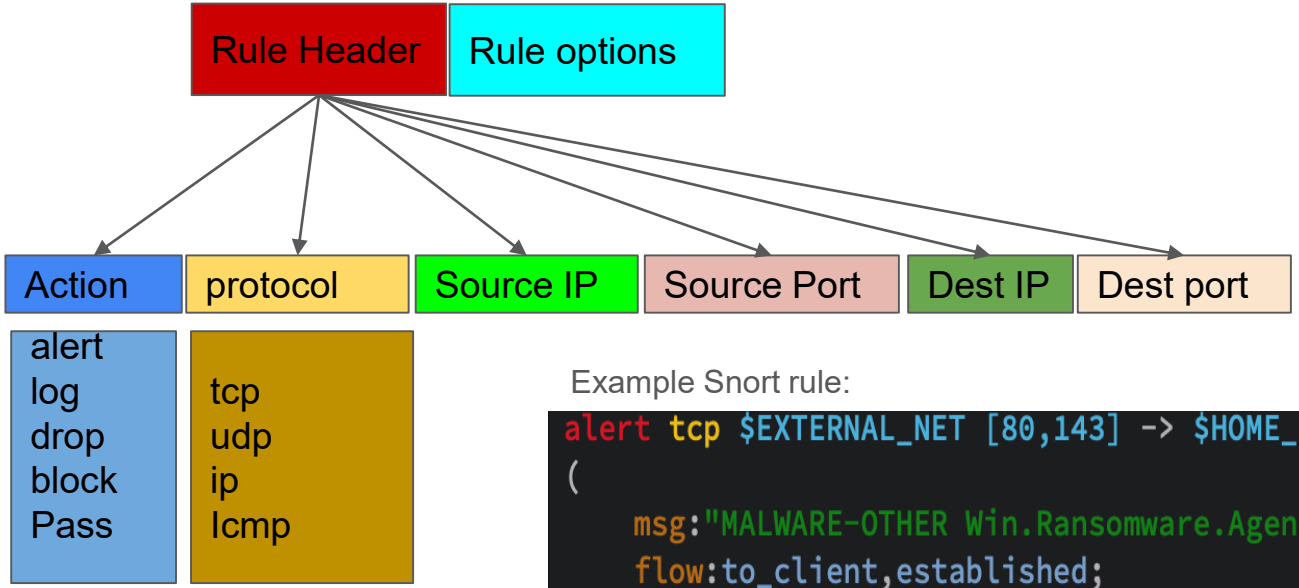
- Most common
- Compares incoming internet traffic against a known database of attack patterns and signatures
- Unable to detect novel attacks or variants of current attacks
- Needs to be updated frequently to keep up with latest threats
- Resource intensive and slows down the network process

Anomaly-based NIDS

- Establishes a baseline for network behavior using AI/ML and looks for deviations from the baseline
- Requires establishment and maintenance of a baseline
- False positives on new, yet valid behaviors
- Costly and complex to implement

Most effective when combined.

Primer on Snort Rules: Rule Header

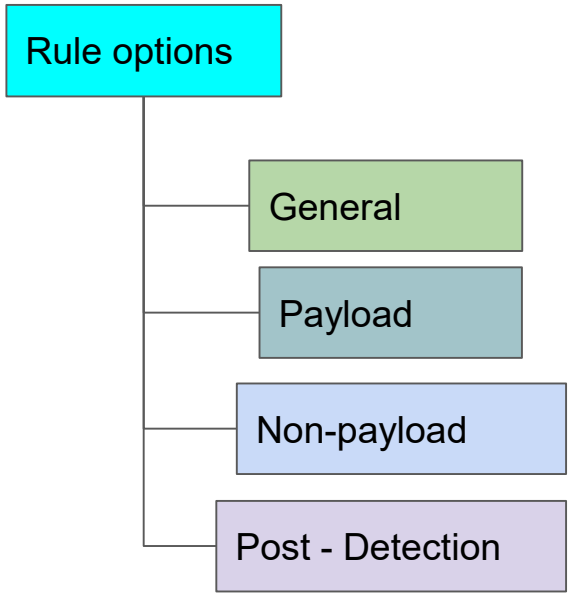


Example Snort rule:

```
alert tcp $EXTERNAL_NET [80,143] -> $HOME_NET any
(
    msg:"MALWARE-OTHER Win.Ransomware.Agent payload download attempt";
    flow:to_client,established;
    file_data; content:"secret_encryption_key",fast_pattern,nocase;
    service:http, imap;
    classtype:trojan-activity;
    sid:1;
)
```

Image source:
https://docs.snort.org/rules/headers/file_rules

Primer on Snort Rules: Rule Options




```
msg:"MALWARE-OTHER Win.Ransomware.Agent payload download attempt";
flow:to_client,established;
file_data; content:"secret_encryption_key",fast_pattern,nocase;
service:http, imap;
classtype:trojan-activity;
sid:1;
)
```

Image source:https://docs.snort.org/rules/

Recent changes to Snort3 rules

- New developments in Snort allow scanning of all source and destination IPs and ports available without needing to explicitly mention them.
- Snort can now process application layer protocols like HTTP, SMTP, POP3, IMAP, SMB, FTP
- The new file identification rules are better than the previous version because they can identify files by the contents of the file and then divide the file type.

