CONFRARIA 0DAY

Invasão de servidores Linux e Windows com técnicas anti-forensic

Luiz Gustavo Corrêa Filho
Entusiasta na área da segurança da informação

PATROCINADORES

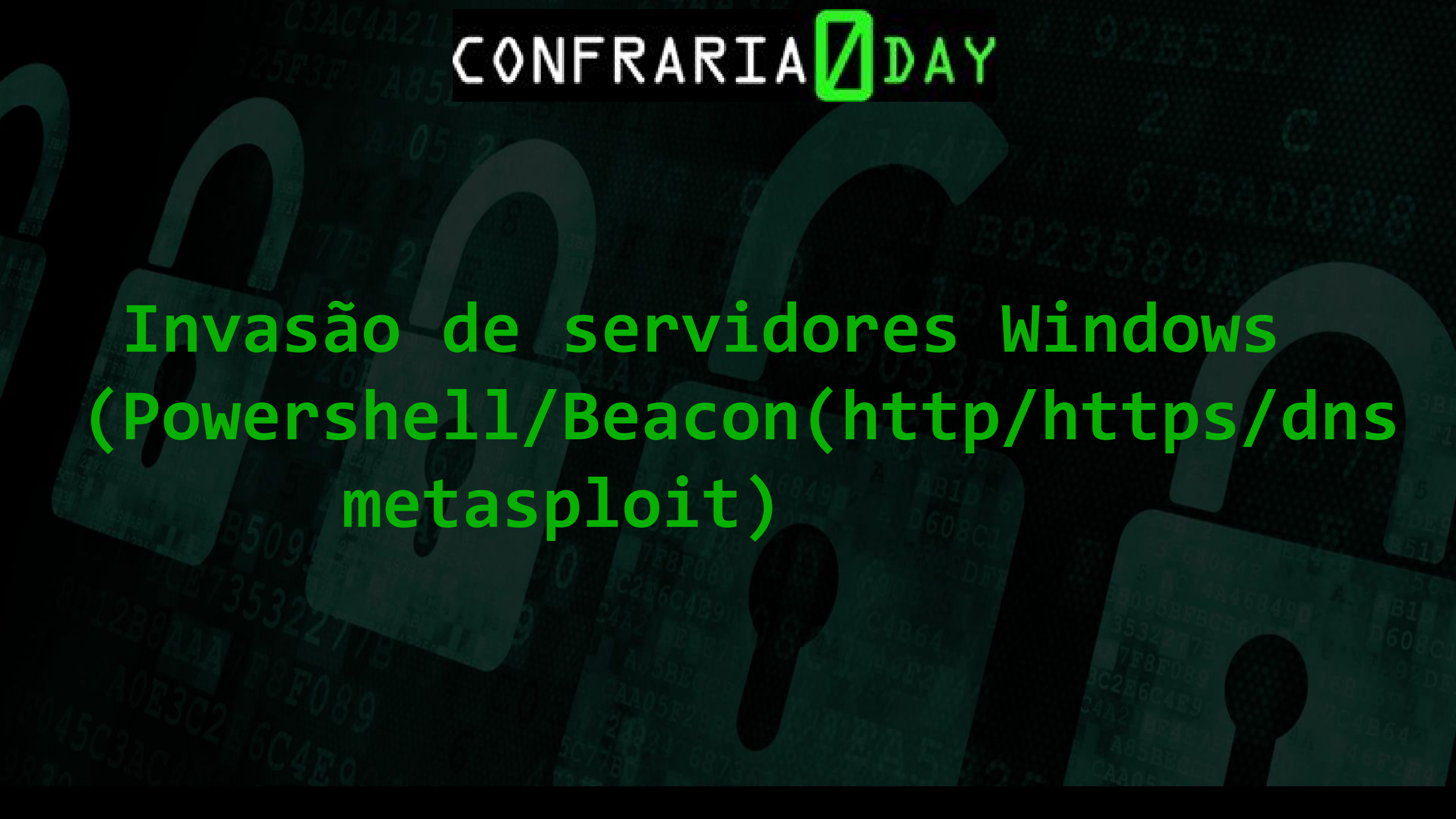
NTSEC
NETWORK SECURITY

Check Point®
SOFTWARE TECHNOLOGIES LTD.

APOIO

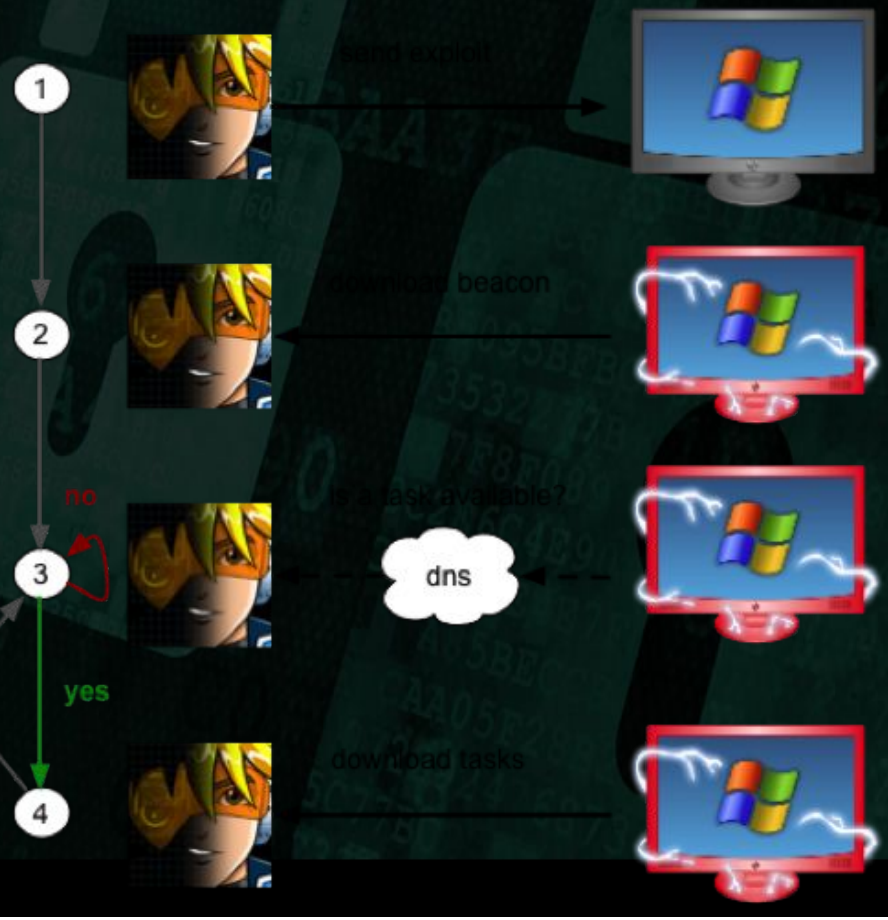
(ISC)² CHAPTER BRAZIL

Cora Hacker Club


CONFRARIA 0 DAY
Invasão de servidores Windows (Powershell/Beacon(http/https/dns metasploit)

