



Berner
Fachhochschule

BTI7301 Project 1

Mail Server Set-Up &
Security-Hardening Script
Bern University of Applied Sciences

Fridolin Zurlinden
Ismael Riedo
Jan Henzi
Tutor: Dr. Simon Kramer



Berner
Fachhochschule

Contents

Introduction

Goals and Requirements

Technical Solution / Realization

Challenges

Fridolin Zurlinden - Jan Henzi - Ismael Riedo | Mail - Server Set-Up & Security-Hardening Script

2



Berner
Fachhochschule

Introduction

IT security for everyone

- Transparency
- Simple
- Vendor independent

Fridolin Zurlinden - Jan Henzi - Ismael Riedo | Mail - Server Set-Up & Security-Hardening Script

3



Berner
Fachhochschule

Goals and Requirements

- Easy as pie “Complexity is the enemy of security”
- Brick by brick
- Power to the people (No vendor lock-in)
- Security by default

Fridolin Zurlinden - Jan Henzi - Ismael Riedo | Mail - Server Set-Up & Security-Hardening Script

4



Berner
Fachhochschule

Technical Solution

Introduction

- Setup
- Firewall
- DNS
- SSH
- Mail



Berner
Fachhochschule

Setup

“Main Script” / “Entry point”

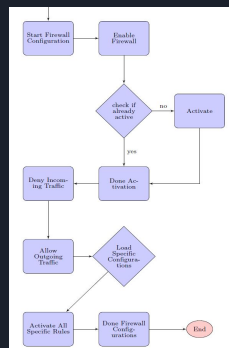
Flags - Leading pleasantly through the script

Handle State - What happens at the second time?