More in detail at : https://docs.snort.org/rules/headers/new_header_types

ML for Anomaly detection

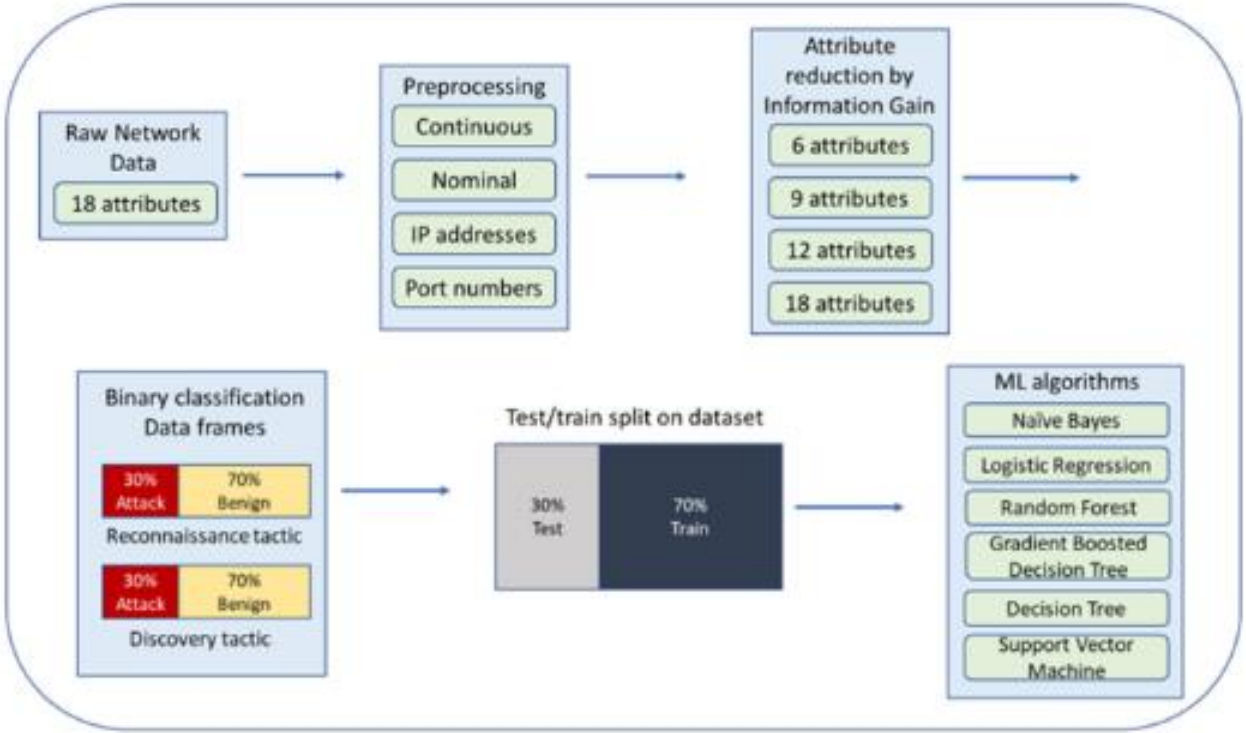
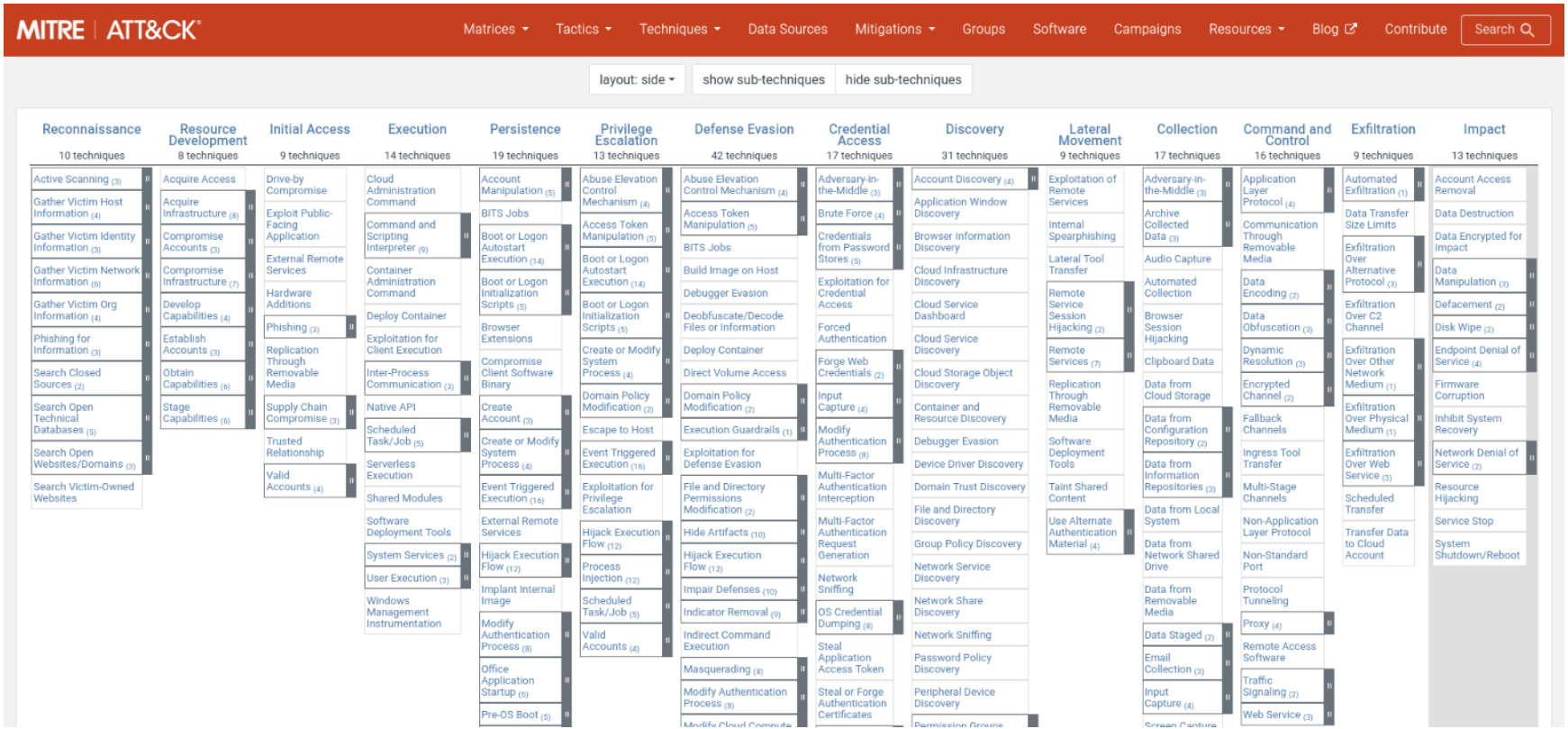


