Nipper

Cisco Router Security Report

of the

R3 Cisco Router

Contents

---

1. About This Report

1.1. Organisation

This Cisco Router R3 report was produced by Nipper on Tuesday 30th July 2024. The report contains the following sections:

- a security audit report section that details any identified security-related issues. Each security issue includes a description of the issue, its impact, how easy it would be to exploit and a recommendation. The recommendations include, where appropriate, the command(s) to resolve the issue;
- a configuration report section that details the configuration settings;
- an abbreviations appendix section that expands any abbreviations used within the report;
- a common ports appendix section that details the TCP and UDP port numbers for the common services outlined within the report;
- an appendix section detailing the logging severity levels used by the logging facility;
- a time zones appendix section that details a number of the most commonly used time zones;
- an appendix section detailing the software used to produce this report.

1.2. Conventions

This report makes use of the text conventions outlined in Table 1.

Convention	Description
`command`	This text style represents the Cisco Router command text that has to be entered literally.
`string`	This text style represents the Cisco Router command text that the you have to enter.
`[ ]`	Used to enclose a Cisco Router command option.
`{ }`	Used to enclose a Cisco Router command requirement.
`|`	Divides command option or requirement choices.

Table 1: Report text conventions

---

2. Security Audit

2.1. Introduction

Nipper performed a security audit of the Cisco Router R3 on Tuesday 30th July 2024. This section details the findings of the security audit together with the impact and recommendations.

2.2. Inbound TCP Connection Keep Alives

Observation: Connections to a Cisco Router device could become orphaned if a connection becomes disrupted. An attacker could attempt a Denial of Service (DoS) attack against a Cisco Router by exhausting the number of possible connections. Transmission Control Protocol (TCP) keep alive messages can be configured to confirm that a remote connection is valid and then terminate any orphaned connections.

Nipper determined that TCP keep alive messages are not sent for connections from remote hosts.

Impact: An attacker could attempt a DoS by exhausting the number of possible connections.

Ease: Tools are available on the Internet that can open large numbers of TCP connections without correctly terminating them.

Recommendation: Nipper recommends that TCP keep alive messages be sent to detect and drop orphaned connections from remote systems. TCP keep alive messages can be enabled for connections from remote systems using the following command:

```
service tcp-keepalives-in
```

2.3. Connection Timeout

Observation: Connection timeouts can be configured for a number of the device services. If a timeout were configured on an administrative service, an administrator that did not correctly terminate the connection would have it automatically closed after the timeout expires. However, if a timeout is not configured, or is configured to be a long timeout, an unauthorised user may be able to gain access using the administrator's previously logged-in connection.

Nipper identified three connection settings that were not configured to timeout within ten minutes, these are listed in Table 2.

Connection	Timeout
Console line 0	No Timeout
Auxiliary line 0	No Timeout
VTY lines 0 to 4	No Timeout

Table 2: Connections with inadequate timeout periods

Impact: An attacker who was able to gain access to a connection that had not expired, would be able to continue using that connection. A connection could be a console port on the device that was not correctly terminated or a remote administrative connection.

Ease: The attacker would have to gain physical access to the device to use the console port, or gain remote access to an administration machine that is attached to the port. To gain access to remote connections, an attacker would have to be able to intercept network traffic between the client and R3. The attacker would then have to take over the connection, which could be very difficult with some services. Tools are available on the Internet that would facilitate the monitoring of network connections.

Recommendation: Nipper recommends that a timeout period of ten minutes be configured for connections to the device R3.

2.4. Auxiliary Port

Observation: The auxiliary port's primary purpose is to provide a remote administration capability. It can allow a remote administrator to use a modem to dial into the Cisco device.

Nipper determined that the auxiliary port on the Cisco device R3 allowed exec connections and did not appear to have the callback feature configured.

Impact: An attacker may discover the modem number for the device during a war-dial. If an attacker were able to connect to the device remotely, then they may be able to brute-force the login to gain access to the device.

Ease: The attacker would have to first identify the telephone number of the device, probably through a war-dial. A modem attached to a telephone line would have to be attached directly to the Cisco device's auxiliary port. Then the attacker would be able to attach to the device in order to perform a brute-force of the login.

Recommendation: Nipper recommends that, if not required, the auxiliary port exec be disabled. Exec can be disabled on the aux port with the following command:

```
no exec
```

If the auxiliary port is required for remote administration, the callback feature can be configured to dial a specific preconfigured telephone number.

