

Forum:[Hack Forums](#)

Thread: [Theoretical Methodology for Detecting ICMP Reflected Attacks: SMURF Attacks](#)

chintanmandexgurjar - March 22, 2014, 4:43 am

There are plenty of different ways to track the original source of a DoS attack, but those techniques are not efficient enough to track a reflected ICMP attack. When I say “reflected ICMP attack,” that means a SMURF attack. Here I am going to show you a new model to trackback the reflective DOS attack caused by ICMP packets. This is a very efficient method, because you can do this with the help of a really few attack packets. We have seen that, to detect ICMP attacks in direct attack, we need a large amount of packets to be revised, which is not true in this case.

Introduction

In this digital era, it is really difficult to protect your network from DOS attack. Big brands have faced this type of attacks even if they secured their network. It is the responsibility of the host that they send and receive packets from their network to the client and vice versa. It destination's responsibility to receive and verify the packet's validity sent by the source.

Attack Classification

There are two types of attacks.

Direct attacks

Indirect/reflective attacks

A direct attack is explained by its name: Packets are sent directly to the victim. However, in a reflective attack, the packets are sent to the intermediate network and then they goes to the victim. This intermediate network can be a custom proxy or a custom network. a SMURF attack is an example of reflective attack. The attacker sends ICMP echo packets to the network; that is called an amplifier. This is done by using the source address, which is the IP address of a victim. Finally, the machine will send the reply to a victim machine. This thing is illustrated in the figure below.

[img]http://resources.infosecinstitute.com/wp-content/uploads/031414_1600_Theoretical1.png[img]

How many replies it will get depends on the number of machines connected to that amplifier network. This attack is easy to implement and hard to detect because a single identity can attack a large enterprise, even using only very few machines or resources. Now I am going to show you a new theoretical method to track back the reflective ICMP flood attack.

For back-tracking ICMP reflective packets, we have to understand the following terms;

1. Packet Marking

This is a very basic approach, in which the router itself adds some information to the packet. By doing this, the router can locate the source of the flow of a packet. This router adds the IP address to the packet header of any packet. The victim constructs the attack path after receiving the marking. That marking is the address of the router that lies between the attacker and the victim. In this case, the victim will need a ton of packets in order to reconstruct a path. To accomplish this

process, both the single router and participating routers will need multiple packets to transmit on its own IP address.

[img]http://resources.infosecinstitute.com/wp-content/uploads/031414_1600_Theoretical2.png[/img]
2. ICMP Traceback

In this, the reconstructed path is generated by sending the out-of-band traceback details to the destination by a router. There is an old method named iTrace, in which the router sends ICMP echo packets to the destination with an attack path. Due to this, those packets contain details about the marking router. The victim traces back the information after collecting those ICMP packets. Then the victim reconstructs the attack path.

In this approach, routers send out-of-band traceback information to the destination of the flow to reconstruct the attack path. Bellovin proposed iTrace [15]. Routers send ICMP packets, along with the attack path, to another destination. The ICMP packets contain information about the marking router. The victim collects the ICMP packets during the attack and extracts traceback information. The victim will be able to reconstruct the attack path.

With this new method, fewer signaling packets are used to send to the destination. Whatever studies have been done up to now don't deal with the reflective attacks. These methods are only dealing with direct attacks.

Problems Faced During the Traceback

In packet logging, the hash value will be different after reflection, so in that case the traceback approach is not useful.

In packet marking, the identification field will be different after any reflection. On top of that, a marking will be received by the victim only after a successful reflection so, in that case, traceback is also not helpful.

In the traditional ICMP traceback method, packets that will be received by the victim contain only path information between the amplifier network and the victim, so no legitimate and proper real information about the attacker will be there.