Figure 5. Experimental flow.

Image Source:https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9610873/bin/sensors-22-07999-g005.jpg

Review of Offensive Tactics & Techniques



Fictitious attack that can be detected by NIDS

1. Attacker does **network service discovery** to gather information
2. Attacker sends a **phishing** email to victim
3. Victim clicks the link which **executes malicious code**
4. The malicious code helps establish an **encrypted C2 channel**
5. Cover C2 channel tracks with **traffic signaling**
6. **Manipulate DNS with AiTM** to get user credentials & session cookies
7. Use valid (stolen) accounts to **log in remotely via SSH**
8. Collects data from a **network shared drive**
9. Steals that data through **exfiltration over C2 channel**
10. **Denial of service** on critical network services as a grand exit

Discovery: Network Service Discovery

Network Traffic Flow indicators:

- uncommon data flows
- port scans
- unusually high failed login attempts, logins from suspicious IPs
- DNS requests
- Custom protocols or protocol anomalies

Evasion Techniques:

- Stealth scanning
- Slow scanning
- Encrypted traffic
- Customized scans

Initial access: Phishing attachment/link

Network Traffic Content indicators:

- email with a malicious link or attachment
- file type, size, names
- unusual email client
- sender reputation
- sender's name and address don't match
- empty TO-field
- use of homoglyphs
- email header anomalies
- sender email is from a public domain

Network Traffic Flow indicators:

- non-standard port use
- suspicious path between sender and receiver

Evasion Techniques:

- obfuscated URLs or domain
- encrypting or obfuscating the payload
- ***impersonation***
- social engineering techniques to trick users into ignoring warning messages

Image source: https://www.insightportal.io/news/all-news/homoglyph-characters-being-used-for-malicious-web-domains

Evasion: Impersonation

Type of Impersonation	Forge Name	Forge Email	Real Life Example
Address Spoofer	May or may not	YES	Date: Fri, 14 Aug 2015 12:04:00 -0500 (CDT) From: "A Alivisatos" <aalivisatos@lbl.gov> To: XXXXXX@lbl.gov Subject: Good Morning ← Note Reply-To: aalivisatoslbl@mail.com Send me the balance on all our accounts as of today's date. Thanks
HistoricallyNewAttacker	Unseen Name	Unseen Email (@lbl.gov = forged)	Date: Tue, 08 Nov 2016 17:38:28 +0000 From: Computer Maintenance <compmaint@lbl.gov> To: afXXXXXXXh@lbl.gov Subject: Urgent: Email reactivation
NameSpoofer	Yes	Yes	From: Steven Chu <david@huismanauction.com> Date: January 9, 2017 at 11:22:42 PM PST To: undisclosed-recipients:; Subject: Steven Chu shared a File with you

Image Source: https://old.zeek.org/brocon2017/slides/spear_phish.pdf

Execution: User execution of malicious link/file

Network Connection Creation indicators:	**Network Traffic Content indicators:**	**Evasion Techniques:**
● new connections to malicious destinations ● multiple network connections or redirects ● outbound traffic from the victim's device to the phishing website or malicious server	● in use of files that do not normally initiate network connections ● malicious bash code execution patterns ● outbound traffic from the victim's device to the phishing website or malicious server ● multiple network connections or redirects ● non-standard port use ● suspicious path between sender and receiver	● Encrypted traffic ● Protocol Obfuscation ● Traffic fragmentation ● Timing-based evasion ● ***DNS Tunneling***