2.5. IP Source Routing

Observation: IP source routing is a feature whereby a network packet can specify how it should be routed through the network. Cisco routers normally accept and process source routes specified by a packet, unless the feature has been disabled.

Nipper determined that IP source routing was not disabled.

Impact: IP source routing can allow an attacker to specify a route for a network packet to follow, possibly to bypass a Firewall device or an Intruder Detection System (IDS). An attacker could also use source routing to capture network traffic by routing it through a system controlled by the attacker.

Ease: An attacker would have to control either a routing device or an end point device in order to modify a packets route through the network. However, tools are available on the Internet that would allow an attacker to specify source routes. Tools are also available to modify network routing using vulnerabilities in some routing protocols.

Recommendation: Nipper recommends that, if not required, IP source routing be disabled. IP source routing can be disabled by issuing the following Internet Operating System (IOS) command:

```
no ip source routing
```

2.6. Telnet

Observation: Telnet is widely used to provide remote command-based access to a variety of devices and is commonly used on network devices for remote administration. However, Telnet is a clear-text protocol and is vulnerable to various packet capture techniques.

Nipper determined that Telnet was enabled on R3.

Impact: An attacker who was able to monitor network traffic could capture sensitive information or authentication credentials.

Ease: Network packet and password sniffing tools are widely available on the Internet and some of the tools are specifically designed to capture clear-text protocol authentication credentials. However, in a switched environment an attacker may not be able to capture network traffic destined for other devices without employing an attack such as Address Resolution Protocol (ARP) spoofing.

Recommendation: Nipper recommends that, if possible, Telnet be disabled. If remote administrative access to the device is required, Nipper recommends that Secure Shell (SSH) be configured. The Telnet service can be disabled on individual lines with the following command:

```
transport input none
```

The following Cisco IOS command can be used to disable Telnet on individual lines, but enable SSH:

```
transport input ssh
```

2.7. ICMP Redirects

Observation: Internet Control Message Protocol (ICMP) redirect messages allow systems to change the route that network traffic takes. On networks with functional network routing, disabling ICMP redirects will have little to no effect. ICMP redirects are usually enabled by default on Cisco devices.

Nipper determined that the device R3 had support for ICMP redirects enabled on the network interfaces listed in Table 3.

Interface	Description
FastEthernet0/0	
FastEthernet1/0	

Table 3: Interfaces with ICMP redirects enabled

Impact: An attacker could use ICMP redirect messages to route network traffic through their own router, possibly allowing them to monitor network traffic.

Ease: Tools are widely available that can send ICMP redirect messages.

Recommendation: Nipper recommends that, if not required, ICMP redirects be disabled on all network interfaces. ICMP redirects can be disabled on each individual network interface using the following command:

```
no ip redirects
```

2.8. Access Control Lists

Observation: Access Control List (ACL) are sequential lists of allow and deny Access Control Entries (ACE) that specify whether network traffic should be allowed or dropped. ACLs are used to restrict access to services and network devices, preventing access to services and devices that should not be accessible.

Nipper identified seven security-related issues with the configured ACL, these are listed in Table 4.

ACL	Line	Description
1	1	Allows access from a network source.
1	2	Allows access from a network source.
1	N/A	ACL does not end with a deny and log.
100	1	Allows access from a network source to any address. Allows access from 192.168.11.0 / 0.0.0.255 to any destination. Allows access from 192.168.11.0 / 0.0.0.255 to any destination service.
100	N/A	ACL does not end with a deny all and log.

Table 4: Insecure Access Control Entries

Impact: If ACEs are not sufficiently restrictive, an attacker may be able to access services or network devices that should not be accessible. Furthermore, an attacker who had compromised a device could install a backdoor which could listen on a network port that was not filtered.

Ease: N/A

Recommendation: Nipper recommends that the ACLs be reviewed and, where possible, modified to ensure that:

- ACE do not allow access from any source;
- ACE do not allow access from entire source networks;
- ACE do not allow access to any destination;
- ACE do not allow access to entire destination networks;
- ACE do not allow access to any destination port;
- ACE log denied access;
- ACL end with a deny all and log.

However, in certain circumstances, such as a public web server, a more relaxed configuration may be required to allow any host to access specific hosts and services.

