

Forum:[Hack Forums](#)

Thread: [\[TUT\] Bypassing Firewalls/IPS \[TUT\] \[SAMARITANS\]](#)

Play Boy - May 9, 2018, 4:03 pm

Hello everyone,

This will be a short guide on bypassing firewalls and/or a intrusion prevention system. To start, I'll explain what a firewall is and what it does.

A firewall is either a software integrated or hardware integrated security tool used to prevent unwanted traffic from reaching a specific network or host. Firewalls do this by inspecting the data packets destined for a network or host and determines, based off a set of created rules, whether to drop the data or to allow the data in. That being said, a correctly configured firewall/IPS will be close to impossible to bypass and other routes of exploitation are necessary.

But say I want to get data past this annoyance and the firewall/IPS isn't correctly configured. This is where things get interesting.

For the entire guide; I will be using nmap as my tool in examples.

Spoofing your IP or MAC address:

`nmap -sS -S <IP_address> or nmap -sS --spoof-mac <MAC address>`

Spoofing your IP/MAC can bypass rules in place that only allow traffic in from specific destinations. Obviously you won't run into this a lot as it's easily bypassed but it can be fairly challenging finding IP/MAC addresses that are allowed in the network.

Add extra data:

`nmap -sS --data`

Adding extra data to your packet is a great way of bypassing firewalls that expect to be port scanned but are poorly configured. When performing a port scan or even pinging a host; the amount of data sent is very little which can trigger some firewalls. If these packets contained more data; perhaps the firewall wouldn't care as much.

TTL (Time to live):

`nmap -sS --ttl <time>`

Certain firewalls detect the default nmap scans based off the time to live the packets have. If you

want to be stealthy; it's a good idea to change this as security savvy sys admins who have observed an nmap packet will set this rule in place.

Spoof Source port:

```
nmap -sS -g <port>
```

Spoofing your source port is good to confuse firewalls that are destined to block all but some certain ports. For example, if a firewall is only allowing port 80 traffic in and blocking traffic on the rest; spoofing your source port as 80 would easily bypass this.

Slow down requests:

```
nmap -sS --scan-delay <number>
```

Slowing the rate at which probing packets are sent to a firewall can greatly improve your chances of remaining stealthy and bypassing the firewall. Few firewalls have rules in to either drop traffic of the same type that's being sent to multiple ports at once or alert the sys admin of such behavior. Both of these are bad for us.

Fragmenting packets:

```
nmap -sS -f
```

Fragmenting packets rarely works in my opinion but it's worth the shot to see if this will allow access behind a firewall. Fragmenting occurs by splitting the data packet apart in order to bypass rules denying specific data.

Conclusion:

Firewalls can be a great way to protect yourself if configured correctly but can also be a great headache to bypass. A correctly configured and monitored firewall is a pain to deal with and is not worth the time to figure out all the rules it may have. Your best bet would be to find a vulnerability around the firewall at that point such as the user. My last bit of advice would be to stray as far away from the default nmap scan as possible. As EasyGhost informed me, most firewalls will try to drop a packet based off the default UserAgent an nmap scan produces.

CyberStrike - May 9, 2018, 8:01 pm

Hey good tutorial it's amazing how tweaking packets or just tweaking the order of packets can get around various solutions.

Play Boy - May 9, 2018, 8:33 pm

(May 9, 2018 08:01 PM)sirru5h Wrote: [\[CITE\]](#) Hey good tutorial it's amazing how tweaking packets or just tweaking the order of packets can get around various solutions.

Thanks! Yes, most intrusion prevention devices are designed in ways to stop most default rules but changing even the slightest setting can change that.

CYB3RM4N - May 9, 2018, 8:40 pm

Great read; brief but informative.

Nice visuals too! ?

CyberStrike - May 9, 2018, 9:16 pm

I remember back in the day to get a payload past fw/IDS you used to say send the third packet maybe send packet 1 with a bad checksum then packet 2 can have no data send packet 4 legit then resent packet 1 with a good checksum then packet 2 you resend the legit data and a bad checksum, really old technique. It worked because packet 3 would have a snippet of code then packet 1 is only declined due to the checksum but still kept when have the good checksum it accepts the original packet as good then packet 2 it will add the new data and go with the valid checksum. Odd balled stuff used to work back when the perimeter was not so well defended.