Evasion: DNS tunneling

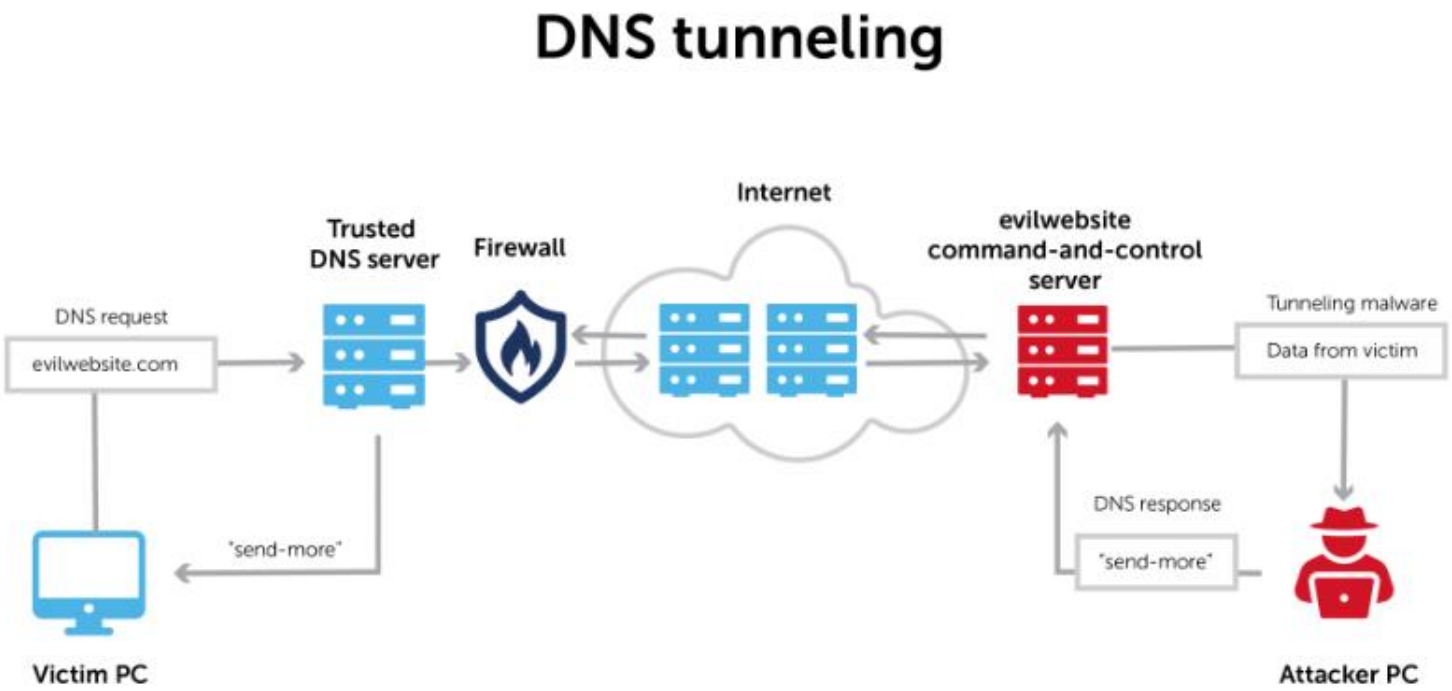


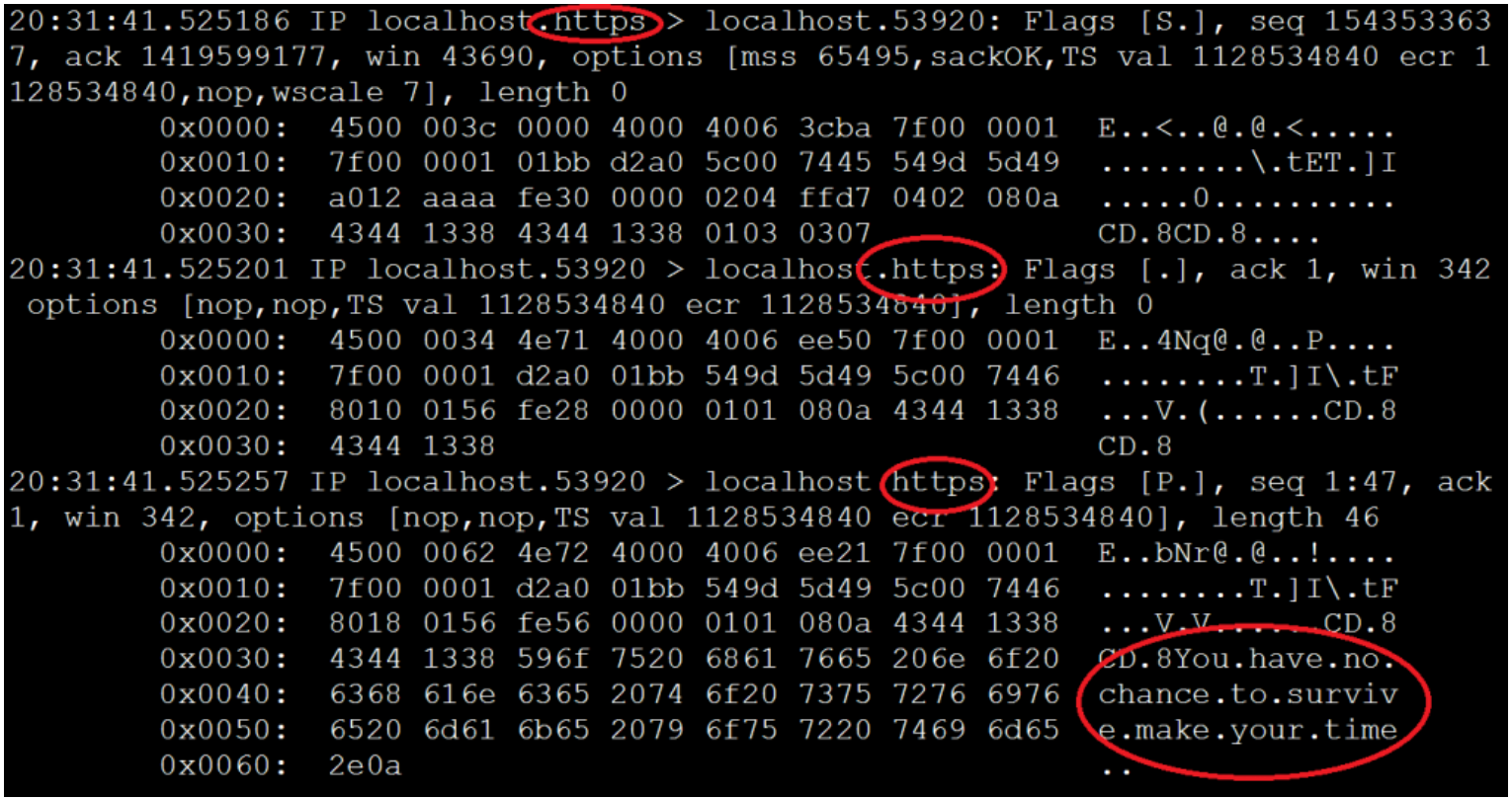
Image Source: DNS-tunneling-2048x976.png

Command & Control: Encrypted Channel

Network Traffic Content indicators:	**Network Traffic Flow indicators:**	**Evasion Techniques:**
● encrypted payloads	● use of non-standard protocols ● protocol mismatch at ports	● Use of non-standard ports ● Mimic legit traffic ● Traffic obfuscation ● ***Custom protocols***

Image Source:
blog_feature_MITRE_ATTCK_Matrix-Custom_C2_Protocol_01.png

Evasion: Custom C2 Protocols



Persistence: Traffic Signaling (port knocking)

Network Traffic Content indicators:	**Network Traffic Flow:**	**Evasion Techniques:**
● packets to detect application layer protocols are non-standard ● Unusual flags	● Connection attempts to closed ports ● Suddenly opened ports ● unexpected protocol standards and traffic volume	● Encryption ● Obfuscation ● Timing ● Use of multiple IPs ● Looking legitimate

Persistence: Traffic Signaling (port knocking)

