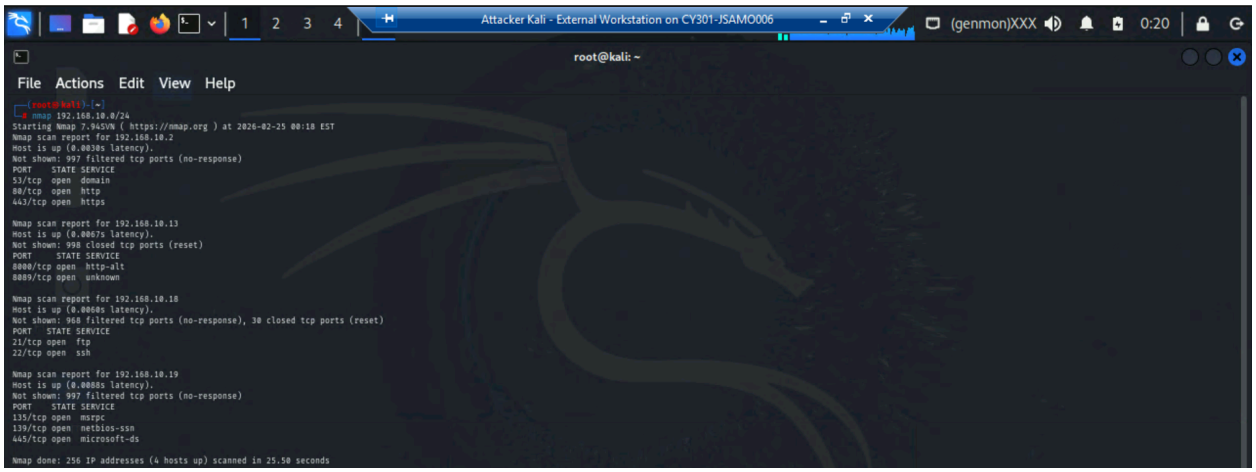
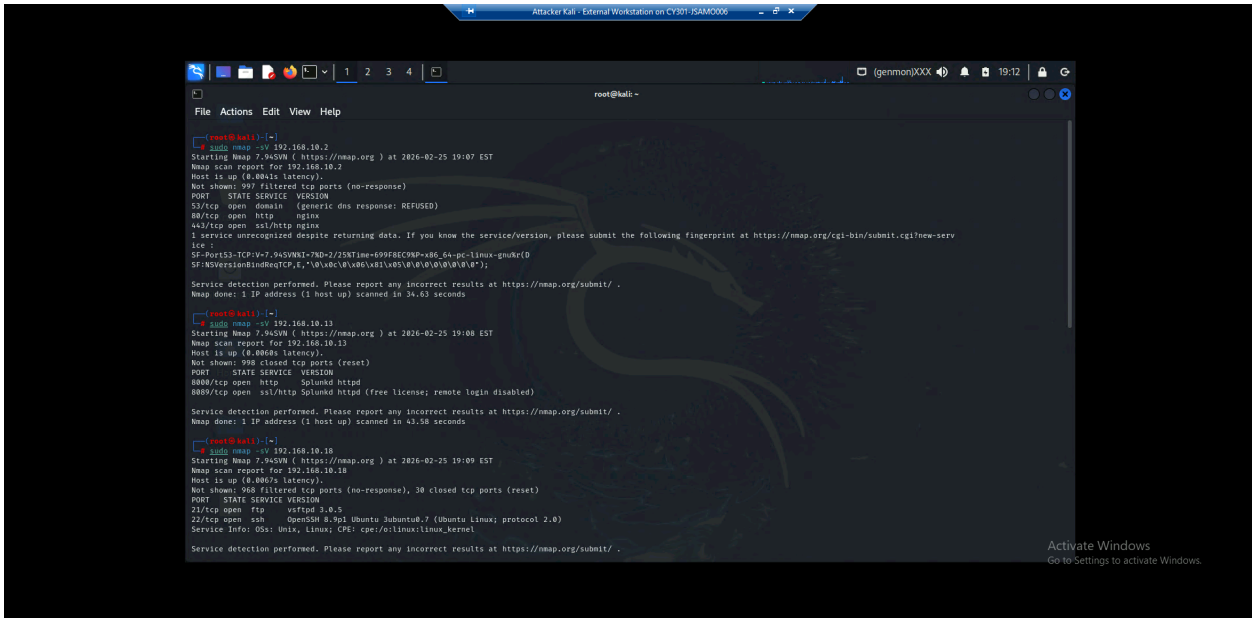
Old Dominion University
CYSE 301 Cybersecurity Techniques and Operations