Cobaltstrike payload beacon

Hybrid HTTP e DNS Beacon



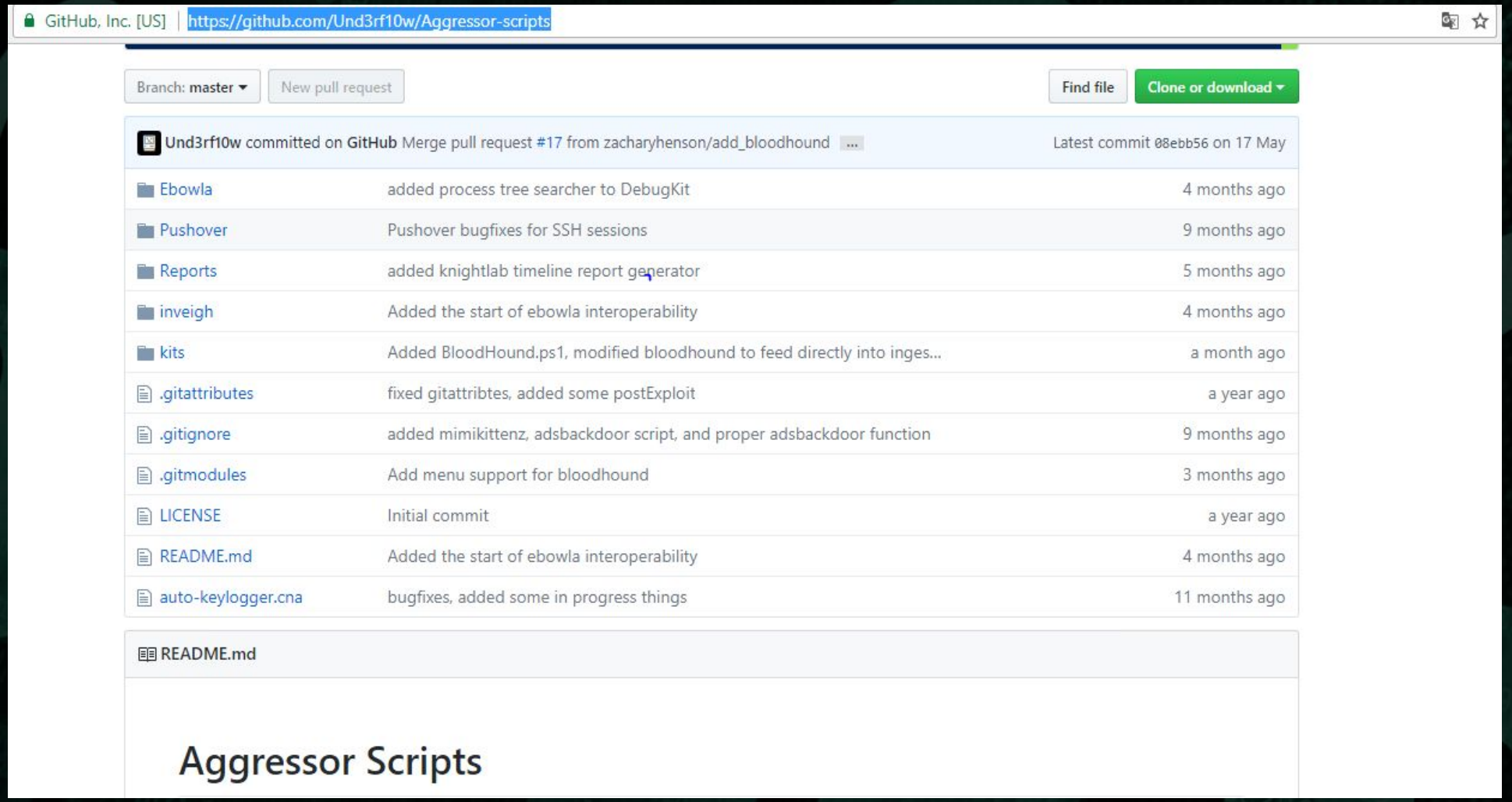
CONFRARIA 0DAY


Cobaltstrike ataque powershell
CONFRARIA 0 DAY

AntivirusBypass	Set all module versions to 3.0	2 years ago
CodeExecution	Fixed FreeLibrary function signature #146	a year ago
Exfiltration	fixed little-endian encoding	7 months ago
Mayhem	Set all module versions to 3.0	2 years ago
Persistence	Added ScheduledTaskHourly to New-UserPersistenceOption	a year ago
Privesc	typo fix for #179	7 months ago
Recon	Updated Get-ExploitableSystem	7 months ago
ScriptModification	Set all module versions to 3.0	2 years ago
Tests	removed Pester test for non-exported Invoke-ThreadedFunction function	7 months ago
.gitignore	Revert "Normalizing all files to ascii encoding"	2 years ago
LICENSE	Changed licensing to BSD 3-Clause	5 years ago
PowerSploit.psd1	Renamed Get-RegistryAutoRun to Get-ModifiableRegistryAutoRun	a year ago
PowerSploit.psm1	Excluding the Tests folder from being loaded as a module	2 years ago
PowerSploit.pssproj	Updated .psproj to reflect additions/removals	2 years ago
PowerSploit.sln	Adding Visual Studio 2015 project file	2 years ago
README.md	Added Get-GPPAutologon.ps1	7 months ago