2.9. Proxy ARP

Observation: ARP is a protocol that network hosts use to translate network addresses into media addresses. Under normal circumstances, ARP packets are

confined to the sender's network segment. However, a Cisco router with Proxy ARP enabled on network interfaces can act as a proxy for ARP, responding to queries and acting as an intermediary.

Nipper identified two interfaces that had Proxy ARP enabled. These are listed in Table 5.

Interface	Description
FastEthernet0/0	
FastEthernet1/0	

Table 5: Interfaces with Proxy ARP enabled

Impact: A router that acts as a proxy for ARP requests will extend layer two access across multiple network segments, breaking perimeter security.

Ease: A Cisco device with Proxy ARP enabled will proxy ARP requests for all hosts on those interfaces.

Recommendation: Nipper recommends that, if not required, Proxy ARP be disabled on all interfaces. Proxy ARP can be disabled on each interface with the following Cisco IOS command:

```
no ip proxy-arp
```

2.10. Cisco Discovery Protocol

Observation: Cisco Discovery Protocol (CDP) is a proprietary protocol that is primarily used by Cisco, but has been used by others. CDP allows some network management applications and CDP aware devices to identify each other on a Local Area Network (LAN) segment. Cisco devices, including switches, bridges and routers are configured to broadcast CDP packets by default. The devices can be configured to disable the CDP service or disable CDP on individual network interfaces.

Nipper determined that the CDP service had not been disabled, and additionally, had not been disabled on all the active network interfaces.

Impact: CDP packets contain information about the sender, such as hardware model information, operating system version and IP address details. This information would allow an attacker to gain information about the configuration of the network infrastructure.

Ease: CDP packets are broadcast to an entire network segment. An attacker could use one of the many publicly available tools to capture network traffic and view the leaked information.

Recommendation: Nipper recommends that, if not required, the CDP service be disabled on the Cisco device R3. If CDP is required, Nipper recommends that CDP be disabled on all interfaces except those that are explicitly required.

The CDP service can be disabled by issuing the following Cisco IOS command:

```
no cdp run
```

CDP can be disabled on individual interfaces using the following command:

```
no cdp enable
```

In some configurations with IP phones, deployed using either Auto Discovery or Dynamic Host Configuration Protocol (DHCP), the CDP service may need to be enabled. In this situation CDP should be disabled on all network interfaces for which it is not required.

2.11. Classless Routing

Observation: Classless routing is enabled by default on Cisco routers. If a router has classless routing enabled and it receives a network packet for which there is no configured route, the router will forward the packet to the best destination. With classless routing disabled, the router would discard any network traffic for which no route is defined.

Nipper determined that classless routing was enabled on R3.

Impact: Network traffic that should not be routed by the router may be routed when classless routing is enabled.

Ease: N/A

Recommendation: Nipper recommends that, if possible, classless routing be disabled. Classless routing can be disabled with the following command:

```
no ip classless
```

2.12. Minimum Password Length

Observation: Cisco introduced an option from IOS version 12.3(1) which forces user, enable, secret and line passwords to meet a minimum length. This setting was introduced to help prevent the use of short passwords such as "cisco".

Nipper determined that a minimum password length of six characters was configured.

Impact: With a small minimum password length configured, it would be possible for a short password to be used. If an attacker were able to gain a password through dictionary-based guessing techniques or by a brute-force method, the attacker could gain a level of access to R3.

Ease: A number of dictionary-based password guessing and password brute-force tools are available on the Internet.

Recommendation: Nipper recommends that a minimum password length of at least eight characters be configured. The minimum password length can be configured with the following command:

```
security passwords min-length {length}
```

2.13. BOOTP

Observation: BOOTstrap Protocol (BOOTP) is a datagram protocol that allows compatible hosts to load their operating system over the network from a BOOTP server. Cisco routers are capable of acting as BOOTP servers for other Cisco devices and the service is enabled by default. However, BOOTP is rarely

used and may represent a security risk.

Nipper determined that BOOTP was not disabled. However, it is worth noting that not all Cisco devices support BOOTP.

Impact: An attacker could use the BOOTP service to download a copy of the router's IOS software.

Ease: Tools are available on the Internet to access BOOTP servers.

Recommendation: Nipper recommends that, if not required, the BOOTP service be disabled. The following command can be used to disable BOOTP:

```
no ip bootp server
```

2.14. IP Unreachables

Observation: ICMP IP unreachable messages can be generated by a Cisco device when a host attempts to connect to a non-existent host, network, or use an unsupported protocol. ICMP IP unreachable messages will let the connecting host know that the host, network or protocol is not supported or cannot be contacted. Therefore, the host does not have to wait for a connection time-out. ICMP IP unreachable messages are normally enabled by default on Cisco devices and must be explicitly disabled.