Assignment #3: Sword Vs Shield

Julian Samonte
01227173

Task A: Sword - Network Scanning (5 + 15+ 20 = 40 points)
Power on the listed VMs,
• External Kali
• pfSense
• Ubuntu
• Windows Server 2022
Make sure not to add/delete any firewall rules/policies before continuing.
1. Run Wireshark in the Internal Kali VM while External Kali is scanning the network.
2. Use Nmap in External Kali to profile the basic information about the subnet topology (including open ports information, operating systems, etc.)






```
└─# sudo nmap -O 192.168.10.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-25 04:02 EST
Nmap scan report for 192.168.10.2
Host is up (0.0014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.23 seconds

┌──(root㉿kali)-[~]
└─# sudo nmap -O 192.168.10.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-25 04:03 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.44 seconds

┌──(root㉿kali)-[~]
└─# sudo nmap -O 192.168.10.18
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-25 04:03 EST
Nmap scan report for 192.168.10.18
Host is up (0.0036s latency).
Not shown: 968 filtered tcp ports (no-response), 30 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
Device type: general purpose|storage-misc|firewall|WAP
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X|5.X|2.4.X (92%), Synology DiskStation Manager 5.X (86%), WatchGuard Fireware 11.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8 cpe:/o:linux:linux_kernel:2.4
Aggressive OS guesses: Linux 2.6.32 (92%), Linux 2.6.32 or 3.10 (92%), Linux 4.4 (92%), Linux 2.6.32 - 2.6.35 (90%), Linux 2.6.32 - 2.6.39 (90%), Linux 2.6.32 - 3.0 (88%), Linux 5.0 - 5.4 (88%), Linux 3.11 - 4.1 (88%), Linux 3.2 - 3.8 (88%), Linux 4.0 (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.82 seconds

┌──(root㉿kali)-[~]
└─# sudo nmap -O 192.168.10.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-25 04:04 EST
Nmap scan report for 192.168.10.19
Host is up (0.022s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|11|2016 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2022 (97%), Microsoft Windows 11 21H2 (91%), Microsoft Windows Server 2016 (91%)
No exact OS matches for host (test conditions non-ideal).
```

```
┌──(root㉿kali)-[~]
└─# sudo nmap -O 192.168.10.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-25 19:18 EST
Nmap scan report for 192.168.10.13
Host is up (0.0062s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
8000/tcp open  http-alt
8089/tcp open  unknown
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=2/25%OT=8000%CT=1%CU=30569%PV=Y%DS=2%DC=I%G=Y%TM=69
OS:9F9170%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10B%TI=Z%II=I%TS=A)OPS
OS:(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST1
OS:1NW7%O6=M5B4ST11)WIN(W1=7C70%W2=7C70%W3=7C70%W4=7C70%W5=7C70%W6=7C70)ECN
OS:(R=Y%DF=Y%T=40%W=7D78%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=
OS:0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RU
OS:CK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.45 seconds
```

You need to submit a table summarizing the following (please add more rows if required):

IP Address of the VMs	Open Ports	Service Versions	Operating System Detection	Backend Software Information
Host 1: 192.168.10.2	53/tcp 80/tcp 443/tcp	Domain Http ssl/http	FreeBSD	Generic dns response: refused Nginx Nginx
Host 2: 192.168.10.13	8080/tcp 8009/tcp	Http asl/http	Linux	Splunkd httpd Splunkd httpd
Host 3: 192.168.10.18	21/tcp 22/tcp	Ftp ssh	Linux	Vsftpd openssh
Host 4: 192.168.10.19	135/tcp 139/tcp 445/tcp	msrpc Netbios-ssn microsoft-ds	Microsoft Windows	Microsoft Windows RPC Microsoft windows netbios-ssn

