RESULTS AND RECOMMENDATIONS

Severity	Description
High	Security vulnerabilities that can give an attacker total or partial control over a system or allow access to or manipulation of sensitive data.
Medium	Security vulnerabilities that can give an attacker access to sensitive data but require special circumstances or social methods to fully succeed.
Low	Security vulnerabilities that can have a negative impact on some aspects of the security or credibility of the system or increase the severity of other vulnerabilities, but which do not by themselves directly compromise the integrity of the system.
Info.	Informational findings are observations that were made during the assessment that could have an impact on some aspects of security but in themselves do not classify as Security vulnerabilities.

Vulnerability	High	Medium	Low	Info.
Backdoor in unrealIRCd	X			

Table 2: identified vulnerabilities

Backdoor in unrealircd

Severity high:

Background

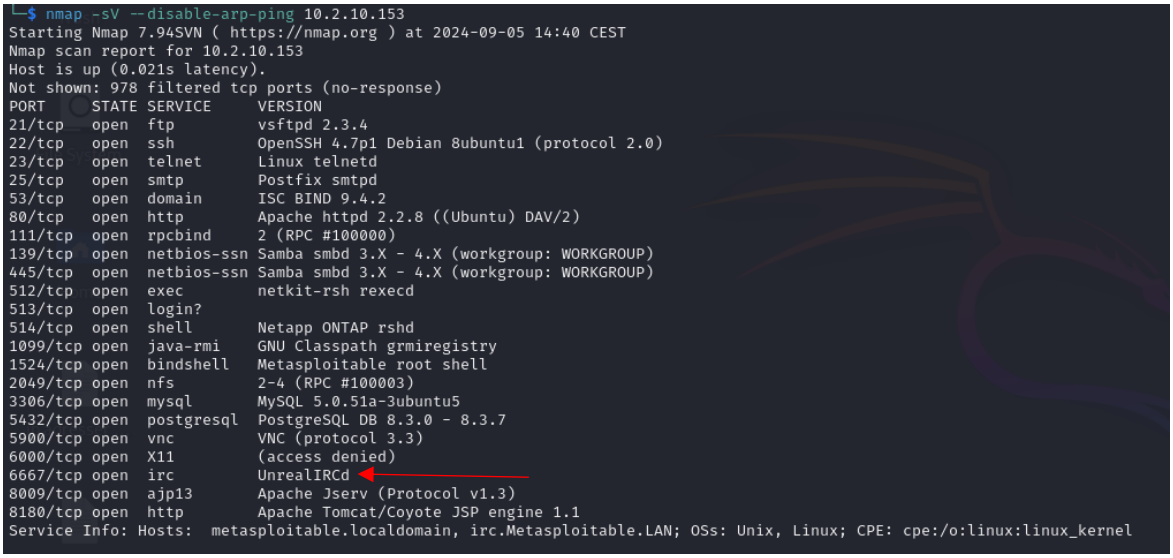
When testing one of the servers in the network a backdoor was found. A backdoor is a typically covert method of bypassing normal authentication or encryption. Backdoors are most often used for securing remote access to a computer or obtaining access to plaintext in cryptosystems. From there it may be used to gain access to privileged information like passwords, corrupt or delete data on hard drives, or transfer information within autoschediastic networks.

Description

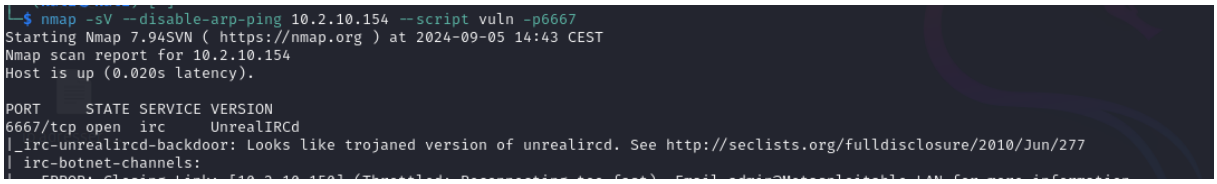
The tested server 10.2.10.153 was using a version of unrealIRCd (version 3.2.8.1) that is known to be a trojaned version. Meaning that running a modified script would potentially allow an remote attacker to get access to customer data and functionalities. The backdoor has been previously proven and documented in cve-2010-2075
https://nvd.nist.gov/vuln/detail/CVE-2010-2075

unrealIRCd is an irc server. Irc is a text-based chat system for instant messaging giving users the possibility to communicate in forums or private messages with each other.

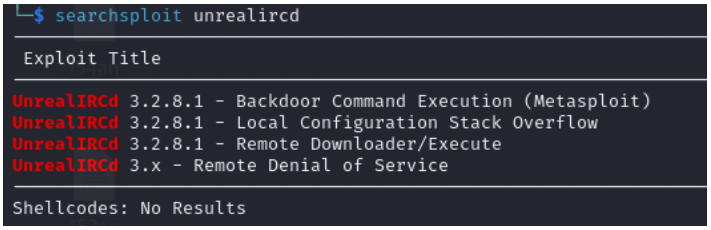
The backdoor was only accessible in a version of unrealIRCd that came preconfigured with it and was available for download between 2009 and 2010 meaning that everyone running UnrealIRCd from this period is likely to have the backdoor installed. The backdoor is located in the DEBUG3_DOLOG_SYSTEM macro. The severity of the backdoor is high as it might allow an attacker to get full root access. The exploit can be used even without great knowledge as it is available as a ready-made script via programs that specifically target penetration of software making the severity higher as the exploit is easily obtainable.



running an scan on the network confirms that UnrealIRCd is running using port 6667.



Further scanning focusing on port 6667 that we can see UnrealIRCd is using confirms that the version running most likely is trojaned.



Using a searchengine for known exploit we can find preconfigured scripts that will allow an attacker to gain access to the backdoor. This also show us that other exploitations are available and can be used for this aplication such as ddos-attacks (distributed denial of service) that overworks the server resulting in a crash.

```
print_status("Connected to #{rhost}:#{rport}...")
banner = sock.get_once(-1, 30)
banner.to_s.split("\n").each do |line|
        print_line("    #{line}")
end

print_status("Sending backdoor command...")
sock.put("AB;" + payload.encoded + "\n")

handler
disconnect
```

Examining the code for the exploit shows that sending a request to the program and putting "AB;" in front of a payload will have the program execute the payload. The payload can be configured to contain anything the attacker want but is most likely set to establish a new user or get info on all available user with their password. Creating a new user and elevate it would give the attacker root privilege.

Recommendations

The backdoor for unrealIRCd 3.2.8.1 have been patched out in later versions of the program. Updating the program to a newer version should fix the problem. Further recommendations is to verify that the integrity of all users and files is untouched and that no one have been manipulating them or gained access to them before patching. If patching to a newer version for some reason is not possible then the code should be checked and the backdoor removed from it. UnrealIRCd is open source meaning it is possible to make change to it at will. This should in no way affect the overall performance of the program.