Penetration Test Evidence Log

Exploit: Reconnaissance and Attack Surface Mapping
Target: 18.214.228.138
Analysis Date: 2026-03-02 15:32:25 UTC

Target Intelligence & Service Discovery

Target Information

Field	Value
IP / Hostname / URL	18.214.228.138, https://18.214.228.138:443
Target Type	Network host
Cloud Provider	AWS
Reverse DNS	ec2-18-214-228-138.compute-1.amazonaws.com
ASN / Org	AS14618 Amazon.com, Inc.
Location	Ashburn, Virginia, US
WHOIS Organization	Amazon Technologies Inc.

Open Ports & Services

Port	Service	Banner / Version
443	https	—

Service Map

- **HTTPS on port 443:**
  - The service is using a self-signed TLS certificate with no Common Name or Subject Alternative Names.
  - A generic "Admin Panel" was detected at the path `/admin/`.

Tool Commands & Responses

whois

Command: `whois 18.214.228.138`
Purpose: Retrieves registration and network allocation information for an IP address.
Result Summary: The IP address is allocated to Amazon Technologies Inc. and hosted on AWS in Ashburn, Virginia.

```
None
IP Address    : 18.214.228.138
Reverse DNS   : ec2-18-214-228-138.compute-1.amazonaws.com
ASN / Org     : AS14618 Amazon.com, Inc.
ISP           : Amazon.com, Inc.
Location      : Ashburn, Virginia, US
Cloud Provider: AWS
Hosting       : Yes

WHOIS Data:
  NetRange:       18.32.0.0 - 18.255.255.255
  CIDR:           18.32.0.0/11, 18.64.0.0/10, 18.128.0.0/9
  NetName:        AT-88-Z
  NetHandle:      NET-18-32-0-0-1
  Parent:         NET18 (NET-18-0-0-0-0)
  NetType:        Direct Allocation
  Organization:   Amazon Technologies Inc. (AT-88-Z)
  RegDate:        2019-10-07
  Updated:        2021-02-10
  Ref:            https://rdap.arin.net/registry/ip/18.32.0.0

  OrgName:        Amazon Technologies Inc.
```

```
OrgId:          AT-88-Z
Address:        410 Terry Ave N.
City:           Seattle
StateProv:      WA
PostalCode:     98109
Country:        US
RegDate:        2011-12-08
Updated:        2024-01-24
Ref:            https://rdap.arin.net/registry/entity/AT-88-Z

OrgAbuseHandle: AEA8-ARIN
OrgAbuseName:   Amazon EC2 Abuse
```

`httpx`

Command: `httpx -u 18.214.228.138 -p 443`
Purpose: Probes for running web servers on specified ports.
Result Summary: A web server responding over HTTPS was discovered on port 443.

None

```
Discovered Endpoints (1):
  - https://18.214.228.138:443
```

`wafw00f`

Command: `wafw00f https://18.214.228.138:443`
Purpose: Detects and fingerprints Web Application Firewall (WAF) products.
Result Summary: No Web Application Firewall was detected on the target.

None

```
WAF Detected: No
```

Port Scan (`nmap -sV`)

Command: `nmap -sV 18.214.228.138`
Purpose: Scans a target to discover open ports and the services running on them.
Result Summary: The scan found port 443 (https) open on the target.

```
None
PORT     SERVICE          VERSION / BANNER
-------- ----------------
----------------------------------------
443      https
```

SSL Certificate Analysis (`nmap`)

Command: `nmap -p 443 --script ssl-cert 18.214.228.138`
Purpose: Analyzes the SSL/TLS certificate presented by a service.
Result Summary: The service on port 443 uses an expired, self-signed certificate with no Common Name.

```
None
Port 443:
  Common Name (CN)    : (empty)
  Subject Alt Names   : (none)
  Issuer              : (unknown)
  Expiry              : (unknown)
  Days Until Expiry   : -1
  Self-Signed         : True
  Weak TLS Versions   : None detected
```

Directory Fuzzing (`ffuf`)

Command: `ffuf -w wordlist.txt -u https://18.214.228.138:443/FUZZ`
Purpose: Fuzzes for hidden files and directories on a web server.
Result Summary: A generic admin panel was discovered at the path `/admin/`.

```
None
  Product     : Admin Panel (Generic)
  Port        : 443
```

```
Path        : /admin/
HTTP Status : 200
```

Attack Surface Inventory

Discovered Endpoints

None

```
GET  https://18.214.228.138:443/admin/  [200]
GET  https://18.214.228.138:443
```

Technologies Detected

- AWS
- Admin Panel (Generic)

None

Reconnaissance Summary & Risk Assessment

Findings Narrative

The overall attack surface of the target at `18.214.228.138` is assessed as **minimal**. A single open TCP port, 443, hosts a single web endpoint. No other network services, API endpoints, or web application parameters were identified during the initial reconnaissance phase. The target resolves to an AWS host, indicating cloud-based infrastructure. The limited exposure focuses all subsequent testing efforts on the identified web application.

The sole service is HTTPS on port 443, hosting a web application that includes a generic administrative panel. The absence of other exposed services (SSH, FTP, databases) suggests an attempt to limit external exposure. However, the presence of a web service inherently introduces risks associated with vulnerabilities such as XSS or SQLi. The security of the entire system is dependent on this single web application.

Notable findings include the open port 443 and an administrative interface at `/admin/` responding with HTTP 200. This confirms a management portal that is likely a high-value target for attackers. Critically, **no WAF is present**, meaning the application is directly exposed to automated and manual attacks without a protective filtering layer.

Several significant security misconfigurations were observed. The TLS certificate is self-signed, expired, and lacks a Common Name or Subject Alternative Names — making the server unverifiable and vulnerable to man-in-the-middle attacks. The exposed admin panel at `/admin/` represents an additional misconfiguration, as such interfaces should be protected by network-level access controls in addition to authentication.

Evidence Summary

Reconnaissance Activities Performed:
IP intelligence gathering, TCP port scanning, TLS certificate analysis, and web directory fuzzing against `18.214.228.138`.

Key Discoveries:
A single open port, 443 (HTTPS), was found. The running web application exposes an administrative panel at `/admin/`. The host is AWS-based (US region). No other services, endpoints, or parameters were discovered.

Security Observations:

- No WAF detected
- HTTPS certificate is expired and self-signed with no subject name configured
- No weak TLS versions detected

Recommendations

1. **Replace TLS certificate** — Install a valid certificate from a trusted CA to ensure data integrity and prevent MITM attacks.
2. **Deploy a WAF** — Protect the web application from automated scanning and common web attacks.
3. **Restrict `/admin/` access** — Limit network access to the admin panel by IP allowlist or VPN.
4. **Conduct web application assessment** — Perform a focused vulnerability assessment on the exposed administrative interface.

Final Status

Analysis complete: Reconnaissance completed
Status: Attack surface mapped — 1 endpoint, 1 service, 0 parameters discovered