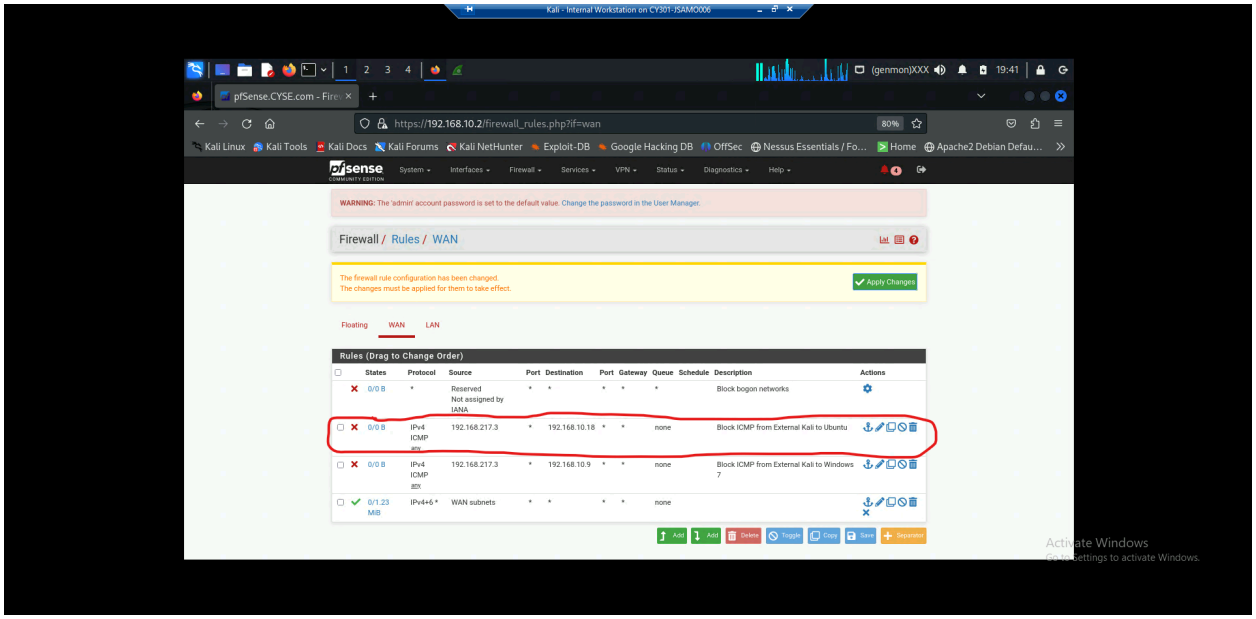
Using the command sudo nmap -sV with the combination of the IP addresses of the VMs, I was able to find that host 1 has open ports: 53/tcp, 80/tcp, and 443/tcp. Host 2 has open ports 8080/tcp and 8009/tcp. Host 3 has open ports 21/tcp and 22/tcp. Host 4 has 135/tcp, 139/tcp, and 445/tcp. Also using the command sudo nmap -sV with the combination of the IP address I was able to find that the service versions for host 1 were Domain, Http, and ssl/http. Host 2 service versions were http and asl/http. Host 3 versions were ftp and ssh. Host 4 versions were msrpc, Netbios-ssn, and microsoft-ds. Using the same command I was able to find the backend software information for each host. Using the command sudo nmap -O I was able to find the operating systems of each host. Host 1 is FreeBSD, host 2 is Linux, host 3 is Linux, and host 4 is Microsoft Windows. These commands are useful for attacker kali to gather information on a target before trying to attack it. It helps attacker kali understand what is exposed and where a weakness could possibly be.

Task B: Shield – Protect your network with a firewall (10 + 15+ 15 + 20 = 60 points) In order to receive full credits, you need to fill the table (add more rows if needed), implement the firewall rule(s), attach the screenshot of your rule

configured in the firewall table, and attach the screenshot of the rule and the Ping test verification of the rules.

