HACKYCORP OSINT

PASSIVE RECONNAISSANCE

Domain Information

- **Name:** HACKYCORP.COM
- **Registry Domain ID:** 2506038815_DOMAIN_COM-VRSN
- **Domain Status:**
  clientTransferProhibited
- **Nameservers:**
  NS-104-A.GANDI.NET
  NS-123-C.GANDI.NET
  NS-219-B.GANDI.NET

Dates

- **Registry Expiration:** 2025-03-22 07:53:04 UTC
- **Updated:** 2022-01-24 03:03:38 UTC
- **Created:** 2020-03-22 07:53:04 UTC

Registrar Information

- **Name:** Gandi SAS
- **IANA ID:** 81
- **Abuse contact email:** abuse@gandi.net
- **Abuse contact phone:** tel:+33.170377661

DNSSEC Information

- **Delegation Signed:** Unsigned

Authoritative Servers

- **Registry Server URL:** https://rdap.verisign.com/com/v1/domain/hackycorp.com
- **Last updated from Registry RDAP DB:** 2022-12-11 16:55:29 UTC
- **Registrar Server URL:** https://rdap.gandi.net/domain/HACKYCORP.COM
- **Last updated from Registrar RDAP DB:** 2022-01-24 07:03:38 UTC

HACKYCORP'S URLS

URL	MIME	Type From	To
http://hackycorp.com/robots.txt	text/plain	Dec 4, 2021	Mar 16, 2022
http://hackycorp.com/favicon.ico	warc/revisit	Jan 11, 2022	Mar 26, 2022
https://hackycorp.com/admin/	text/html	Oct 29, 2022	Oct 29, 2022
https://hackycorp.com/images/	text/html	Oct 29, 2022	Oct 29, 2022
https://hackycorp.com/startpage/	text/html	Oct 29, 2022	Oct 29, 2022
http://hackycorp.com	text/html	Jun 26, 2020	Nov 18, 2022
http://hackycorp.com/images/logo.png	image/png	Jun 26, 2020	Nov 18, 2022
https://hackycorp.com/images/key.txt	text/plain	Oct 29, 2022	Nov 18, 2022

IP Address	Location	IP Address Owner	Last seen on this IP
51.158.147.132	Paris - France	Scaleway - Amsterdam	2022-12-11
51.158.152.91	Paris - France	Scaleway - Amsterdam	2020-07-23

Basic Information

Reverse DNS	51-158-147-132.rev.poneytelecom.eu
OS	Debian Linux 10.2
Network	Online SAS (FR)
Routing	51.158.128.0/17 via AS12876
Protocols	22/SSH , 53/DNS , 80/HTTP , 443/HTTP

22/SSH(tcp)
Software
linux
OpenBSD OpenSSH 7.9
Debian Linux 10.2

Details
Host Key
Algorithm
ecdsa-sha2-nistp256
Fingerprint
4815235839a3ac471cb5327777f83c0a87e63a17435b7e5f5eee297b5b51c39b
Negotiated
Key Exchange
curve25519-sha256@libssh.org
Symmetric Cipher
aes128-ctr
MAC
hmac-sha2-256

53/DNS(udp)
Details
Server Type
AUTHORITATIVE
R Code
REFUSED

80/HTTP(tcp)
Software
nginx

Details
http://51.158.147.132
Request
GET /
Protocol

HTTP/1.1
Status Code
200
Status Reason
OK
Body Hash
sha1:a3f586c68517415f5779135a935b294e5e692838

443/HTTPS(tcp)
Software
nginx

Details
https://51.158.147.132
Request
GET /
Protocol
HTTP/1.1
Status Code
200
Status Reason
OK
Body Hash
sha1:3bbf1cc3dcd1d16d09e95bc744dc9ec2bb46347d
Response Body

TLS
Fingerprint
JARM
3fd3fd15d3fd3fd21c3fd3fd3fd3fdc110bab2c0a19e5d4e587c17ce497b15
JA3S
a4a4c81b00b746b978f1513c9d74831e
Handshake
Version Selected
TLSv1_2
Cipher Selected
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
Leaf Certificate
1d31f9c2bc4da2a16864e737571bc1dd7ab582c8d7e4a4b82b7d9162755e8580
CN=hackycorp.com
C=US, O=Let's Encrypt, CN=R3
Issuer Chain
67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd
6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f99b9d47cf7ff1c24f