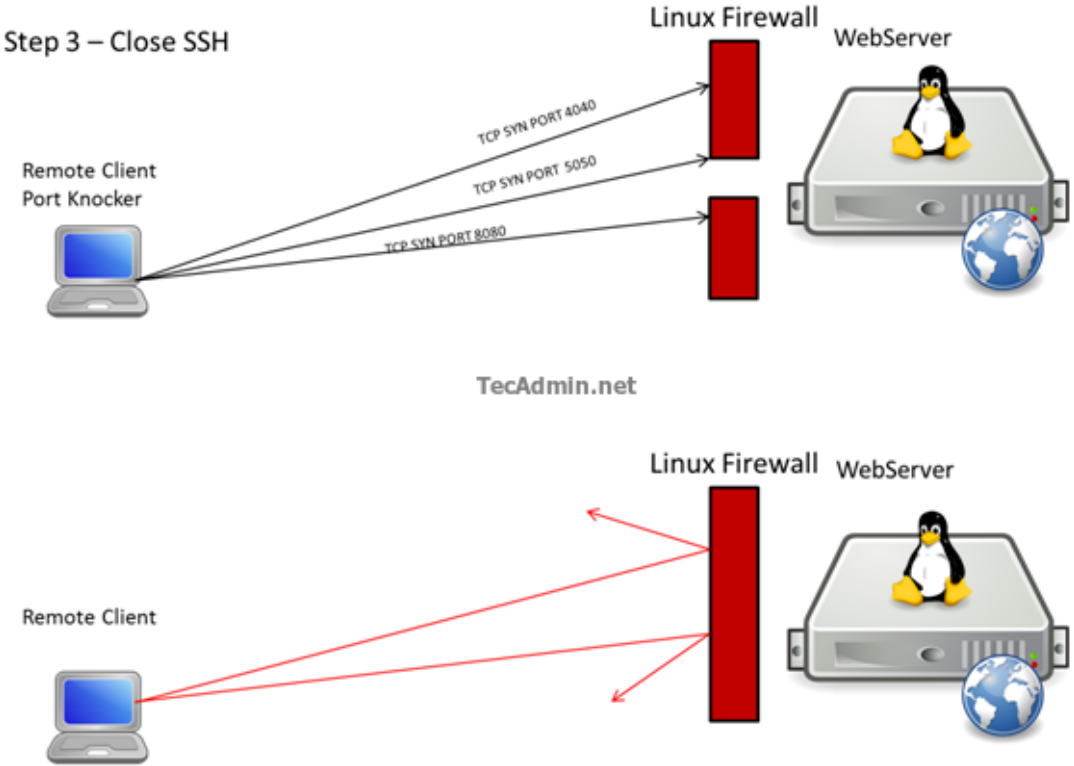


Image source: https://tecadmin.net/secure-ssh-connections-with-port-knocking-linux/

Credential Access: Adversary-in-the-middle

Network Traffic Content indicators:	**Network Traffic Flow indicators:**	**Evasion Techniques:**
● anomalies associated with AiTM behavior	● network traffic from unknown/unexpected hardware ● MAC addresses, DHCP ● events associated with network protocols ● suspiciously amped network flow through a device	● Encrypted traffic ● Legitimate access ● Non-standard ports ● Protocol mismatches ● Small, targeted attacks