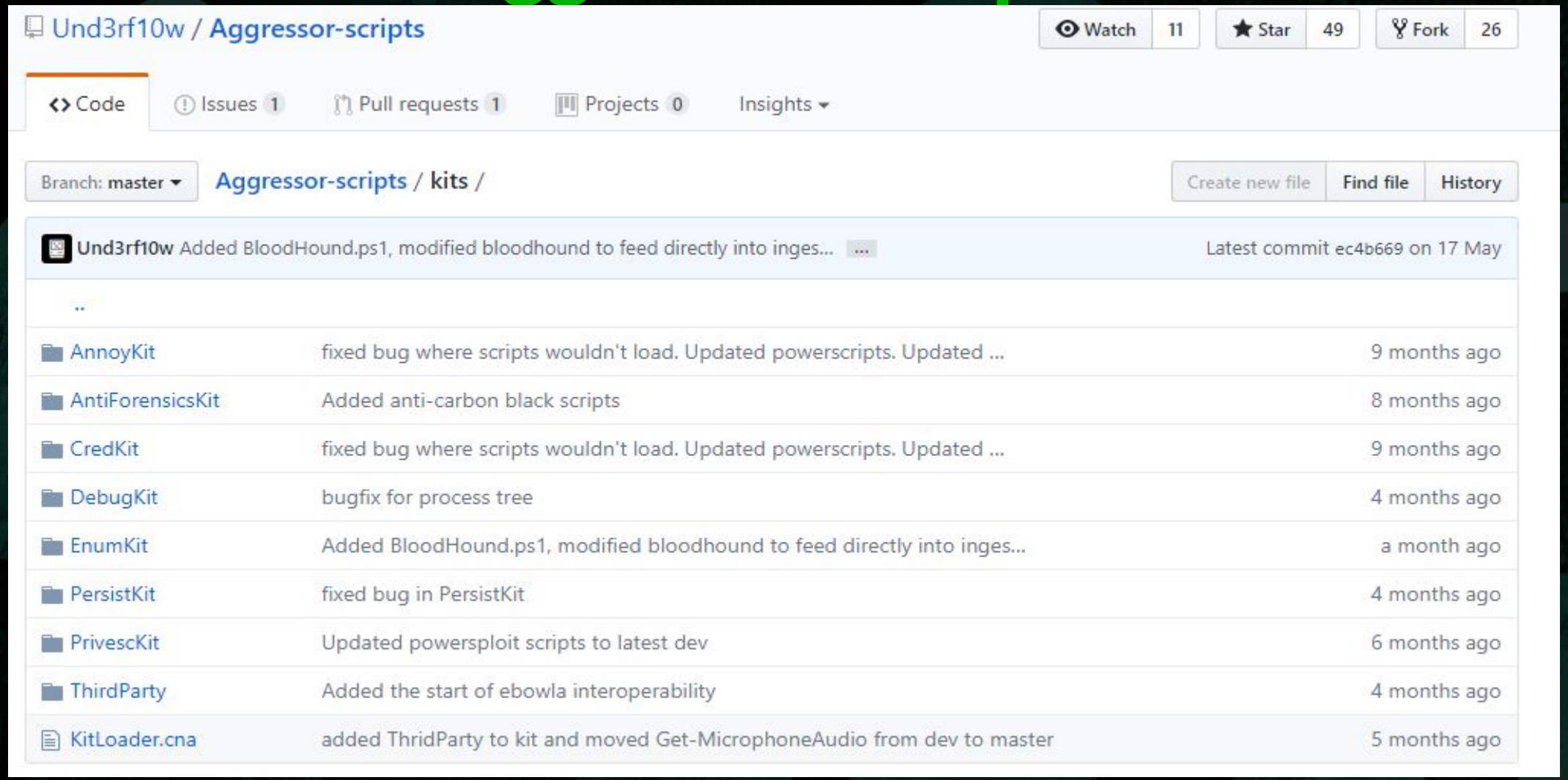

O poder do Cobaltstrike
CONFRARIA 0 DAY

Aggressor Scripts



CONFRARIA 0DAY

Aggressor Scripts



Und3rf10w / Aggressor-scripts

Watch 11 | Star 49 | Fork 26

Code | Issues 1 | Pull requests 1 | Projects 0 | Insights

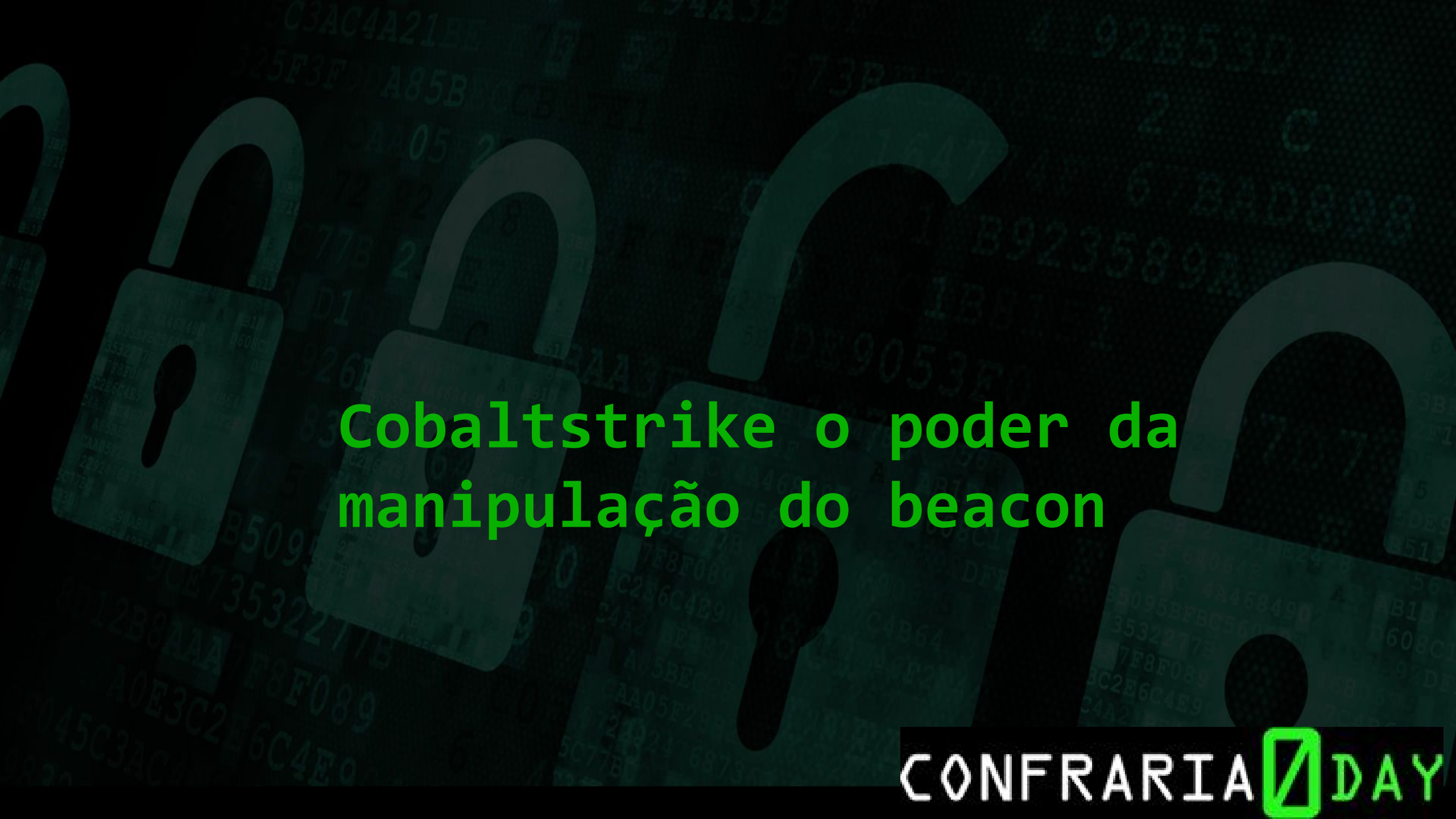
Branch: master | Aggressor-scripts / kits / | Create new file | Find file | History

Und3rf10w Added BloodHound.ps1, modified bloodhound to feed directly into inges... ... Latest commit ec4b669 on 17 May

..

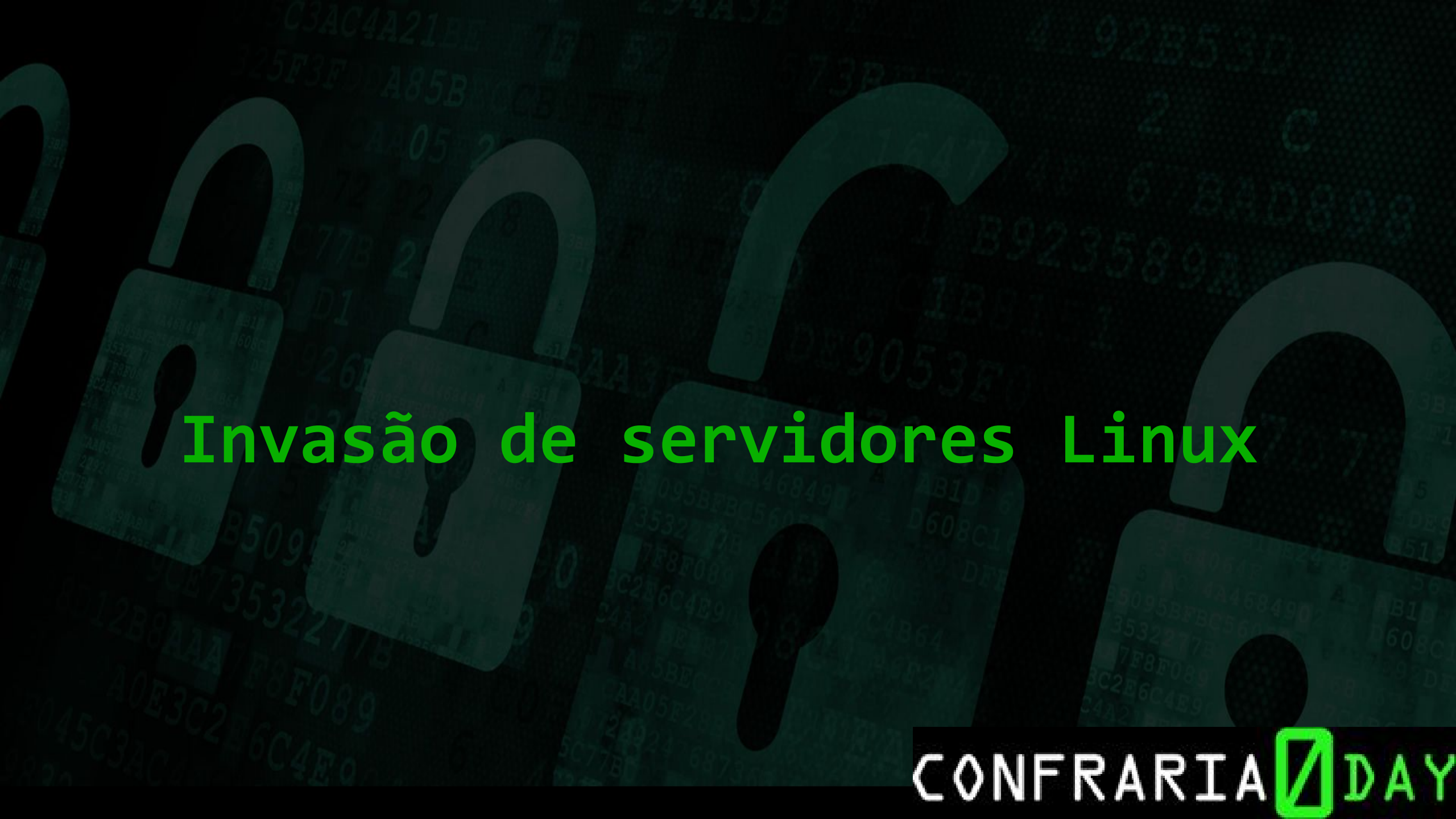
AnnoyKit	fixed bug where scripts wouldn't load. Updated powerscripts. Updated ...	9 months ago
AntiForensicsKit	Added anti-carbon black scripts	8 months ago
CredKit	fixed bug where scripts wouldn't load. Updated powerscripts. Updated ...	9 months ago
DebugKit	bugfix for process tree	4 months ago
EnumKit	Added BloodHound.ps1, modified bloodhound to feed directly into inges...	a month ago
PersistKit	fixed bug in PersistKit	4 months ago
PrivescKit	Updated powersploit scripts to latest dev	6 months ago
ThirdParty	Added the start of ebowla interoperability	4 months ago
KitLoader.cna	added ThridParty to kit and moved Get-MicrophoneAudio from dev to master	5 months ago