Host

Attribute	Value
ip	51.158.147.132
location.continent	Europe
location.country	France
location.country_code	FR
location.city	Paris

```
location.postal_code                        75001
location.timezone                                   Europe/Paris
location.province                                   Île-de-France
location.coordinates.latitude               48.8323
location.coordinates.longitude                      2.4075
location.registered_country                 France
location.registered_country_code            FR
location_updated_at                  2022-12-04T01:22:09.234527Z
autonomous_system.asn                               12876
autonomous_system.description               Online SAS
autonomous_system.bgp_prefix                51.158.128.0/17
autonomous_system.name                      Online SAS
autonomous_system.country_code              FR
autonomous_system_updated_at         2022-12-01T07:06:42.117447Z
operating_system.uniform_resource_identifier
                          cpe:2.3:o:debian:debian_linux:10.2:*:*:*:*:*:*:*
operating_system.part                               o
operating_system.vendor                             Debian
operating_system.product                    Linux
operating_system.version                    10.2
operating_system.other.family                       Linux
dns.names                                           hackycorp.com
dns.names                                           www.hackycorp.com
dns.names                                   51-158-147-132.rev.poneytelecom.eu
dns.names                 66177e3f25e3ea0713807b1dc5f0b9df.hackycorp.com
dns.records.www.hackycorp.com.record_type   A
dns.records.www.hackycorp.com.resolved_at   2022-12-07T13:38:28.897260811Z
dns.records.66177e3f25e3ea0713807b1dc5f0b9df.hackycorp.com.record_type
                          A
dns.records.66177e3f25e3ea0713807b1dc5f0b9df.hackycorp.com.resolved_at
      2022-11-24T13:28:53.752976537Z
dns.records.51-158-147-132.rev.poneytelecom.eu.record_type                A
dns.records.51-158-147-132.rev.poneytelecom.eu.resolved_at      2022-11-
                                            23T18:11:31.875257521Z
dns.records.hackycorp.com.record_type                       A
dns.records.hackycorp.com.resolved_at  2022-11-20T13:27:58.738557514Z
dns.reverse_dns.names                       51-158-147-132.rev.poneytelecom.eu
dns.reverse_dns.resolved_at          2022-11-30T22:57:49.384047856Z
last_updated_at                             2022-12-09T16:28:33.885Z
```

22/SSH(tcp)

Attribute	Value
services.banner	SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
services.banner_hashes	sha256:989054422845f7fb4a0f578fbb62a589973974ff9b7310e0e
services.banner_hex	5353482d322e302d4f70656e5353485f372e397031204465626961
services.extended_service_name	SSH
services.observed_at	2022-12-09T16:28:28.089867361Z
services.perspective_id	PERSPECTIVE_TELIA
services.port	22
services.service_name	SSH
services.software.product	openssh
services.software.other.comment	Debian-10+deb10u2
services.software.source	OSI_APPLICATION_LAYER
services.software.uniform_resource_identifier	cpe:2.3:o:*:linux:*:*:*:*:*:*:*
services.software.part	o
services.software.product	linux
services.software.source	OSI_TRANSPORT_LAYER
services.software.uniform_resource_identifier	cpe:2.3:a:openbsd:openssh:7.9:p1:*:*:*:*:*
services.software.part	a
services.software.vendor	OpenBSD
services.software.product	OpenSSH
services.software.version	7.9
services.software.update	p1
services.software.other.family	OpenSSH
services.software.source	OSI_APPLICATION_LAYER
services.software.uniform_resource_identifier	cpe:2.3:o:debian:debian_linux:10.2:*:*:*:*:*:*
services.software.part	o
services.software.vendor	Debian
services.software.product	Linux
services.software.version	10.2
services.software.other.family	Linux
services.software.source	OSI_APPLICATION_LAYER
services.source_ip	167.94.146.59
services.ssh.endpoint_id.raw	SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
services.ssh.endpoint_id.protocol_version	2.0
services.ssh.endpoint_id.software_version	OpenSSH_7.9p1
services.ssh.endpoint_id.comment	Debian-10+deb10u2
services.ssh.kex_init_message.kex_algorithms	curve25519-sha256
services.ssh.kex_init_message.kex_algorithms	curve25519-sha256@libssh.org
services.ssh.kex_init_message.kex_algorithms	ecdh-sha2-nistp256
services.ssh.kex_init_message.kex_algorithms	ecdh-sha2-nistp384
services.ssh.kex_init_message.kex_algorithms	ecdh-sha2-nistp521
services.ssh.kex_init_message.kex_algorithms	diffie-hellman-group-exchange-sha256