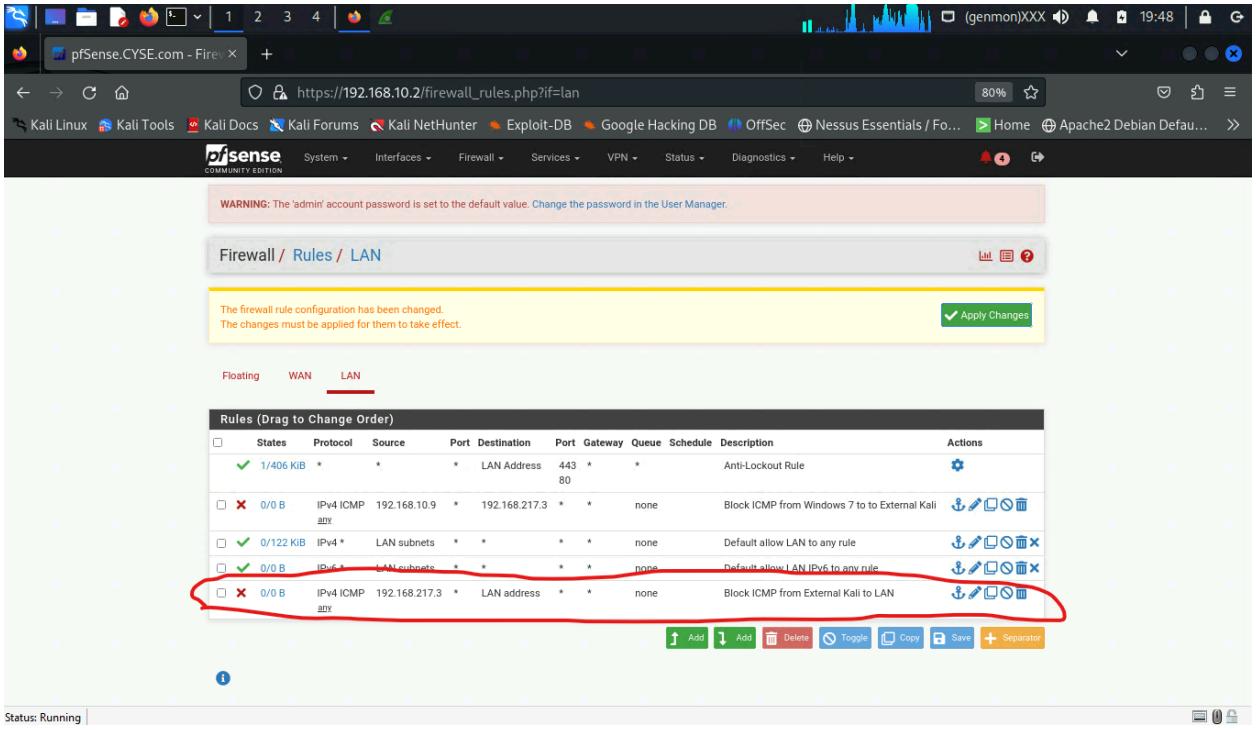
Important: Open Pfsense using a browser on the Internal Kali.

1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to the Ubuntu VM.



Rule #	Interface	Action	Source IP	Destination IP	Protocol
2	WAN	Block	192.168.217.3	192.168.10.18	IPv4 ICMP