Berner
Fachhochschule

Firewall



src/fw/fw.sh

src/fw/enableUfw.sh

src/fw/controlTraffic.sh

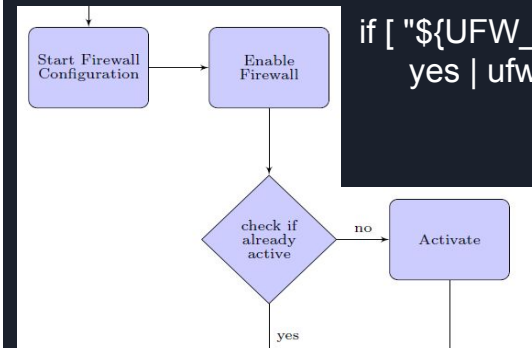
src/fw/specificConfigurations.sh

src/files/fw.conf



Berner
Fachhochschule

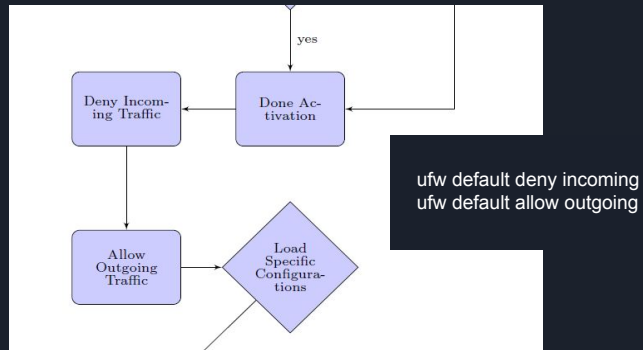
Firewall



if ["\${UFW_STATUS}" == "inactive"]; then
yes | ufw enable > /dev/null 2>&1

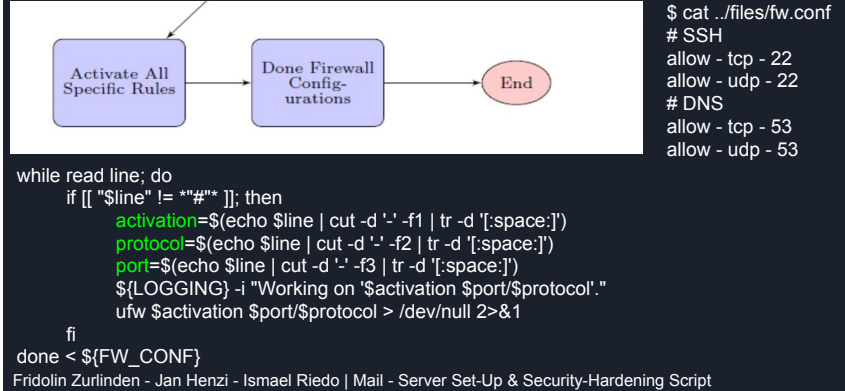
Firewall

Berner
Fachhochschule



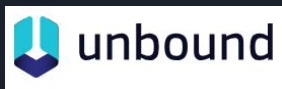
Firewall

Berner
Fachhochschule



DNS

Berner
Fachhochschule



Unbound is a validating, recursive, caching DNS resolver



NSD is an authoritative DNS name server

DNS

Berner
Fachhochschule



Unbound is a validating, recursive, caching DNS resolver




NSD is an authoritative DNS name server

F


H

DNS


Berner
Fachhochschule

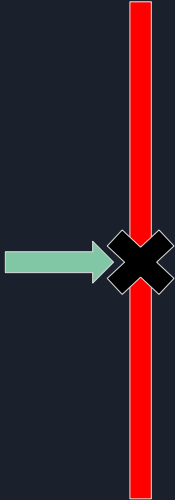


Unbound is a validating, recursive, caching DNS resolver



NSD is an authoritative DNS name server





Fridolin Zurlinden - Jan Henzi - Ismael Riedo | Mail - Server Set-Up & Security-Hardening Script

13

F

H

Unbound

Berner
Fachhochschule

```

# Read the root hints from this file. Default is nothing, using built in
# hints for the IN class. The file has the format of zone files, with root
# nameserver names and addresses only. The default may become outdated,
# when servers change, therefore it is good practice to use a root-hints
# file. get one from https://www.internic.net/domain/named.root
root-hints: "/var/lib/unbound/root.hints"

# Require DNSSEC data for trust-anchored zones, if such data is absent, the
# zone becomes bogus. Harden against receiving dnssec-stripped data. If you
# turn it off, failing to validate dnskey data for a trustanchor will trigger
# insecure mode for that zone (like without a trustanchor). Default on,
# which insists on dnssec data for trust-anchored zones.
hardened-dnssec-stripped: yes

```

Fridolin Zurlinden - Jan Henzi - Ismael Riedo | Mail - Server Set-Up & Security-Hardening Script

14

F

H

Unbound

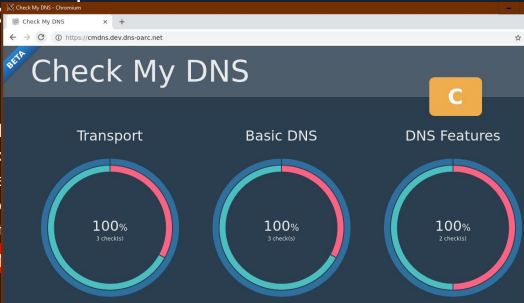
Berner
Fachhochschule

```

# Read the root hints from this file. Default is nothing, using built in
# hints for the IN class. The file has the format of zone files, with root
# nameserver names and addresses only. The default may become outdated,
# when servers change, therefore it is good practice to use a root-hints
# file. get one from https://www.internic.net/domain/named.root
root-hints: "/var/lib/unbound/root.hints"

# Require DNSSEC data for trust-anchored zones, if such data is absent, the
# zone becomes bogus. Harden against receiving dnssec-stripped data. If you
# turn it off, failing to validate dnskey data for a trustanchor will trigger
# insecure mode for that zone (like without a trustanchor). Default on,
# which insists on dnssec data for trust-anchored zones.
hardened-dnssec-stripped: yes

```



Fridolin Zurlinden - Jan Henzi - Ismael Riedo | Mail - Server Set-Up & Security-Hardening Script

15

F

H

Unbound

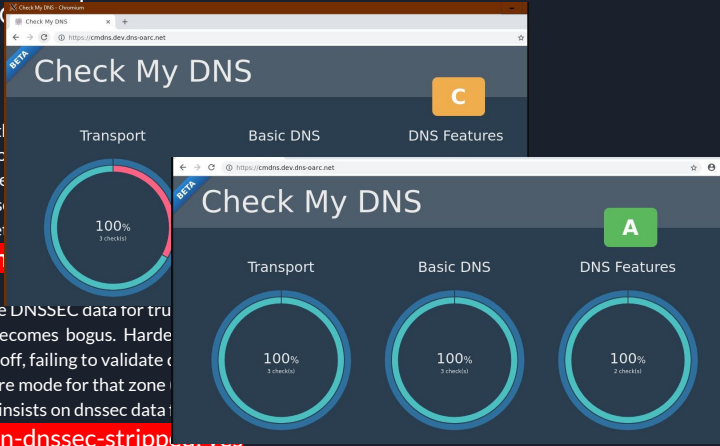
Berner
Fachhochschule

```

# Read the root hints from this file. Default is nothing, using built in
# hints for the IN class. The file has the format of zone files, with root
# nameserver names and addresses only. The default may become outdated,
# when servers change, therefore it is good practice to use a root-hints
# file. get one from https://www.internic.net/domain/named.root
root-hints: "/var/lib/unbound/root.hints"

# Require DNSSEC data for trust-anchored zones, if such data is absent, the
# zone becomes bogus. Harden against receiving dnssec-stripped data. If you
# turn it off, failing to validate dnskey data for a trustanchor will trigger
# insecure mode for that zone (like without a trustanchor). Default on,
# which insists on dnssec data for trust-anchored zones.
hardened-dnssec-stripped: yes