Attribute	Value
services.ssh.kex_init_message.kex_algorithms	diffie-hellman-group16-sha512
services.ssh.kex_init_message.kex_algorithms	diffie-hellman-group18-sha512
services.ssh.kex_init_message.kex_algorithms	diffie-hellman-group14-sha256
services.ssh.kex_init_message.kex_algorithms	diffie-hellman-group14-sha1
services.ssh.kex_init_message.host_key_algorithms	rsa-sha2-512
services.ssh.kex_init_message.host_key_algorithms	rsa-sha2-256
services.ssh.kex_init_message.host_key_algorithms	ssh-rsa
services.ssh.kex_init_message.host_key_algorithms	ecdsa-sha2-nistp256
services.ssh.kex_init_message.host_key_algorithms	ssh-ed25519
services.ssh.kex_init_message.client_to_server_ciphers	chacha20-poly1305@openssh.com
services.ssh.kex_init_message.client_to_server_ciphers	aes128-ctr
services.ssh.kex_init_message.client_to_server_ciphers	aes192-ctr
services.ssh.kex_init_message.client_to_server_ciphers	aes256-ctr
services.ssh.kex_init_message.client_to_server_ciphers	aes128-gcm@openssh.com
services.ssh.kex_init_message.client_to_server_ciphers	aes256-gcm@openssh.com
services.ssh.kex_init_message.server_to_client_ciphers	chacha20-poly1305@openssh.com
services.ssh.kex_init_message.server_to_client_ciphers	aes128-ctr
services.ssh.kex_init_message.server_to_client_ciphers	aes192-ctr
services.ssh.kex_init_message.server_to_client_ciphers	aes256-ctr
services.ssh.kex_init_message.server_to_client_ciphers	aes128-gcm@openssh.com
services.ssh.kex_init_message.server_to_client_ciphers	aes256-gcm@openssh.com
services.ssh.kex_init_message.client_to_server_macs	umac-64-etm@openssh.com
services.ssh.kex_init_message.client_to_server_macs	umac-128-etm@openssh.com
services.ssh.kex_init_message.client_to_server_macs	hmac-sha2-256-etm@openssh.com
services.ssh.kex_init_message.client_to_server_macs	hmac-sha2-512-etm@openssh.com
services.ssh.kex_init_message.client_to_server_macs	hmac-sha1-etm@openssh.com
services.ssh.kex_init_message.client_to_server_macs	umac-64@openssh.com
services.ssh.kex_init_message.client_to_server_macs	umac-128@openssh.com
services.ssh.kex_init_message.client_to_server_macs	hmac-sha2-256
services.ssh.kex_init_message.client_to_server_macs	hmac-sha2-512
services.ssh.kex_init_message.client_to_server_macs	hmac-sha1
services.ssh.kex_init_message.server_to_client_macs	umac-64-etm@openssh.com
services.ssh.kex_init_message.server_to_client_macs	umac-128-etm@openssh.com
services.ssh.kex_init_message.server_to_client_macs	hmac-sha2-256-etm@openssh.com
services.ssh.kex_init_message.server_to_client_macs	hmac-sha2-512-etm@openssh.com
services.ssh.kex_init_message.server_to_client_macs	hmac-sha1-etm@openssh.com
services.ssh.kex_init_message.server_to_client_macs	umac-64@openssh.com
services.ssh.kex_init_message.server_to_client_macs	umac-128@openssh.com
services.ssh.kex_init_message.server_to_client_macs	hmac-sha2-256