Credential Access: Adversary-in-the-middle

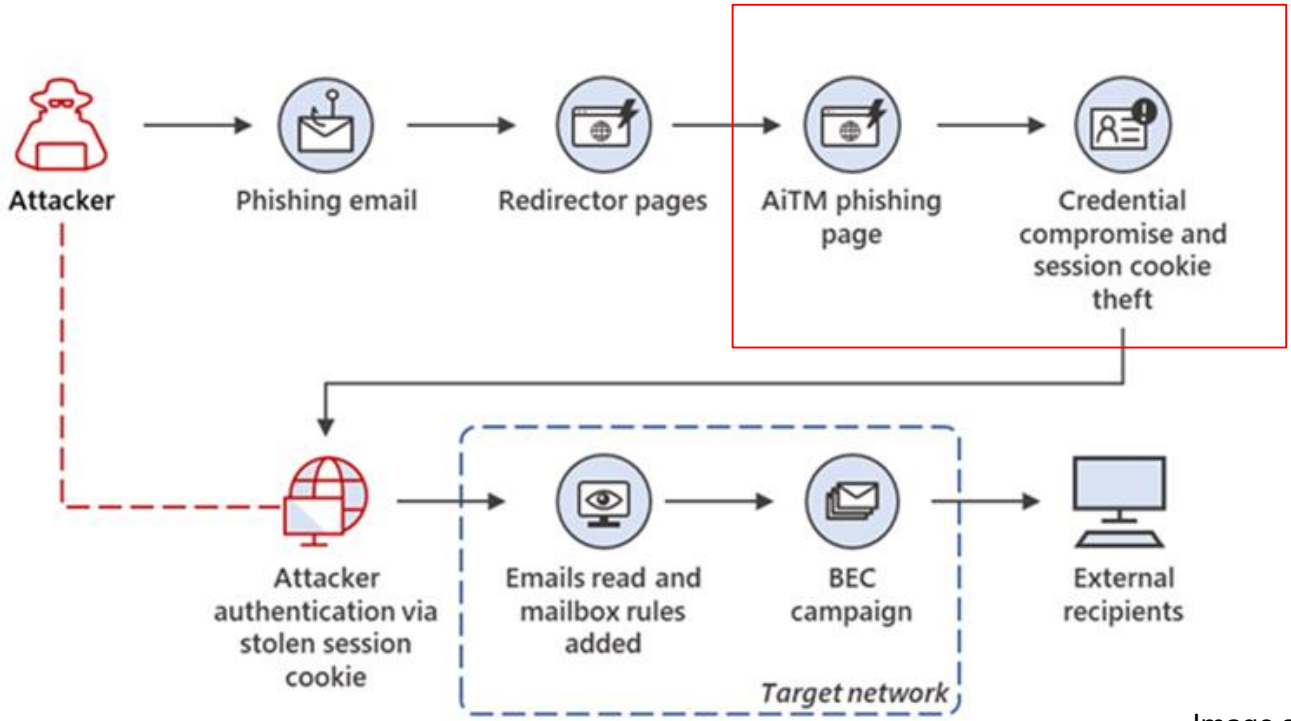


Image source: https://www.armorblox.com/blog/microsoft-phishing-attack/

Credential Access: Adversary-in-the-middle

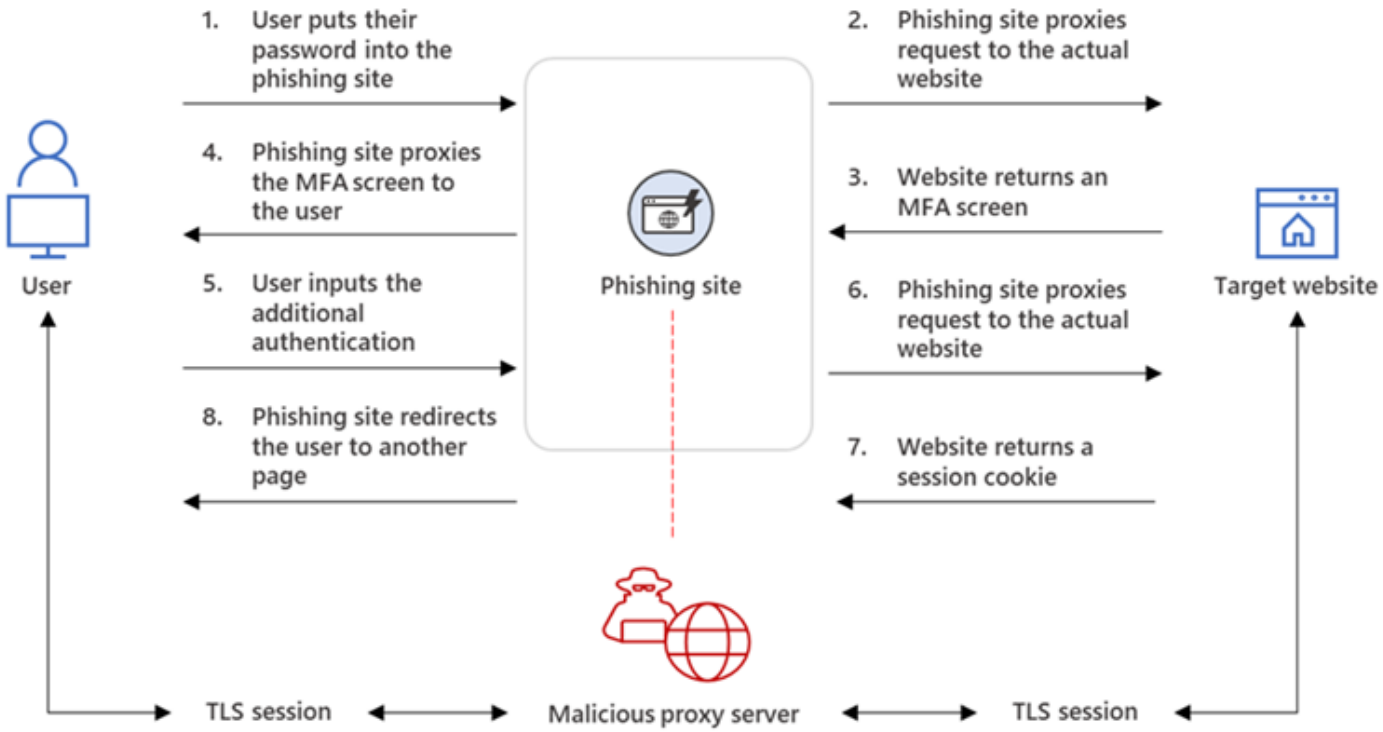


Image source: https://www.armorblox.com/blog/microsoft-phishing-attack/

Lateral Movement: Remote Services/SSH

Network Connection Creation indicators:	Evasion Techniques:
• new network connections (typically port 22) that may use valid accounts to log into remote machines using SSH	• Encrypted traffic • Use of legitimate access • Non-standard ports • ***Encrypted SSH tunnels***

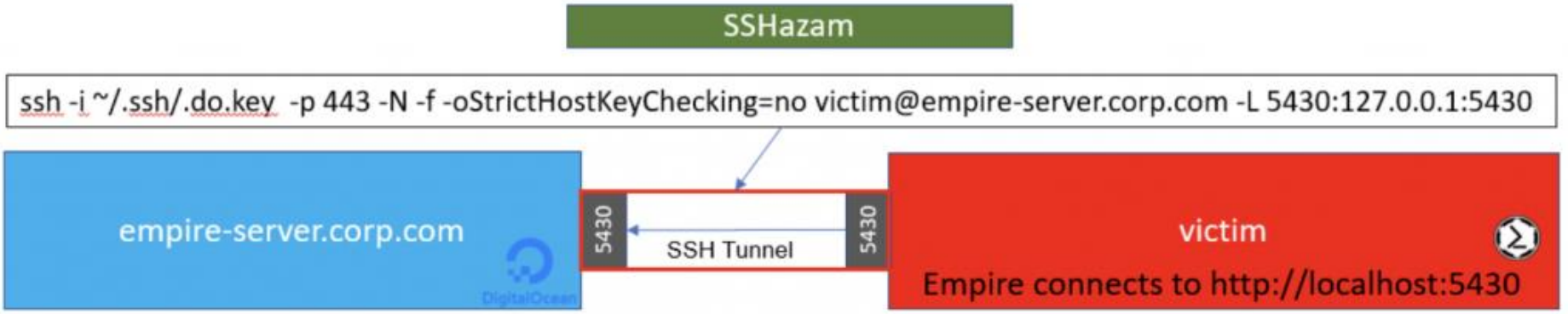


Image source:https://www.blackhillsinfosec.com/wp-content/uploads/2019/01/Screen-Shot-2019-01-01-at-8.01.30-PM.png