Nipper determined that the Cisco device R3 had ICMP IP unreachable messages enabled on the interfaces listed in Table 6.

Interface	Description
FastEthernet0/0	
FastEthernet1/0	

Table 6: Interfaces with IP unreachables enabled

Impact: An attacker who was performing network scans to determine what services were available would be able to scan a device more quickly.

Ease: Tools are available on the Internet that can perform a wide variety of scan types.

Recommendation: Nipper recommends that, if not required, IP unreachables be disabled on all network interfaces. However, whilst disabling IP unreachables will not stop scans, it does make it more difficult for an attacker. The IP unreachables option is disabled or enabled individually for each network interface. It can be disabled with the following command:

```
no ip unreachables
```

2.15. Service Password Encryption

Observation: Cisco service passwords are stored by default in their clear-text form rather than being encrypted. However, it is possible to have these passwords stored using the reversible Cisco type-7 encryption.

Nipper determined that the Cisco device R3 was not running the password encryption service that helps provide a basic level of encryption to passwords that otherwise would be stored in clear-text.

Impact: If a malicious user were to see a Cisco configuration that contained clear-text passwords, they could use the passwords to access the device. However, an attacker who had access to a Cisco configuration file would easily be able to reverse the passwords.

Ease: Even though it is trivial to reverse Cisco type-7 passwords, they do provide a greater level of security than clear-text passwords. Tools are widely available on the Internet that reverse Cisco type-7 passwords.

Recommendation: Nipper recommends that the Cisco password encryption service be enabled. The Cisco password encryption service can be started with the following Cisco IOS command:

```
service password-encryption
```

2.16. Login Banner

Observation: A banner message can be shown to users who connect to one of the remote management services, such as Telnet. Typically banner messages will include information on the law with regard to unauthorised access to the device, warning users who do not have the authority to access the device about the consequences.

Nipper determined that no login banner was configured.

Impact: Attackers who have gained access to a device could avoid legal action if no banner is configured to warn against unauthorised access.

Ease: N/A

Recommendation: Nipper recommends that a banner be configured that warns against unauthorised access. Banners are configured on Cisco devices using a delimiter character. A delimiter character is specified in the banner command and is used again to mark the end of the banner. The Cisco command to add a login banner, that is presented to users prior to authentication, is:

```
banner login {delimiter} The banner text {delimiter}
```

2.17. Packet Assembler / Disassembler

Observation: The Packet Assembler / Disassembler (PAD) service enables X.25 connections between network systems. The PAD service is enabled by default on most Cisco IOS devices but it is only required if support for X.25 links is necessary.

Nipper determined that the PAD service had not been disabled.

Impact: Running unused services increases the chances of an attacker finding a security hole or fingerprinting a device.

Ease: N/A

Recommendation: Nipper recommends that, if not required, the PAD service be disabled. Use the following command to disable the PAD service:

```
no service pad
```

2.18. Conclusions

Nipper performed a security audit of the Cisco Router device R3 on Tuesday 30th July 2024 and identified 16 security-related issues. Nipper determined that:

- TCP keep alive messages are not configured for inbound connections;
- all connections were not configured with secure connection timeout periods;
- the AUX port was configured to allow EXEC connections without the callback functionality;
- IP source routing was enabled;
- clear-text remote administration was enabled using Telnet;
- ICMP redirects were not disabled for all network interfaces;
- insecure ACL were configured;
- ARP request proxying was not disabled on all network interfaces;
- CDP was not disabled;
- classless routing was enabled;
- an inadequate minimum password length was configured;
- BootP was enabled;
- IP unreachables have not been disabled on all interfaces;
- the service passwords are stored in clear-text;
- no login banner has been configured;
- the PAD service was enabled.

---

3. Device Configuration

3.1. Introduction

This section details the configuration settings of the Cisco Router device R3.