Attribute	Value
services.ssh.kex_init_message.server_to_client_macs	hmac-sha2-512
services.ssh.kex_init_message.server_to_client_macs	hmac-sha1
services.ssh.kex_init_message.client_to_server_compression	none
services.ssh.kex_init_message.client_to_server_compression	zlib@openssh.com
services.ssh.kex_init_message.server_to_client_compression	none
services.ssh.kex_init_message.server_to_client_compression	zlib@openssh.com
services.ssh.kex_init_message.first_kex_follows	false
services.ssh.algorithm_selection.kex_algorithm	curve25519-sha256@libssh.org
services.ssh.algorithm_selection.host_key_algorithm	ecdsa-sha2-nistp256
services.ssh.algorithm_selection.client_to_server_alg_group.cipher	aes128-ctr
services.ssh.algorithm_selection.client_to_server_alg_group.mac	hmac-sha2-256
services.ssh.algorithm_selection.client_to_server_alg_group.compression	none
services.ssh.algorithm_selection.server_to_client_alg_group.cipher	aes128-ctr
services.ssh.algorithm_selection.server_to_client_alg_group.mac	hmac-sha2-256
services.ssh.algorithm_selection.server_to_client_alg_group.compression	none
services.ssh.server_host_key.fingerprint_sha256	4815235839a3ac471cb5327777f83c0a87e63a17435b7e5f5eee29
services.ssh.server_host_key.ecdsa_public_key.b	WsY12Ko6k+ez671VdpiGvGUdBrDMU7D2O848PifSYEs=
services.ssh.server_host_key.ecdsa_public_key.curve	P-256
services.ssh.server_host_key.ecdsa_public_key.gx	axfR8uEsQkf4vOblY6RA8ncDfYEt6zOg9KE5RdiYwpY=
services.ssh.server_host_key.ecdsa_public_key.gy	T+NC4v4af5uO5+tKfA+eFivOM1drMV7Oy7ZAaDe/UfU=
services.ssh.server_host_key.ecdsa_public_key.length	256
services.ssh.server_host_key.ecdsa_public_key.n	/////wAAAAD//////////7zm+q2nF56E87nKwvxjJVE=
services.ssh.server_host_key.ecdsa_public_key.p	/////wAAAAEAAAAAAAAAAAAAAAD///////////////8=
services.ssh.server_host_key.ecdsa_public_key.x	+SxKb83ZFcaoL64X173TJbLpirJymTDFJYvq4jN5FXA=
services.ssh.server_host_key.ecdsa_public_key.y	FNhzYBgs1vNAA5xNjjJQrbMEPp2tfn7MAEV7IYxWbRg=
services.ssh.hassh_fingerprint	b12d2871a1189eff20364cf5333619ee
services.transport_fingerprint.id	262
services.transport_fingerprint.os	CentOS
services.transport_fingerprint.raw	65160,64,true,MSTNW,1460,false,false
services.transport_protocol	TCP
services.truncated	false

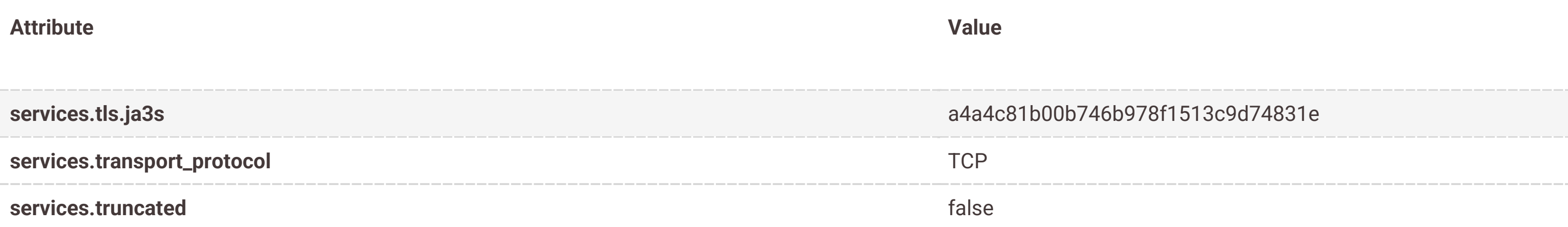
80/HTTP(tcp)