CONFRARIA 0DAY



Cobaltstrike o poder da manipulação do beacon

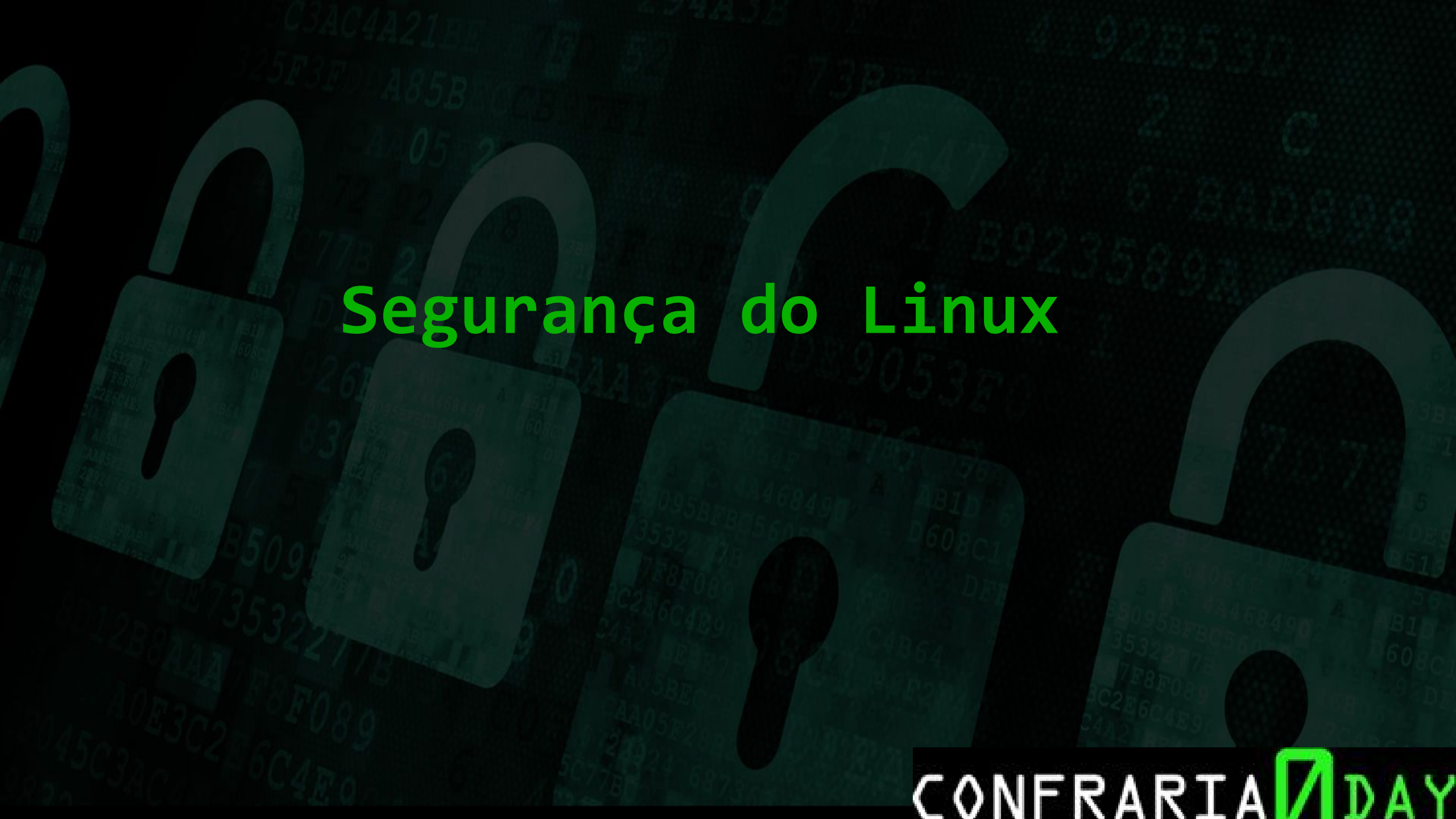
CONFRARIA 0 DAY


Invasão de servidores Linux
CONFRARIA 0 DAY


Daemons(root)
CONFRARIA 0 DAY

Utilizar senhas padrões

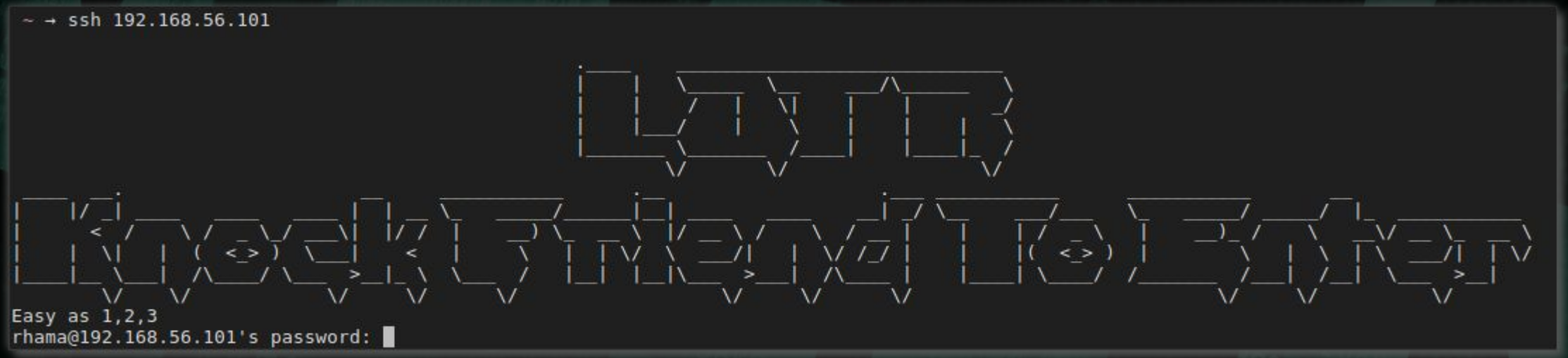
CONFRARIA 0 DAY



Segurança do Linux

CONFRARIA 0DAY

sempre que possível usar portknock



CONFRARIA 0DAY

Port Knocking

```
~ → knock 192.168.56.101 1 2 3 -v
hitting tcp 192.168.56.101:1
hitting tcp 192.168.56.101:2
hitting tcp 192.168.56.101:3
```