3.2. General

Description	Setting
Hostname	R3
IOS Version	12.4
Service Password Encryption	Disabled
Minimum Password Length	6 characters
IP Source Routing	Enabled
BOOTP	Enabled
Service Config	Disabled
TCP Keep Alives (In)	Disabled
TCP Keep Alives (Out)	Disabled
Cisco Express Forwarding	Enabled
Gratuitous ARPs	Disabled
Classless Routing	Enabled

Table 7: General device settings

3.3. Services

Service	Status
Telnet	Enabled
SSH	Enabled
HTTP	Disabled
Finger	Disabled
TCP Small Services	Disabled
UDP Small Services	Disabled
CDP	Enabled
PAD	Enabled

Table 8: Device services

3.4. Domain Name Settings

Description	Setting
Domain Name	dxc.intern
Domain Lookup	Disabled

Table 9: Domain name settings

3.5. Time Zone Settings

Description	Setting
Time Zone	UTC
UTC Offset	None
Summer Time Zone	Disabled
Authorative Time Source	No

Table 10: Time zone settings

Description	Setting

3.6. User Accounts and Privilages

Level	Password	Encryption
15	<unknown>	MD5

Table 11: Enable Passwords

Username	Privilage	Password	Encryption
admin	15	<unknown>	MD5

Table 12: User Accounts

3.7. Logging

Description	Setting
Logging	Enabled
Log Configuration Changes	Disabled
Console Logging	System Default
Console Logging Severity Level	Default
Syslog Logging	Enabled
Syslog Logging Severity Level	Informational (6)
Syslog Logging Facility	local7
Syslog Message Counting	System Default
Syslog Logging Server	message-counter
Buffer Logging	System Default
Buffer Size	Default
Buffer Logging Severity Level	Debugging (7)
Terminal Line Logging	Enabled
Terminal Line Logging Severity Level	Debugging (7)

Table 13: Logging configuration

3.8. Secure Shell

Description	Setting
SSH	Enabled
Protocol version	2
Login time-out	Default
Login retries	Default

Table 14: SSH configuration

3.9. HyperText Transfer Protocol

Description	Setting
HTTP Server	Disabled
Authentication Type	Enable Password
Access Class (Access List Number)	Unconfigured

Table 15: HTTP configuration

3.10. Routing

A network device's routing tables can be configured with static routes or updated dynamically. Routing protocols are used by network routing devices to dynamically update the routing tables that devices use to forward network traffic to their destination. Router protocols can be split into two different categories; Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs). IGPs are usually used in situations where the routing devices are all controlled by a single entity, such as within a company. EGPs are usually used in situations where routing devices are managed by a number of entities, such as the Internet. Typically routing devices support a number of standard routing protocols.

IP Address	Net Mask	Gateway
0.0.0.0	0.0.0.0	192.168.11.1
0.0.0.0	0.0.0.0	dhcp

Table 16: Static routes

3.11. Lines

The Cisco line configuration settings are used to configure administrative access to the device. The console line type is used for accessing the Cisco device directly through a cable attached to the device's console port. The auxiliary lines are used for remote access to the device, typically through attached modems. The Virtual Teletype (VTY) lines are used for access to the device through a remote access service such as SSH or Telnet.

Line Type	Start Line	End Line	Logins	Exec	Authorization	Accounting	Telnet	SSH	Timeout	Exec Timeout	Session Timeout	Absolute Timeout	Password	Password Encryption
Console	0		Allowed	On	Off	Off	On	Off	0s	0s	0s	0s		
Auxiliary	0		Allowed	On	Off	Off	On	Off	0s	0s	0s	0s		
VTY	0	4	Local	On	Off	Off	Off	On	0s	0s	0s	0s		

Table 17: Line configuration

3.12. Interfaces

Interface	Active	IP Address	Proxy ARP	IP Unreachable	IP Redirect	IP Mask Reply	IP Direct Broadcast	NTP	CDP	uRPF	MOP
FastEthernet0/0	Yes	11.0.0.1 255.255.255.0	On	On	On	Off	Off	On	On	Off	Off
FastEthernet1/0	Yes	dhcp	On	On	On	Off	Off	On	On	Off	Off
FastEthernet1/1	No	None	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Off	N/A
ATM2/0	No	None	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Off	N/A

Table 18: Interfaces

3.13. NAT

Network Address Translation (NAT) is used to map an IP address to an alternative IP address and is commonly used to map internal network IP addresses to Internet visible IP addresses. There are four different types of NAT on Cisco Router devices, dynamic NAT, static NAT, port static NAT and network static NAT. Static NAT translates one specific IP address into another specific IP address. Dynamic NAT translates an IP address into one of a pool of IP addresses. Port static NAT translates a specific IP address and port to another specific IP address and port. Finally, network static NAT translates a specific network subnet to another specific network subnet.