Attribute	Value
services.banner	HTTP/1.1 200 OK\r\nServer: nginx\r\nDate: <REDACTED>\r\nConte 020 02:55:52 GMT\r\nTransfer-Encoding: chunked\r\nConnection: ab_recon_09: 99d0738b-1e52-4a00-8885-b15894b2c79e\r\nConte
services.banner_hashes	sha256:a9b7577ca3886f6c57e39b9cd0593db0fbd63cdb70314ec
services.banner_hex	485454502f312e3120323030204f4b0d0a5365727665723a206e6 443e0d0a436f6e74656e742d547970653a20746578742f68746d6 2c2030312041707220323032302030323a35353a353220474d54 6368756e6b65640d0a436f6e6e656374696f6e3a206b6565702d6 3262382d3663220d0a70656e7465737465726c61625f7265636f6 6130302d383838352d6231353839346232633739650d0a436f6e
services.extended_service_name	HTTP
services.http.request.method	GET
services.http.request.uri	http://51.158.147.132/
services.http.request.headers.User_Agent	Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys
services.http.request.headers.Accept	*/*
services.http.response.protocol	HTTP/1.1
services.http.response.status_code	200
services.http.response.status_reason	OK
services.http.response.headers.Etag	W/"5e8402b8-6c"
services.http.response.headers.Last_Modified	Wed, 01 Apr 2020 02:55:52 GMT
services.http.response.headers.Connection	keep-alive
services.http.response.headers.Pentesterlab_recon_09	99d0738b-1e52-4a00-8885-b15894b2c79e
services.http.response.headers.Content_Type	text/html
services.http.response.headers.Server	nginx
services.http.response.headers.Date	<REDACTED>
services.http.response.body_size	108
services.http.response.body	<h1>Well done! You solved recon_06 </h1>\n\nThe key for this exe
services.http.response.body_hashes	sha256:33ee28c82cdd91676125bc06c3be0ec6e15f7907d52821b
services.http.response.body_hashes	sha1:a3f586c68517415f5779135a935b294e5e692838
services.http.response.body_hash	sha1:a3f586c68517415f5779135a935b294e5e692838
services.http.supports_http2	false
services.observed_at	2022-12-09T09:04:04.775240228Z
services.perspective_id	PERSPECTIVE_TATA
services.port	80
services.service_name	HTTP
services.software.uniform_resource_identifier	cpe:2.3:a:nginx:nginx:*:*:*:*:*:*:*:*
services.software.part	a
services.software.vendor	nginx
services.software.product	nginx

Attribute	Value
services.software.other.family	nginx
services.software.source	OSI_APPLICATION_LAYER
services.source_ip	167.94.138.45
services.transport_protocol	TCP
services.truncated	false