Trackback ICMP Attacks

ICMP echo packets are only echo request-and-reply packets. This is a novel approach for tracing back the ICMP packets, whether they are direct or indirect packets. It's a new marking method. In this method, the data field carries all of the tracing back information. Researchers noticed that the ICMP protocol's behavior remains the same after request and response. In this method, the machine responds with the exact data field contained in the request after receiving the request which also contains the same data field. So, if there is any change in the data field, it will be known by both the receiver and sender. Therefore, packets are sent with this new marking technique, which is explained below.

If a machine receives an ICMP echo request, it will respond with the same data field contained in the echo request. So any modification in the data field, whether in the request or the reply, will be received by the destination. In an ICMP direct attack, the attacker will flood the victim either with ICMP requests or with reply messages with our marking for every ICMP echo packet:

In this methodology, it does not matter whether the packet is direct or reflective. Using this

technique, the marking router will insert the address in the data field in the ICMP message in request as well as in the response. Due to the remaining unchanged data field, the victim will get all traceback information that is related to path between the middle amplifier network as well as attacker.

Problem with this approach. A single packet gets passed by 15 or more different routers. This requires a large amount of space to store the marking of all the routers' information. We have limited space for traceback information storage.

Solution. Researchers used probabilistic technique to note down a complete path starting from the attacker and ending to the destination in a proper flow. The victim gets various IP addresses during any attack. Now he will have to reconstruct the attack path. In order to do that, the router copies various TTL fields, with their respective IP addresses, into the data field. To differentiate between echo requests and echo replies, the router uses different bits of TTL. After that, the victim uses these all bits in order to construct the attack path. This scenario is explained in the figure below.

[img]http://resources.infosecinstitute.com/wp-content/uploads/031414_1600_Theoretical3.png[/img]
Practical Implementation

Up to now, I have talked about the theoretical technique. In real life, practical implementation should be done as shown in the figure below. Researchers proposed this method of implementing this in a virtual environment by using five routers, three reflectors, and a victim and attacker machine, as shown in the figure. One packet travels from the attacker to the victim, but a necessary condition is that the packet must travel through all the routers that are implemented in the virtual lab.

[img]http://resources.infosecinstitute.com/wp-content/uploads/031414_1600_Theoretical4.png[/img]
]

Here all machines are using Linux systems and the routers are also allowing packet forwarding mechanism in order to get the marking of each and every ICMP echo request and reply packets. Then a SMURF attack is launched, in which the attacker sends packets to a victim; the packets are passed through all routers. Each router's responsibility is to mark all packets with their respective TTL and IP addresses. After that, the receiver receives all the packets, analyzes them, and reconstructs the origin of the attack path. Thus, we can trace back the reflective ICMP attacks by using very few packets.

Conclusion

Using this technique, one can trace back ICMP DoS attacks, including direct and reflective attacks as well. Reflective attacks are known as SMURF attacks.

Source

Guerid, H.; Serhrouchni, A.; Achemlal, M.; Mittig, K., "A Novel Traceback Approach for Direct and Reflected ICMP Attacks," Network and Information Systems Security (SAR-SSI).

Chao G & Kamil S. IP Traceback Based on Packet Marking and Logging.

Storm- - March 22, 2014, 4:50 pm

(Mar 22, 2014 01:55 PM)DrDinosaur Wrote: [\[CITE\]](#) I knew the title was too good to be coming originally from someone on HF.

At least he put the source at the bottom and didn't try to hide it :P.

chintanmandexgurjar - March 23, 2014, 2:42 am

is this a +ve reply of negative !! i am still confused

_Silky - March 23, 2014, 3:47 am

(Mar 23, 2014 02:42 AM)chintanmandexgurjar Wrote: [\[CITE\]](#) is this a +ve reply of negative !! i am still confused

Lol wha? It's from InfosecInstitute", they're good teachers..

pwntoken - March 23, 2014, 8:15 am

Code

[img]http://resources.infosecinstitute.com/wp-content/uploads/031414_1600_Theoretical4.png[img]
is broken, fix it, thanks. And a great read.