Collection: Data from network shared drive

Network Connection Creation indicators:	**Network Traffic Content indicators:**	**Evasion Techniques:**
● newly constructed network ● connections that may search network shares	● packet inspection for protocols that do not follow expected standards and traffic flows ● unexpected files (a .pdf ,doc file) trying to interact with the network shares ● abnormal and unexpected access to the network shares	● Legitimate access ● Data encryption ● Hide data in legitimate traffic ● Mimic legit traffic patterns ● Steganography

Exfiltration: Exfil over C2 Channel

Network Connection Creation indicators:	**Network Traffic Content indicators:**	**Network Traffic Flow indicators:**	**Evasion Techniques:**
● newly constructed network connections by untrusted hosts	● non-standard traffic	● uncommon data flows, such as large amount of data	● Data fragmentation ● Data encryption ● Hiding in legitimate traffic ● Mimic legit traffic patterns ● Use non-standard ports

Impact: Network Denial of Service

Network Traffic Flow indicators:	**Evasion Techniques:**
● uncommon data flows ● Processes using the network that normally do not normally have network communication or have never been seen before ● Sudden increase in ICMP, SYN, TCP, SYN-FIN packets	● Fragmentation ● Traffic variation ● ***Slow-rate attack***

Evasion:
Slow-rate Network Denial of Service

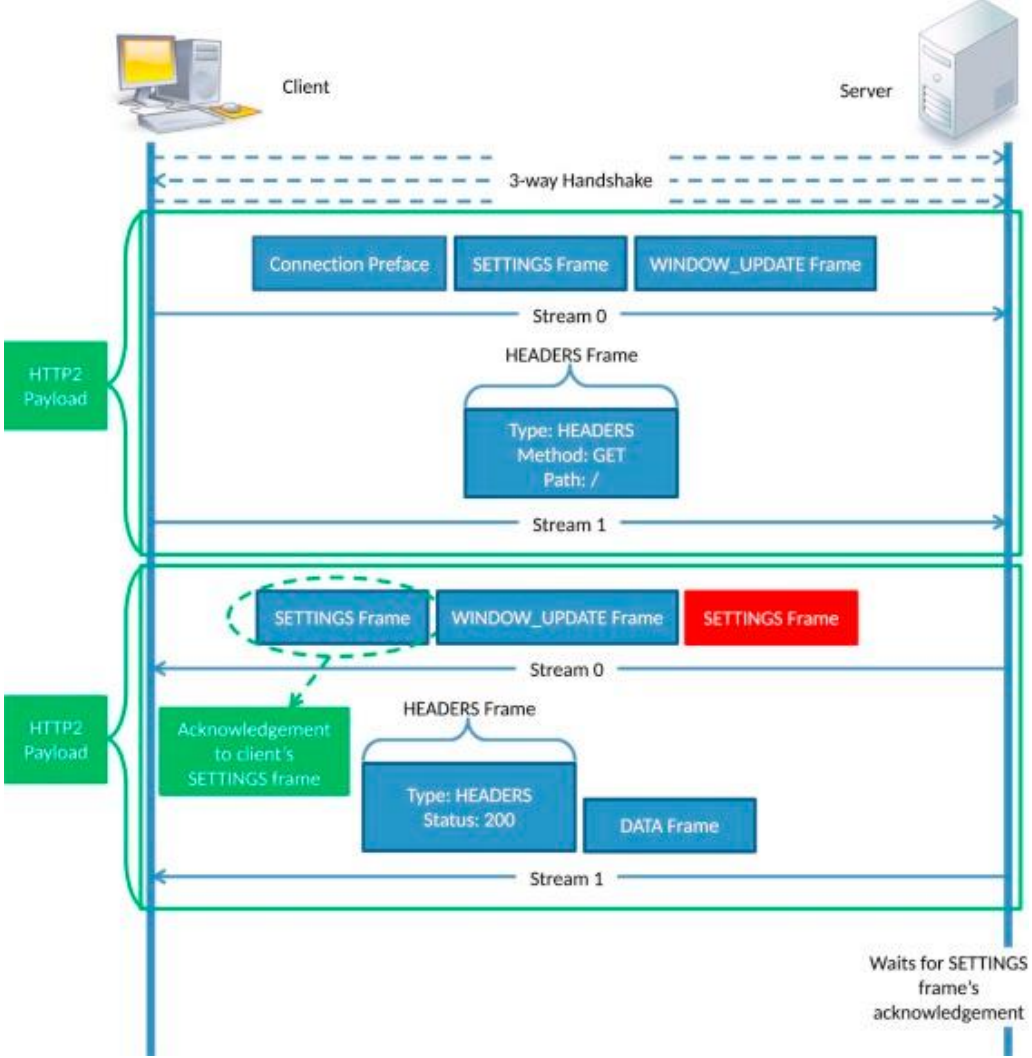


Image source:https://ars.els-cdn.com/content/image/1-s2.0-S0167404817301980-cose1205-fig-0006.jpg

Don’t get caught.

Image Source: https://dribbble.com/shots/11012025-Evil-Hacker