2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

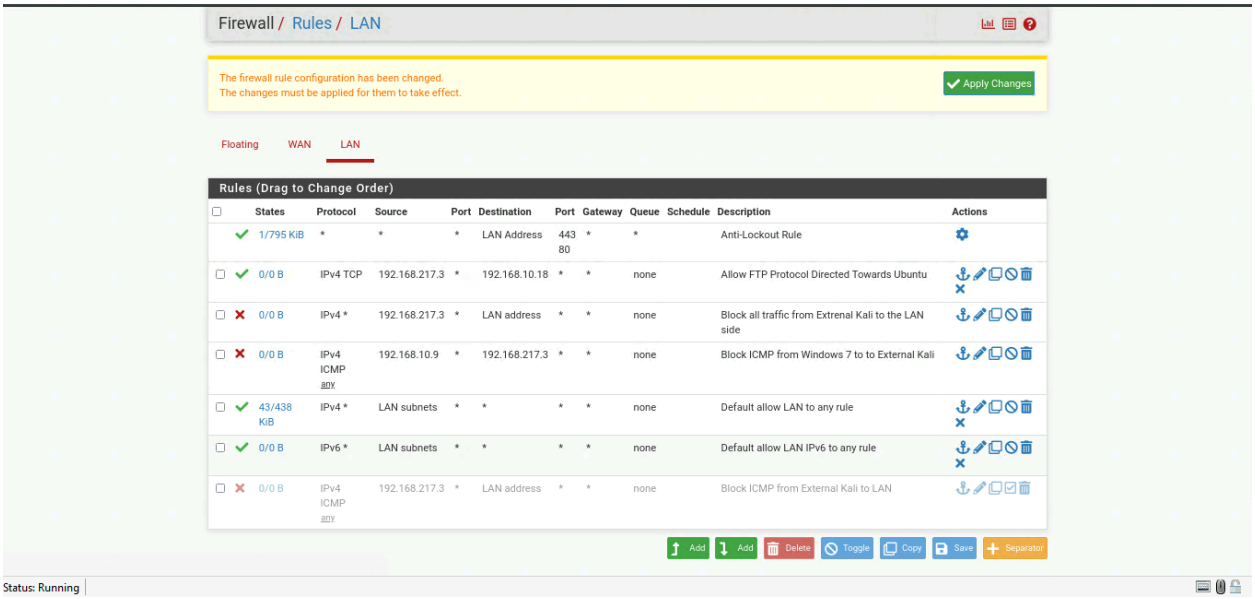


Rule #	Interface	Action	Source IP	Destination IP	Protocol
5	LAN	Block	192.168.217.3	LAN address	IPv4 ICMP

Add your Reflection

Blocking ICMP reduces reconnaissance and prevents attackers from using ping to look at the weaknesses of live hosts. It also makes network mapping harder for the attackers. It also limits scanning techniques because some tools are able to use ICMP to identify active systems before deeper scans. Blocking ICMP can slow down automated scans. It can also prevent ICMP or ping floods as well as some forms of smurf attacks. In this case, the firewall rule will protect Ubuntu and internal kali from the attacker kali. There are also some disadvantages of blocking ICMP such as pinging won't work for connectivity testing, and traceroute could fail or give incomplete paths. Blocking ICMPs can cause slow or broken connections especially VPNs and HTTPS. Attackers are also still able to scan using TCP/UDP even if ICMP is blocked. When configuring pfSense there needs to be a way for the user to allow necessary ICMP type while also blocking unnecessary or risky ICMP types.

3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol directed towards Ubuntu. You can add more rows in the table here, if necessary.



Rule #	Interface	Action	Source IP	Destination IP	Protocol
2	LAN	Allow	192.168.217.3	192.168.10.18	IPv4 FTP
3	LAN	Block	192.168.217.3	LAN address	IPv4*

4. Keep the firewall policies you created in Task B.3 and repeat Task A.1 to rescan the subnet using nmap in External Kali. Now, compare the results/ findings, and complete the following table and add your reflection as asked here.

	Before firewall Rules	After Firewall Rules
Host 1	Open Ports: 53/tcp 80/tcp 443/tcp OS Detection Accuracy: Just Guessing Service Enumeration: Domain Http	Blocked Ports: 53/tcp OS Detection Accuracy: Just Guessing Service Enumeration: Domain Http Https

	ssl/http	
Host 2	Open Ports: 8080/tcp 8009/tcp OS Detection Accuracy: Just Guessing Service Enumeration: Http asl/http	Blocked Ports: None OS Detection Accuracy: No exact OS Matches Service Enumeration: Http ssl/http
Host 3	Open Ports: OS Detection Accuracy: Just Guessing Service Enumeration: Ftp ssh	“Host seems down”
Host 4	Open Ports: OS Detection Accuracy: Just Guessing Service Enumeration: msrpc Netbios-ssn microsoft-ds	Blocked Ports: None OS Detection Accuracy: Just Guessing Service Enumeration: msrpc Netbios-ssn microsoft-ds

Write in your own words (~ 200 words) explaining:
a. Why does Nmap show “filtered” instead of “closed”, if there is any.
b. How firewall behavior affects scan results
c. What information is hidden from attackers

My results didn’t show any “filtered” but it would show filtered instead of closed when it can’t determine if the port is open due to the firewall blocking the traffic. It makes it harder for attackers to see what exactly is defending against them which is good for security reasons. Firewall should directly change what nmap is able to see. Firewalls can leave ports open, closed, or filtered. Open allows traffic and scanners to see service running. Closed is when the firewall allows traffic but no service is listening. Filtered means that the firewall blocks traffic silently and the scanner gets no response. The firewall can also affect the ICMP handling. If the ICMP is blocked the host discovery scans may show as shown but TCP scans can still show open ports. Implementing firewall rules does a more precise job of defending a user and its systems from an attacker that might want to ping their device for reconnaissance. It is hard for an attacker to tell if a service exists, the port is closed, or the firewall is blocking it and they will only see “filtered”. The reason that the attacker can’t access or see the open ports is so that they are unable to trace what is preventing their attempt at an attack.