Cheatsheets

Organic HTTP File Transfer

Posted on January 26, 2018

Living off the land is essential when it comes to penetrating networks. The box that you landed on may be bare bones with only the default corporate software installed. Infiltrating and exfiltrating data is critical to mission success. This cheatsheet is not all inclusive, but should give you a good starting point for organic file transfer mechanisms.

#cheatsheet #tradecraft #tips #tricks #redteam #http **[Read More]**

GoPhish Template Cheatsheet

Posted on January 5, 2018

Variable	Description
{{.FirstName}}	Target's first name
{{.LastName}}	Target's last name
{{.Position}}	Target's position
{{.Email}}	Target's e-mail
{{.From}}	Source e-mail address
{{.TrackingURL}}	URL to tracking handler (per engagement)
{{.Tracker}}	Alias for inserting img tag to read tracking URL
{{.URL}}	URL to the phishing destination

#gophish #cheatsheet #phishing **[Read More]**

Ncat Cheatsheet

Posted on December 19, 2017

Man Page

```
Name
ncat – Concatenate and redirect sockets

Synopsis
ncat [ <OPTIONS> ...] [ <hostname> ] [ <port> ]
```

#ncat #cheatsheet #networking #tcp #udp #pivoting #shells **[Read More]**

OpenSSL Cheatsheet

Posted on December 18, 2017

Generating Certificates

Generate RSA Private Key + CSR

`openssl req -out newkey.csr -new -newkey rsa:[bits] -nodes -keyout priv.key`

Generate Self Signed Certificate + Priv Key

```
openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:[bits] -keyout priv.key -out cert.crt
```

Generate CSR for existing Cert

```
openssl x509 -x509toreq -in cert.crt -out newreq.csr -signkey priv.key
```

#openssl #cheatsheet #ssl #tls **[Read More]**

Network Pivoting Techniques

Posted on December 14, 2017

Basic Pivoting Types

Type	Use Case
Listen - Listen	Exposed asset, may not want to connect out.
Listen - Connect	Normal redirect.
Connect - Connect	Can't bind, so connect to bridge two hosts

#pivoting #regeorg #ncat #tcp #socat #meterpreter #rpivot #proxychains #tradecraft #techniques #redteam **[Read More]**

SSH Cheatsheet

Posted on December 13, 2017

Base Usage

```
ssh [user]@[host]
```

Use Specific Key

```
ssh -i ~/.ssh/id_rsa [user]@[host]
```

Use Alternative Port

```
ssh -i ~/.ssh/id_rsa -p [port] [user]@[host]
```

Dynamic SOCKS Proxy

This can be used with proxychains to forward client traffic through the remote server.

```
ssh -D8080 [user]@[host]
```

#redteam #ssh #openssh #pivoting #ssh-keygen #cheatsheet **[Read More]**

Nmap Cheatsheet

Posted on December 9, 2017

Nmap Quick commands

Ping Sweep

```
nmap -sn <ipaddress range>-<ipaddress range>
```

example

```
nmap -sn 192.168.0.2-100
```

or

```
nmap -sn 192.168.0.2-192.168.1.100
```

#nmap #nmap scripts #cheatsheet #tcp #udp #grep #enumerate **[Read More]**

Dns Recon Cheatsheet

Posted on December 6, 2017

DNS BruteForcing

DNS Wordlists

Description	URL
Top 1000	https://github.com/bitquark/dnspop/tree/master/results
Top 10000	https://github.com/bitquark/dnspop/tree/master/results
Top 100000	https://github.com/bitquark/dnspop/tree/master/results
Top 1000000	https://github.com/bitquark/dnspop/tree/master/results
Various Others	https://github.com/danielmiessler/SecLists/tree/master/Discovery/DNS

DNSRecon

```
$ dnsrecon -d <domain> -D <dir/wordlist> -t brt
```

Output Formats

- –xml
- –json
- –csv
- –db # SQLite file

#dns #redteam #recon #cheatsheet #dig #dnsrecon #nmap #bruteforce

[Read More]