Port Knocking

```
[options]
        UseSyslog

[openSSH]
        sequence    = 7000,8000,9000
        seq_timeout = 5
        command     = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn

[closeSSH]
        sequence    = 9000,8000,7000
        seq_timeout = 5
        command     = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn
```

Port Knocking

```
########## Fases do Segredo ##################################################
/sbin/iptables -N INTO-FASE2
/sbin/iptables -A INTO-FASE2 -m recent --name FASE1 --remove
/sbin/iptables -A INTO-FASE2 -m recent --name FASE2 --set
/sbin/iptables -A INTO-FASE2 -j LOG --log-prefix "INTO FASE2: "

/sbin/iptables -N INTO-FASE3
/sbin/iptables -A INTO-FASE3 -m recent --name FASE2 --remove
/sbin/iptables -A INTO-FASE3 -m recent --name FASE3 --set
/sbin/iptables -A INTO-FASE3 -j LOG --log-prefix "INTO FASE3: "

/sbin/iptables -N INTO-FASE4
/sbin/iptables -A INTO-FASE4 -m recent --name FASE3 --remove
/sbin/iptables -A INTO-FASE4 -m recent --name FASE4 --set
/sbin/iptables -A INTO-FASE4 -j LOG --log-prefix "INTO FASE4: "

/sbin/iptables -A INPUT -m recent --update --name FASE1
```

Port Knocking

```
/sbin/iptables -A INPUT -p tcp --dport 100 -m recent --set --name FASE1
/sbin/iptables -A INPUT -p tcp --dport 200 -m recent --rcheck --seconds 15 --name FASE1 -j INTO-FASE2
/sbin/iptables -A INPUT -p tcp --dport 300 -m recent --rcheck --seconds 15 --name FASE2 -j INTO-FASE3
/sbin/iptables -A INPUT -p tcp --dport 400 -m recent --rcheck --seconds 15 --name FASE3 -j INTO-FASE4

######## Aqui chegamos a FASE4, que é a última deste exemplo, onde será liberada a conexão com a porta 22 (ssh). O tempo aqui está setado para 3600 segundos (1 hora). Depois disso será fechada novamente para o ip em questão, lembrando que se ele ainda estiver logado não fará diferença, será fechada mesmo assim. Então aumente o tempo conforme desejado.#####

/sbin/iptables -A INPUT -p tcp -s $HOST_IP --dport 22 -m recent --rcheck --seconds 3600 --name FASE4 -j ACCEPT

######## Por último fechamos todos acessos a porta 22 #########

/sbin/iptables -A INPUT -p tcp --dport 22 -j DROP
```

Kernel

```
echo "====>PROTECOES DE KERNEL<===="

echo 0 > /proc/sys/net/ipv4/conf/all/accept_source_route

echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects

echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects

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

echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_all

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

echo 0 > /proc/sys/net/ipv4/conf/all/accept_source_route

echo 1 > /proc/sys/net/ipv4/conf/all/rp_filter

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

echo 1 > /proc/sys/net/ipv4/conf/all/log_martians

echo "OK -> proteção para o Kernel ..."
```

Kernel

echo 0 > /proc/sys/net/ipv4/conf/all/accept_source_route (**Router)**

echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts (dos icpm)

Echo 0 > /proc/sys/net/ipv4/conf/all/aceept_source_router(redirecionar pacotes teste de routers)

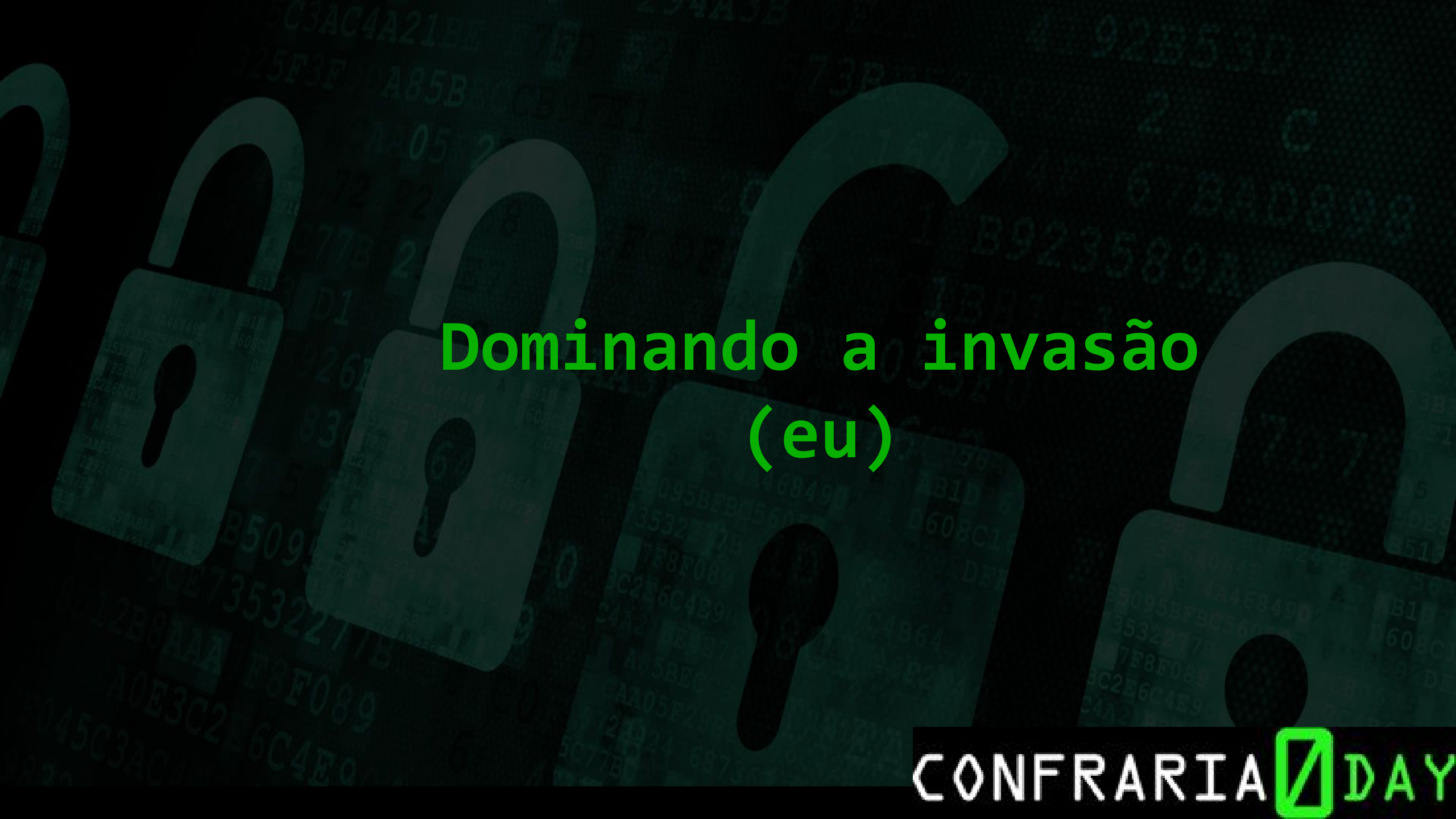
Echo 0 > /proc/sys/net/ipv4/ip_forward (desativando suporte a ip_forward)

Echo 0 > /proc/sys/net/ipv4/tcp_syscookies(not syn flood)

Echo 1 > /proc/sys/net/ipv4/conf/all/log_martians(Isso registra falsificação, bem como "roteamento de origem" e "redirecionamento".)