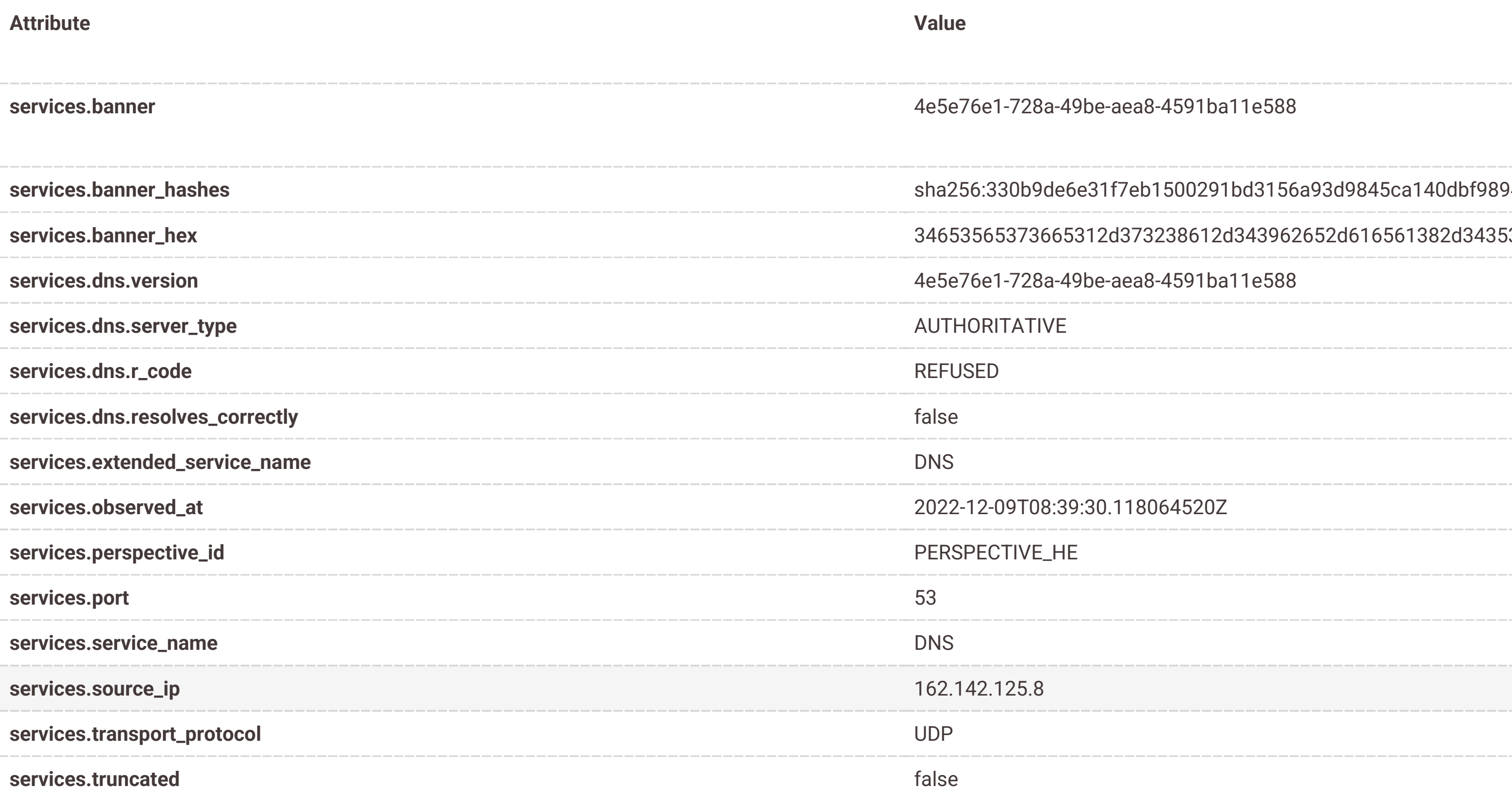
Attribute	Value
services.banner	HTTP/1.1 200 OK\r\nServer: nginx\r\nDate: <REDACTED>\r\nConte 020 03:25:09 GMT\r\nTransfer-Encoding: chunked\r\nConnection: lab_recon_09: 99d0738b-1e52-4a00-8885-b15894b2c79e\r\nConte
services.banner_hashes	sha256:be1ad42562ff33f8e8acaae474c587f7f8cb625a1632c249e
services.banner_hex	485454502f312e3120323030204f4b0d0a5365727665723a206e6 443e0d0a436f6e74656e742d547970653a20746578742f68746d6 2c2030312041707220323032302030333a32353a303920474d54 6368756e6b65640d0a436f6e6e656374696f6e3a206b6565702d6 3939352d3662220d0a70656e7465737465726c61625f7265636f6 6130302d383838352d6231353839346232633739650d0a436f6e
services.certificate	1d31f9c2bc4da2a16864e737571bc1dd7ab582c8d7e4a4b82b7d9
services.extended_service_name	HTTPS
services.http.request.method	GET
services.http.request.uri	https://51.158.147.132/
services.http.request.headers.User_Agent	Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys
services.http.request.headers.Accept	*/*
services.http.response.protocol	HTTP/1.1
services.http.response.status_code	200
services.http.response.status_reason	OK
services.http.response.headers.Last_Modified	Wed, 01 Apr 2020 03:25:09 GMT
services.http.response.headers.Server	nginx
services.http.response.headers.Connection	keep-alive
services.http.response.headers.Etag	W/"5e840995-6b"
services.http.response.headers.Content_Type	text/html
services.http.response.headers.Date	<REDACTED>
services.http.response.headers.Pentesterlab_recon_09	99d0738b-1e52-4a00-8885-b15894b2c79e
services.http.response.body_size	107
services.http.response.body	<h1>Well done! You solved recon_07</h1>\n\nThe key for this exe
services.http.response.body_hashes	sha256:5fd4faa28a439cd2628ed1f741a7ac7674a77714b055702
services.http.response.body_hashes	sha1:3bbf1cc3dcd1d16d09e95bc744dc9ec2bb46347d
services.http.response.body_hash	sha1:3bbf1cc3dcd1d16d09e95bc744dc9ec2bb46347d
services.http.supports_http2	false
services.jarm.fingerprint	3fd3fd15d3fd3fd21c3fd3fd3fd3fdc110bab2c0a19e5d4e587c17ce
services.jarm.cipher_and_version_fingerprint	3fd3fd15d3fd3fd21c3fd3fd3fd3fd
services.jarm.tls_extensions_sha256	c110bab2c0a19e5d4e587c17ce497b15
services.jarm.observed_at	2022-12-03T12:36:04.608838413Z
services.observed_at	2022-12-08T13:45:14.613010291Z
services.perspective_id	PERSPECTIVE_TATA
services.port	443
services.service_name	HTTP
services.software.uniform_resource_identifier	cpe:2.3:a:nginx:nginx:*:*:*:*:*:*:*:*
services.software.part	a
services.software.vendor	nginx
services.software.product	nginx