```



Fridolin Zurlinden - Jan Henzi - Ismael Riedo | Mail - Server Set-Up & Security-Hardening Script

16



NSD

Berner
Fachhochschule

```
$ORIGIN examplerun.cf. ; default zone domain
$TTL 86400 ; default time to live
```

```
@ IN SOA ns1.examplerun.cf. ns2.examplerun.cf. (
2019010917 ; serial number
28800 ; Refresh
7200 ; Retry
1209600 ; Expire
86400 ; Min TTL
)
```

```
NS ns1.examplerun.cf.
NS ns2.examplerun.cf.
MX 10 mail.examplerun.cf.
```

```
examplerun.cf. IN CAA 0 issue "letsencrypt.org"
examplerun.cf. IN CAA 0 iodef
"mailto:postmaster@examplerun.cf"
```

```
IN A 104.248.137.212
IN TXT "v=spf1 mx a ~all"
ns1 IN A 104.248.137.212
ns2 IN A 104.248.137.212
www IN A 104.248.137.212
* IN A 104.248.137.212
```

```
mail IN A 104.248.137.212
IN TXT "v=spf1 mx a ~all"
2019010917._domainkey IN TXT (
"v=DKIM1\059 h=sha256\059 k=rsa\059 s=email\059
p="<DKIM KEY>" )
_adsp._domainkey IN TXT "dkim=all"
_dmarc IN TXT "v=DMARC1\059 p=quarantine\059
sp=quarantine\059 adkim=r\059 aspf=r\059 fo=1\059
rf=afrr\059 rua=mailto:postmaster@examplerun.cf"
```

17



SSH

Berner
Fachhochschule

- SSH config hardening

```
X11Forwarding no
UseDNS yes
PermitRootLogin no
HostKeyAlgorithms
ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ssh-ed25519,ssh-rsa,ecdsa-sha2-nistp521-cert-v01@
openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp5
21,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256

KexAlgorithms
curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exch
ange-sha256

Ciphers
chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
```

18



SSH

Berner
Fachhochschule

- Secure SSH Keys

```
ssh-keygen -b 4096 -C "$user@$DOMAIN" -E sha256 -N mys3cr3t -t rsa -f
/home/alice/.ssh/id_rsa
```

19



Mail - Postfix

Berner
Fachhochschule



20



Mail - TLS

Berner
Fachhochschule

- TLS - Avoid clear text whenever possible
- DOVECOT
 - IMAP Server
 - Mutual Authentication



Mail - TLS

Berner
Fachhochschule

- Letsencrypt to obtain certificate
- Only use secure protocols (>TLSv1.2) and strong ciphers

```
certbot certonly --agree-tos --standalone -n -m  
postmaster@examplerun.cf -d mail.examplerun.cf
```

```
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1  
smtpd_tls_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1  
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1  
smtpd_tls_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1  
smtpd_tls_exclude_ciphers = EXP, MEDIUM, LOW, DES, 3DES, SSLv2  
smtpd_tls_exclude_ciphers = EXP, MEDIUM, LOW, DES, 3DES, SSLv2  
tls_high_cipherlist =  
KEECDH:+KEECDH+SHA:KECDH:+KECDH+SHA:KECDH:+KECDH+SHA:KRSA:+KRSA+SHA:+KRSA+CAMELLIA:1aNULL:1eNULL:1SSLv2:1RC4:1MD5:1DES:1EXP:1S  
EED:1IDEA:13DES:1SHA'  
tls_preempt_cipherlist = yes  
smtpd_tls_ciphers = high  
smtpd_tls_ciphers = high
```



Mail - Dovecot

Berner
Fachhochschule

- Require mutual authentication

```
ssl_verify_client_cert = yes  
ssl_cert_username_field = CN  
auth_ssl_username_from_cert = yes
```

- Map users

```
echo "alice: alice" >> /etc/aliases  
echo "alice@example.cf alice@example.cf" >> /etc/postfix/canonical  
echo "alice:::" >> /etc/dovecot/users-external
```



Mail - Anti-SPAM Measures

Berner
Fachhochschule

- SPF (Sender Policy Framework)
- DKIM (DomainKeys Identified Mail)
- ADSP (Author Domain Signing Practices)
- DMARC (Domain-based Message Authentication, Reporting and Conformance)