Sniffer remonte de sessão

CONFRARIA 0DAY


Dominando a invasão
(eu)
CONFRARIA 0 DAY

Bad god

1. **Root(no-root)**
2. *Criptografia de disco (home/ var/ root/)*
3. *Cuidado com a /etc*
4. *Senhas fortes mínimo 20 dígitos (random)*
5. *Proxy/socks*
6. *Mac*
7. *Ids, ips , honeypost e nc*
8. *Firewall*
9. *Crpt*
10. *criptografia (rsa & aes)*

CONFRARIA 0 DAY


Invasão de servidores Linux
CONFRARIA 0 DAY

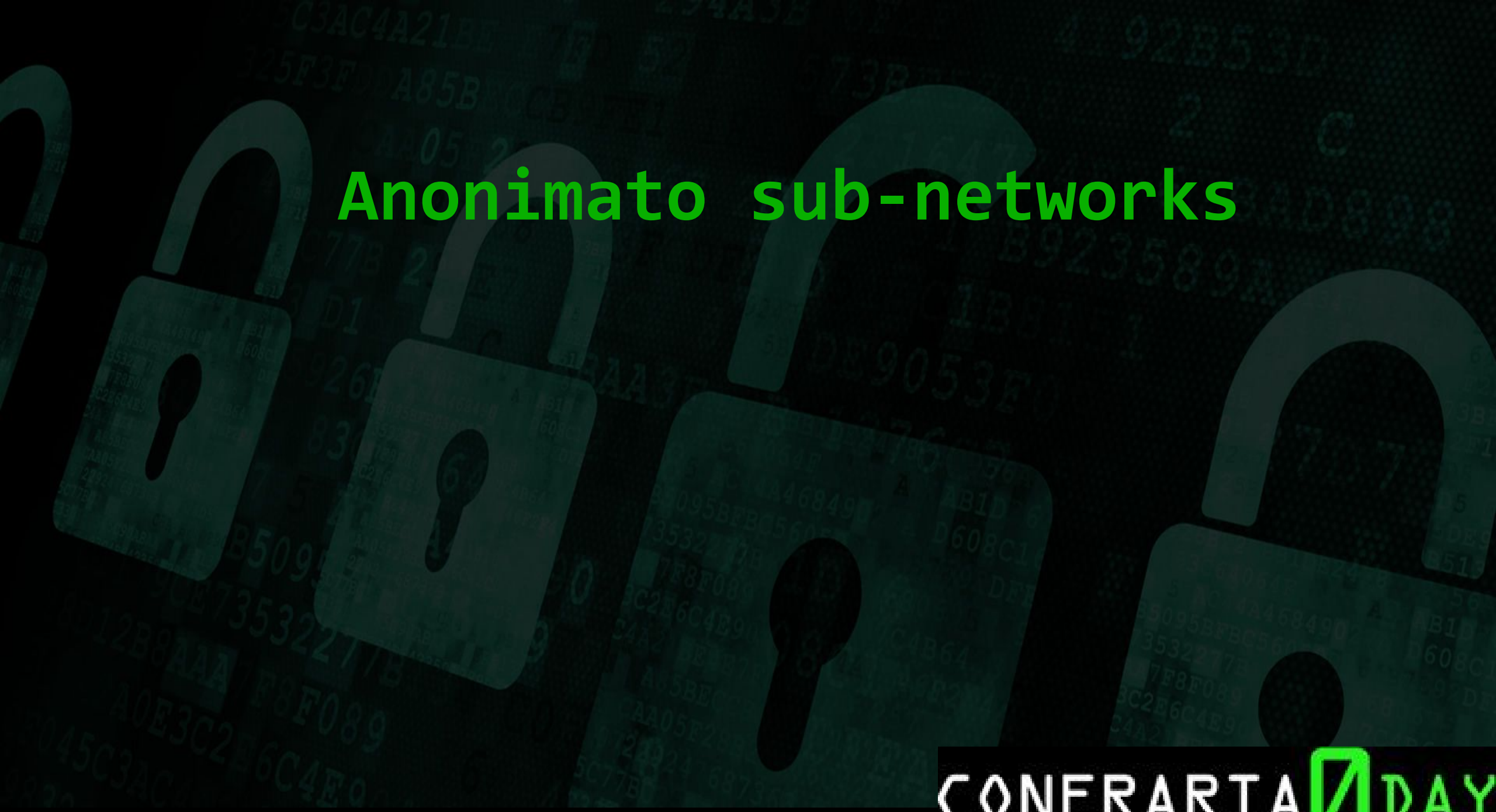
Logs
bad god

1. Logs bad god

1. /var/log/messages
2. /var/log/auth.log
3. /var/log/kern.log
4. /var/log/cron.log
5. /var/log/maillog
6. /var/log/secure
7. /var/log/utmp
   /var/log/wtmp
8. /var/log/boot.log

Sniffer remonte de sessão(bad god)

Anonimato sub-networks




redes
(Tor; Resilio; Maelstrom; Ricochet; i2p;
Retroshare; Soulseek; demonsaw)
CONFRARIA 0 DAY

Navegador
(Firefox, hconstf, mantra)