Attribute	Value
services.software.other.family	nginx
services.software.source	OSI_APPLICATION_LAYER
services.source_ip	167.94.138.45
services.tls.version_selected	TLSv1_2
services.tls.cipher_selected	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
services.tls.certificates.leaf_fp_sha_256	1d31f9c2bc4da2a16864e737571bc1dd7ab582c8d7e4a4b82b7d9
services.tls.certificates.chain_fps_sha_256	67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7
services.tls.certificates.chain_fps_sha_256	6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f99b9d47cf
services.tls.certificates.leaf_data.names	66177e3f25e3ea0713807b1dc5f0b9df.hackycorp.com
services.tls.certificates.leaf_data.names	hackycorp.com
services.tls.certificates.leaf_data.names	www.hackycorp.com
services.tls.certificates.leaf_data.subject_dn	CN=hackycorp.com
services.tls.certificates.leaf_data.issuer_dn	C=US, O=Let's Encrypt, CN=R3
services.tls.certificates.leaf_data.pubkey_bit_size	2048
services.tls.certificates.leaf_data.pubkey_algorithm	RSA
services.tls.certificates.leaf_data.tbs_fingerprint	29f7d41770219de5b7faa1c49d960235f3a8d06f696eec84e4f1e58
services.tls.certificates.leaf_data.fingerprint	1d31f9c2bc4da2a16864e737571bc1dd7ab582c8d7e4a4b82b7d9
services.tls.certificates.leaf_data.issuer.common_name	R3
services.tls.certificates.leaf_data.issuer.organization	Let's Encrypt
services.tls.certificates.leaf_data.issuer.country	US
services.tls.certificates.leaf_data.subject.common_name	hackycorp.com
services.tls.certificates.leaf_data.public_key.key_algorithm	RSA
services.tls.certificates.leaf_data.public_key.rsa.modulus	v3tkGi6VDiMB2KPnGDcTCvw/dMPxduro4N5E5i6J61+GA0gYcehV gGw8xxzYQ1xkQbxtpfwPmgD4Ctm5QDyUfSbDR9e51KAWTWTwj1 VWPcQpQJYIOzh/V8fGwb033b8JZCwz2iTWQJ6QzWY2l/IbdqCcu DBApHzrlp/9/6rKy2nRzDyhJy03QSQEU09T+CUJn7JFYs4ydlTVA4
services.tls.certificates.leaf_data.public_key.rsa.exponent	AAEAAQ==
services.tls.certificates.leaf_data.public_key.rsa.length	256
services.tls.certificates.leaf_data.public_key.fingerprint	a889e5de8fd70648efc29ac1ecbdd5cf2e1ee6aae011c5e4d75b12
services.tls.certificates.leaf_data.signature.signature_algorithm	SHA256-RSA
services.tls.certificates.leaf_data.signature.self_signed	false
services.tls.certificates.chain.fingerprint	67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613
services.tls.certificates.chain.subject_dn	C=US, O=Let's Encrypt, CN=R3
services.tls.certificates.chain.issuer_dn	C=US, O=Internet Security Research Group, CN=ISRG Root X1
services.tls.certificates.chain.fingerprint	6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f99b9d47cf7ff1c24f
services.tls.certificates.chain.subject_dn	C=US, O=Internet Security Research Group, CN=ISRG Root X1
services.tls.certificates.chain.issuer_dn	O=Digital Signature Trust Co., CN=DST Root CA X3
services.tls.server_key_exchange.ec_params.named_curve	29
services.tls.session_ticket.length	176
services.tls.session_ticket.lifetime_hint	86400