Mail - SPF

Berner
Fachhochschule

```
/etc/postfix/master.cf
policyd-spf unix - n n - 0 spawn
user=policyd-spf argv=/usr/bin/policyd-spf
```

```
/etc/postfix/main.cf
policyd-spf_time_limit = 3600
smtpd_recipient_restrictions =
...
reject_unauth_destination,
check_policy_service unix:private/policyd-spf,
...
```

DNS zone file:
IN TXT "v=spf1 mx a ~all"



Mail - SPF

Berner
Fachhochschule

```
/etc/postfix/master.cf
```

Betreff:	this is a test
SPF:	PASS mit IP-Adresse 1

DNS zone file:
IN TXT "v=spf1 mx a ~all"

```
policyd-spf[21065]: Pass; identity=mailfrom; client-ip=127.0.0.1; helo=mail.examplerun.cf;
envelope-from=test@examplerun.cf; receiver=ismaelmartin.riedo@bfh.ch
```

```
reject_unauth_destination,
check_policy_service unix:private/policyd-spf,
...
```



Mail - DKIM & ADSP

Berner
Fachhochschule

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=examplerun.cf;
s=2019010811; t=1546968309; bh=WN9jjFu//8qtE8luk5bNjWZe8eu6jn90bWUEPF3q5DU=;
h=Subject:To:Date:From:From;
b=SMsc9anWhENzauKUptLttlgHXHZvIg9InVCPahOb7uShzCISTzn/MOSmawxf7uBbe
mowBaVZetGiCYBJsMYzGRvNOCLiGjZnb9AJzD4EIOCAbsKJCjBQILtyKEPERcxu9wc
0wiIV/zl3F2u90EJN5gtIMCdqXb9aZloncdYAQu52Fr0MEs6qyWlZjZKUNz1bBvht+
CkGhW8NJ10Bfrs4EPeVI/qay9OOi4Gf5+DyXU3tNmQMqn/hUuY9A4miLX0B+Ml/7y
dEKVz4WSYIRNqLNPFezXjWgXL+dVbiw09PpFnnvyaeTB/u3LiWpXDCVWSeW1WTMR
fEKZ8bjBPiTiQ==
```



Mail - DKIM & ADSP

Berner
Fachhochschule

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=examplerun.cf;
s=2019010811; t=1546968309; bh=WN9jjFu//8qtE8luk5bNjWZe8eu6jn90bWUEPF3q5DU=;
h=Subject:To:Date:From:From;
b=SMsc9anWhENzauKUptLttlgHXHZvIg9InVCPahOb7uShzCISTzn/MOSmawxf7uBbe
mowBaVZetGiCYBJsMYzGRvNOCLiGjZnb9AJzD4EIOCAbsKJCjBQILtyKEPERcxu9wc
0wiIV/zl3F2u90EJN5gtIMCdqXb9aZloncdYAQu52Fr0MEs6qyWlZjZKUNz1bBvht+
CkGhW8NJ10Bfrs4EPeVI/qay9OOi4Gf5+DyXU3tNmQMqn/hUuY9A4miLX0B+Ml/7y
dEKVz4WSYIRNqLNPFezXjW "v=DKIM1\059 h=sha256\059 k=rsa\059 s=email\059 p="
fEKZ8bjBPiTiQ=="
"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAE6N+Xk585yT9WNMgbIS7CvNRdW
FKpSR7Tfo6trV0Ml6O6BHsFiSp5U5" "kbQ/vrK/xg9c4k5BIOk/yL/jd/o/BqjTGDnC/
pL89SLlNe5Z+vWlh4FEw9gmwk3etscUP0CYZ2s5PgvdLBpGfWytirjy+pYlxsFBORXZPlr
pQRfnNYpSR/eAXWF3REliO7NquS8ec985dpbZQW/3MHm" "W82Vwv5oDfh/kMQ9727qMxp
OED0ZQym12kPpdHK87Rg9zGOJDJs880RC3l3d+6tukf7fYyJ51TvpRtndLPrbutKdFgi3e
MMDkQXam+d8f3YHQoIMF7lR0pD2oOcH5gELX7gc6MwIDAQAB" )
_adsp._domainkey IN TXT "dkim=all"
```




Berner
Fachhochschule

DEMO

All documents and code can be found at :

<https://github.com/ifrido/BTI7301>

END



Berner
Fachhochschule

Web - Optional Part

src/web/apache/
enableApache.sh
configureApache.sh

src/web/nginx/
enableNginx.sh
nginxCertConfig.sh
configureNginx.sh

All documents and code can be found at :

<https://github.com/ifrido/BTI7301>

END