CONFRARIA 0DAY

Técnicas anti-forensic

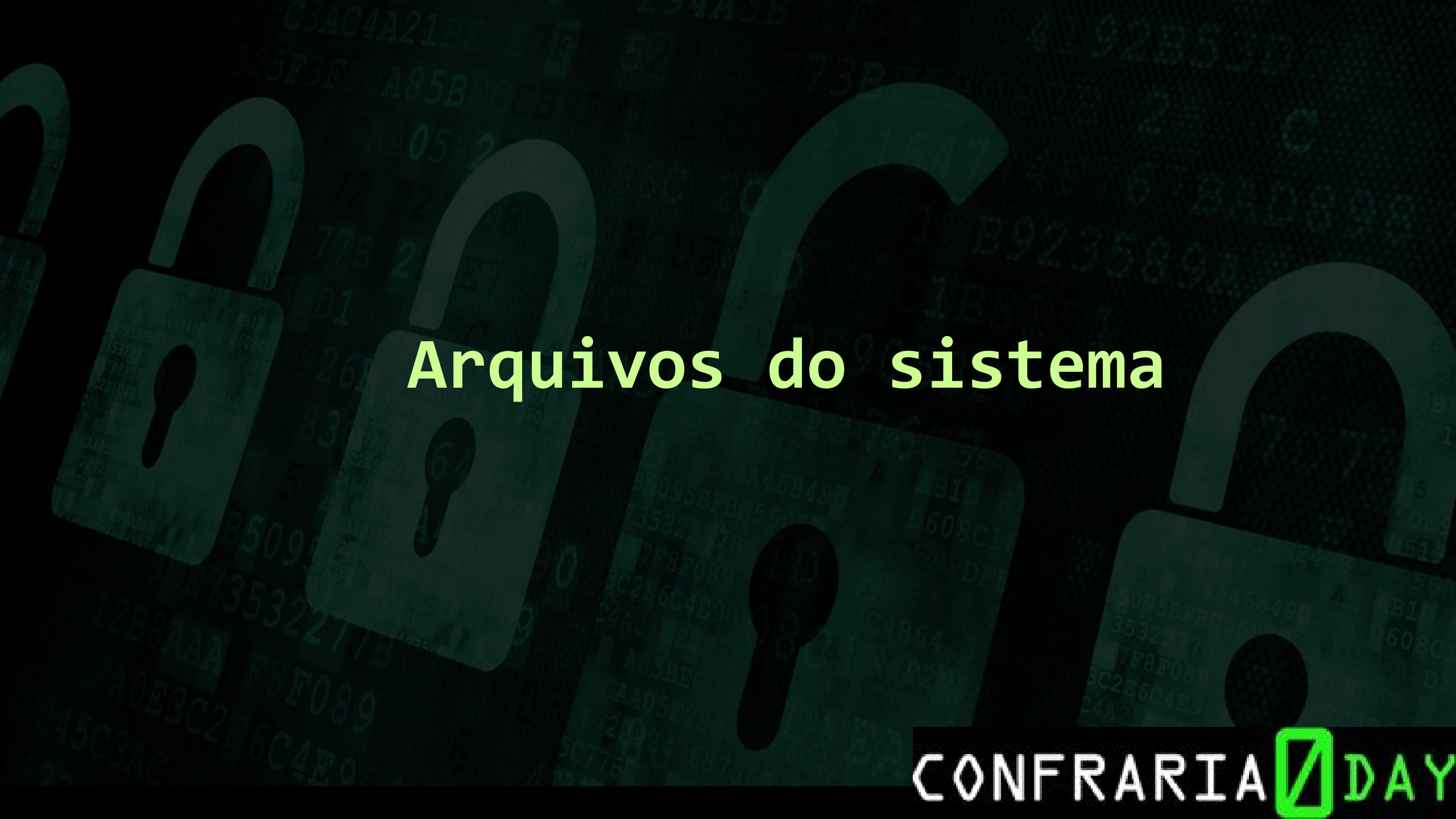
CONFRARIA 0DAY


Após a invasão oque devo fazer ?
CONFRARIA 0 DAY

CONFRARIA 0DAY

bad god logs

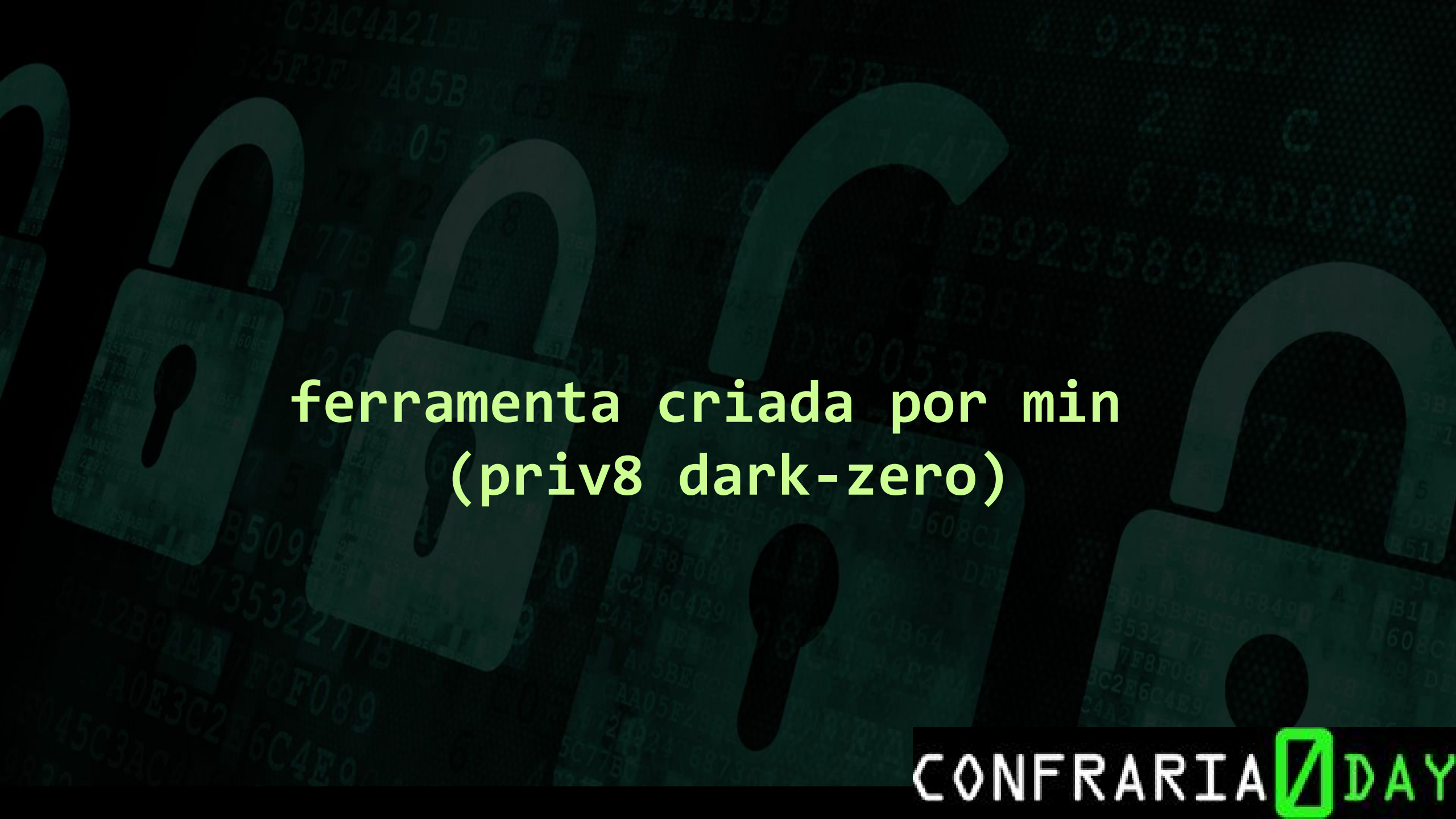
1. Memoria ram
2. Swap
3. E-nodes

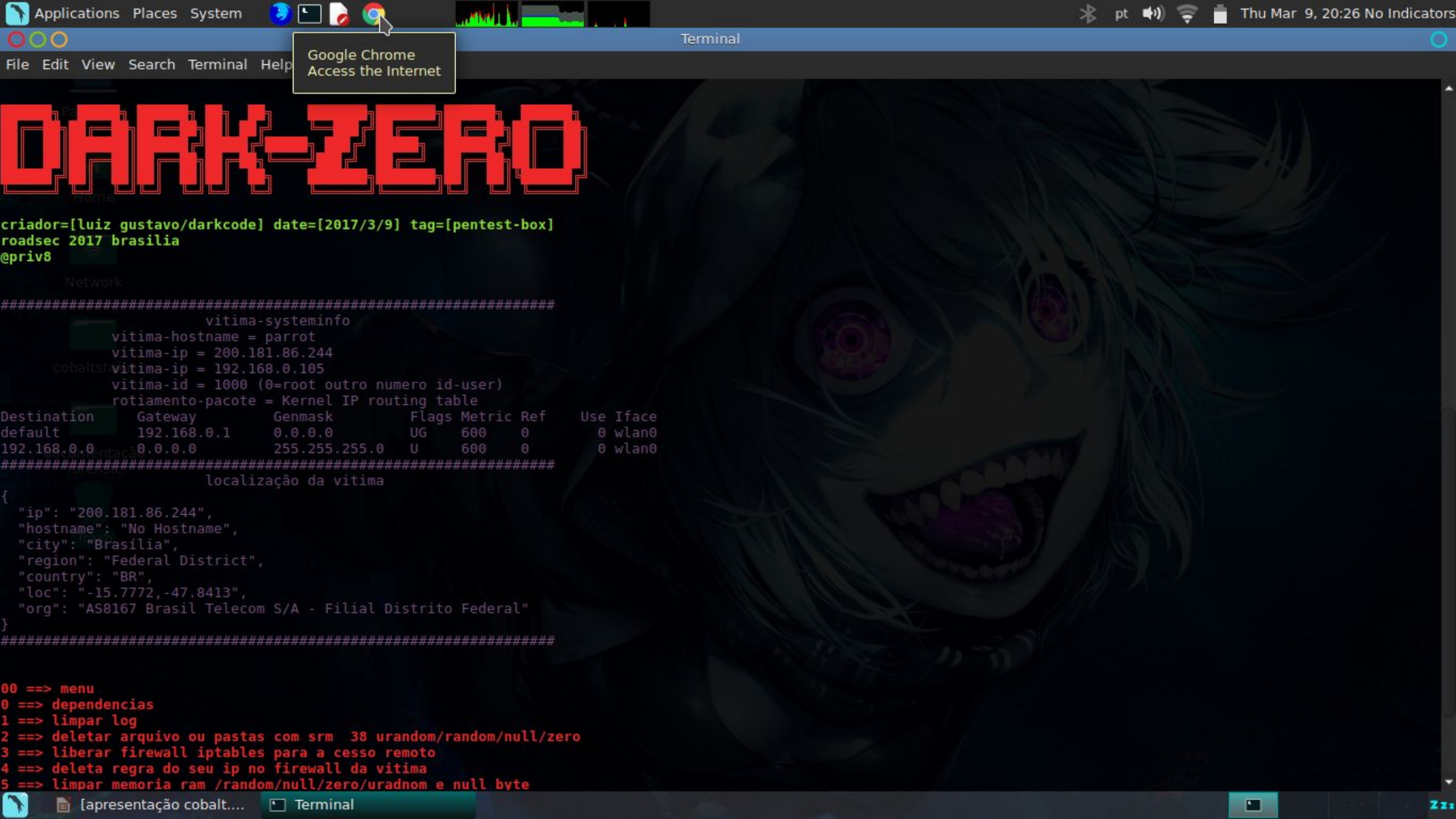


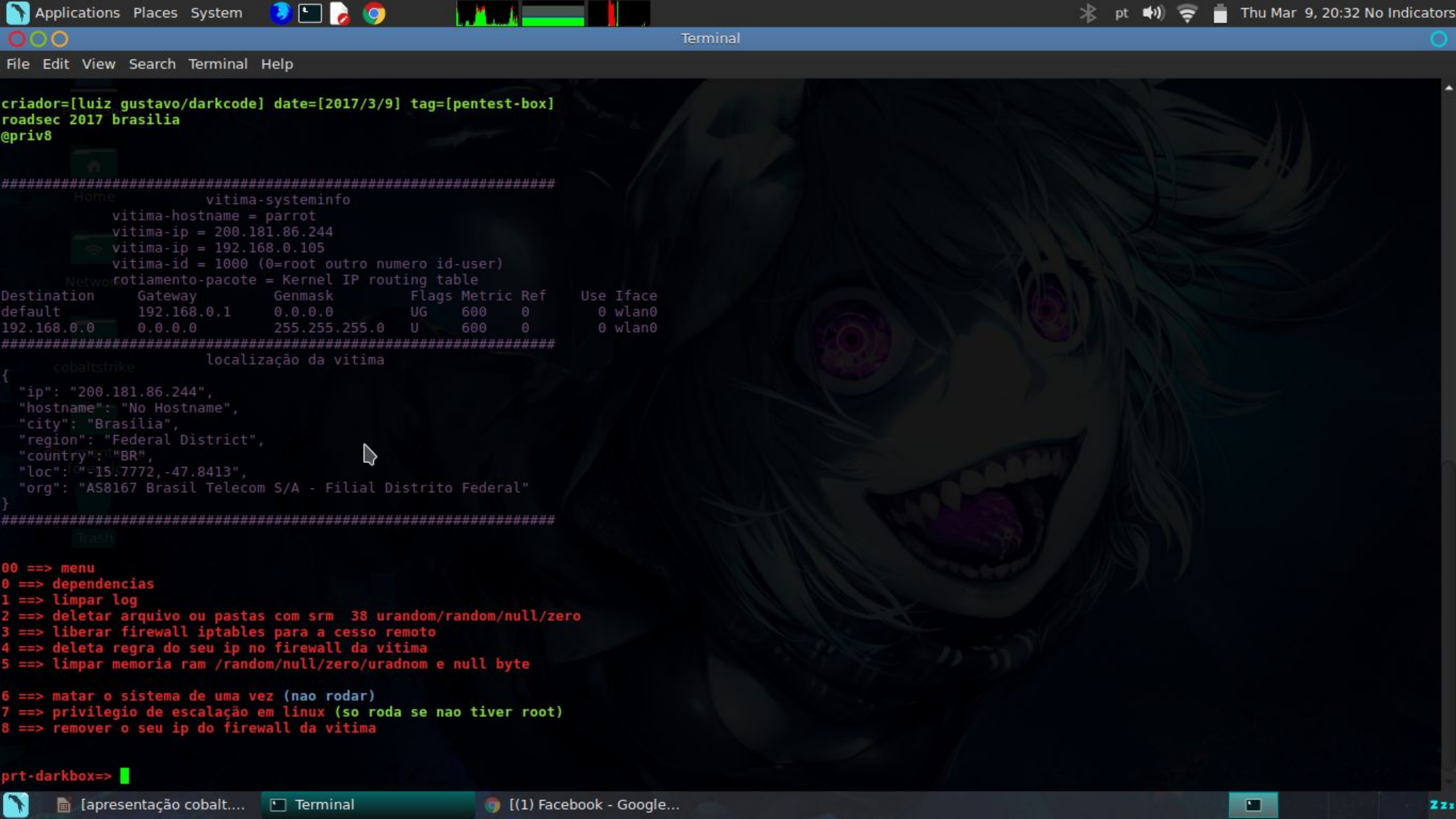
Arquivos do sistema

CONFRARIA 0DAY


Logs (ips / dns)
CONFRARIA 0 DAY


ferramenta criada por min
(priv8 dark-zero)
CONFRARIA 0 DAY


Applications Places System
Google Chrome
Access the Internet
pt
Thu Mar 9, 20:26 No Indicators
Terminal
File Edit View Search Terminal Help
DARK-ZERO
criador=[luiz gustavo/darkcode] date=[2017/3/9] tag=[pentest-box]
roadsec 2017 brasilia
@priv8
vitima-systeminfo
vitima-hostname = parrot
vitima-ip = 200.181.86.244
vitima-ip = 192.168.0.105
vitima-id = 1000 (0=root outro numero id-user)
rotiamento-pacote = Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 192.168.0.1 0.0.0.0 UG 600 0 0 wlan0
192.168.0.0 0.0.0.0 255.255.255.0 U 600 0 0 wlan0
localização da vitima
{
"ip": "200.181.86.244",
"hostname": "No Hostname",
"city": "Brasília",
"region": "Federal District",
"country": "BR",
"loc": "-15.7772,-47.8413",
"org": "AS8167 Brasil Telecom S/A - Filial Distrito Federal"
}
00 ==> menu
0 ==> dependencias
1 ==> limpar log
2 ==> deletar arquivo ou pastas com srm 38 urandom/random/null/zero
3 ==> liberar firewall iptables para a cesso remoto