Attribute	Value
services.tls.ja3s	a4a4c81b00b746b978f1513c9d74831e
services.transport_protocol	TCP
services.truncated	false

53/DNS(udp)



Attribute	Value
services.banner	4e5e76e1-728a-49be-aea8-4591ba11e588
services.banner_hashes	sha256:330b9de6e31f7eb1500291bd3156a93d9845ca140dbf989
services.banner_hex	34653565373665312d373238612d343962652d616561382d34353
services.dns.version	4e5e76e1-728a-49be-aea8-4591ba11e588
services.dns.server_type	AUTHORITATIVE
services.dns.r_code	REFUSED
services.dns.resolves_correctly	false
services.extended_service_name	DNS
services.observed_at	2022-12-09T08:39:30.118064520Z
services.perspective_id	PERSPECTIVE_HE
services.port	53
services.service_name	DNS
services.source_ip	162.142.125.8
services.transport_protocol	UDP
services.truncated	false

ACTIVE RECONNAISSANCE

NMAP

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-11 09:02 EST
Nmap scan report for hackycorp.com (51.158.147.132)
Host is up (0.025s latency).
rDNS record for 51.158.147.132: 51-158-147-132.rev.poneytelecom.eu
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE         VERSION
22/tcp   open   ssh             OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
53/tcp   open   domain          (unknown banner: 4e5e76e1-728a-49be-aea8-4591ba11e588)
80/tcp   open   http            nginx
256/tcp  closed fw1-secureremote
443/tcp  open   ssl/http        nginx
```

```
8080/tcp closed http-proxy
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.93%I=7%D=12/11%Time=6395E30E%P=x86_64-pc-linux-
gnu%r(DNS
SF:VersionBindReqTCP,5F,"\0\]\0\x06\x85\0\0\x01\0\x01\0\x01\0\0\x07version
SF:\x04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\0\0\0%\$4e5e76e1-728a-49
SF:be-aea8-4591ba11e588\xc0\x0c\0\x02\0\x03\0\0\0\0\0\x02\xc0\x0c");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 45.20 seconds
```

GOBUSTER

```
gobuster dir -u hackycorp.com -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://hackycorp.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.3
[+] Timeout:                 10s
===============================================================
2022/12/11 09:04:40 Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 178] [--> http://hackycorp.com/admin/]
/images               (Status: 301) [Size: 178] [--> http://hackycorp.com/images/]
/index.html           (Status: 200) [Size: 16011]
/robots.txt           (Status: 200) [Size: 121]
/startpage            (Status: 301) [Size: 178] [--> http://hackycorp.com/startpage/]
Progress:                 4614                      /                        4615
(99.98%)=============================================================
==
2022/12/11 09:05:21 Finished
```

AMASS

```
amass enum -d hackycorp.com

0xff.a.hackycorp.com
0x07.a.hackycorp.com
```

```
0x04.a.hackycorp.com
66177e3f25e3ea0713807b1dc5f0b9df.hackycorp.com
0x08.a.hackycorp.com
hackycorp.com
0x0d.a.hackycorp.com
0x03.a.hackycorp.com
z.hackycorp.com
0x0f.a.hackycorp.com
0x06.a.hackycorp.com
www.hackycorp.com
balancer.hackycorp.com
0x0a.a.hackycorp.com
mgmt.hackycorp.com
0x01.a.hackycorp.com
gw.hackycorp.com
ns1.hackycorp.com
0x00.a.hackycorp.com
statistics.hackycorp.com
assets.hackycorp.com

OWASP Amass v3.20.0                    https://github.com/OWASP/Amass
--------------------------------------------------------------------------------
21 names discovered - cert: 2, dns: 1, scrape: 6, archive: 12
--------------------------------------------------------------------------------
ASN: 12876 - Online SAS
        51.158.0.0/16          20   Subdomain Name(s)
ASN: 0 - Not routed
        18.160.0.0/15          4    Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database
```