Source	From Type	From	To Type	To
Inside Interface	ACL	1	Interface	FastEthernet1/00
Inside Interface	ACL	100	Pool	NAT_POOL

Table 19: Dynamic NAT

3.14. Access Control List

A Cisco ACL is a sequential list of apply or deny ACEs that a Cisco device will apply to network traffic. The Cisco device will check network traffic against the ACL and the first ACE match will determine whether the packet is accepted or rejected. If the Cisco device does not have an ACE that applies then the packet is denied. When a packet is rejected after access list processing, an ICMP host unreachable message is sent, unless it had been disabled.

There are two different types of ACLs on IOS-based Cisco devices, standard and extended. Standard ACLs have an access list number between 1 and 99, extended ACLs are numbered 100 or above. Standard ACLs only define the source address and process the packet solely based on that. Extended ACLs contain additional checks, such as destination address and network port numbers.

Line	Filter	Source	Log
1	Permit	10.0.0.0 / 0.0.0.255	No
2	Permit	192.168.11.0 / 0.0.0.255	No

Table 20: Standard ACL 1

Line	Filter	Protocol	Source	Source Service	Destination	Destination Service	Log	Options
1	Permit	ip	192.168.11.0 / 0.0.0.255	Any	Any	Any	No	

Table 21: Extended ACL 100

---

4. Appendix

4.1. Abbreviations

ACE	Access Control Entry
ACL	Access Control List
ARP	Address Resolution Protocol
BOOTP	BOOTstrap Protocol
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
EGP	Exterior Gateway Protocol
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intruder Detection System
IGP	Interior Gateway Protocol
IOS	Internet Operating System
IP	Internet Protocol
LAN	Local Area Network
MD5	Message Digest 5
MOP	Maintenance Operations Protocol
NAT	Network Address Translation
NTP	Network Time Protocol
PAD	Packet Assembler / Disassembler
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VTY	Virtual Teletype

4.2. Common Ports

Service	Port
SSH	22
DHCP	67
HTTP	80
NTP	123
SNMP	161

Table 22: Common ports

4.3. Logging Severity Levels

Level	Level Name	Description
0	Emergencies	System is unstable
1	Alerts	Immediate action is required
2	Critical	Critical conditions
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Significant conditions
6	Informational	Informational messages
7	Debugging	Debugging messages

Table 23: Logging message severity levels

4.4. Time Zones

Region	Acronym	Time Zone	UTC Offset
Australia	CST	Central Standard Time	+9.5 hours
Australia	EST	Eastern Standard/Summer Time	+10 hours
Australia	WST	Western Standard Time	+8 hours
Europe	BST	British Summer Time	+1 hour
Europe	CEST	Central Europe Summer Time	+2 hours
Europe	CET	Central Europe Time	+1 hour
Europe	EEST	Eastern Europe Summer Time	+3 hours
Europe	EST	Eastern Europe Time	+2 hours
Europe	GMT	Greenwich Mean Time	
Europe	IST	Irish Summer Time	+1 hour
Europe	MSK	Moscow Time	+3 hours
Europe	WEST	Western Europe Summer Time	+1 hour
Europe	WET	Western Europe Time	+1 hour
USA and Canada	ADT	Atlantic Daylight Time	-3 hours
USA and Canada	AKDT	Alaska Standard Daylight Saving Time	-8 hours
USA and Canada	AKST	Alaska Standard Time	-9 hours
USA and Canada	AST	Atlantic Standard Time	-4 hours
USA and Canada	CDT	Central Daylight Saving Time	-5 hours
USA and Canada	CST	Central Standard Time	-6 hours
USA and Canada	EDT	Eastern Daylight Time	-4 hours
USA and Canada	EST	Eastern Standard Time	-5 hours
USA and Canada	HST	Hawaiian Standard Time	-10 hours
USA and Canada	MDT	Mountain Daylight Time	-6 hours
USA and Canada	MST	Mountain Standard Time	-7 hours
USA and Canada	PDT	Pacific Daylight Time	-7 hours
USA and Canada	PST	Pacific Standard Time	-3 hours

Table 24: Common time zone acronyms

4.5. Nipper Details

This report was generated using Nipper version 0.11.10. Nipper is an Open Source tool designed to assist security professionals and network system administrators securely configure network infrastructure devices. The latest version of Nipper can be found at the following URL:

http://nipper.titania.co.uk.