4 ==> deleta regra do seu ip no firewall da vitima
5 ==> limpar memoria ram /random/null/zero/uradnom e null byte
[apresentação cobalt....
Terminal


Applications Places System
pt
Thu Mar 9, 20:32 No Indicators
Terminal
File Edit View Search Terminal Help
criador=[luiz gustavo/darkcode] date=[2017/3/9] tag=[pentest-box]
roadsec 2017 brasilia
@priv8
vitima-systeminfo
vitima-hostname = parrot
vitima-ip = 200.181.86.244
vitima-ip = 192.168.0.105
vitima-id = 1000 (0=root outro numero id-user)
rotiamento-pacote = Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 192.168.0.1 0.0.0.0 UG 600 0 0 wlan0
192.168.0.0 0.0.0.0 255.255.255.0 U 600 0 0 wlan0
localização da vitima
{
"ip": "200.181.86.244",
"hostname": "No Hostname",
"city": "Brasília",
"region": "Federal District",
"country": "BR",
"loc": "-15.7772,-47.8413",
"org": "AS8167 Brasil Telecom S/A - Filial Distrito Federal"
}
00 ==> menu
0 ==> dependencias
1 ==> limpar log
2 ==> deletar arquivo ou pastas com srm 38 urandom/random/null/zero
3 ==> liberar firewall iptables para a cesso remoto
4 ==> deleta regra do seu ip no firewall da vitima
5 ==> limpar memoria ram /random/null/zero/uradnom e null byte
6 ==> matar o sistema de uma vez (nao rodar)
7 ==> privilegio de escalação em linux (so roda se nao tiver root)
8 ==> remover o seu ip do firewall da vitima
prt-darkbox=>
[apresentação cobalt....
Terminal
[(1) Facebook - Google...