## CyberRealm Sentinels  - Guardians of Partnered Firms

# Penetration Test Report for Design World

**9/29/25**

Content

## 1. Executive Summary

A comprehensive penetration test of Design World's assigned hosts and networks was conducted by the security engineering team on 9/29/2025. The test was successful in identifying critical security weaknesses. These findings have a negative impact on the firm's current security posture. The identified critical security vulnerabilities also directly expose the firm's intellectual property and sensitive data, thereby placing it at immediate risk. A series of simulated attacks were conducted to assess the vulnerability of critical security weaknesses to unauthorized access. The results of these attacks demonstrated that determined adversaries could exploit these identified weaknesses to gain unauthorized access to sensitive design data and intellectual property. If these identified high-risk issues are not addressed, Design World's intellectual property will be directly exposed to potential compromise.

**Key Findings (critical to low)**

- Exploitable vulnerabilities in Microsoft Windows SMBv1 (MS17-010 / EternalBlue family, including CVE-2017-0143 and related CVEs) have high-to-critical severity ratings (CVSS 8.1–9.8) and can allow full compromise of affected systems.
- Multiple instances of medium strength SSL cipher suites (SWEET32) and deprecated RC4 cipher suites, which can be exploited to intercept and decrypt sensitive communications.
- Configuration weaknesses and patching deficiencies that increase susceptibility to widely known exploits.

### Business Impact of Unaddressed Identified Critical Security Weaknesses

The exploitation of these identified critical vulnerabilities by organized cybercriminals could result to, among others, the following:

- Continued and unabated loss of financial revenue of proprietary design intellectual property.
- Loss of competitive advantage and lasting reputational damage.
- Potential non-compliance with regulatory and contractual obligations.
- Complete compromise of the Design World’s global enterprise network.

### Remediation Roadmap

- Immediate (0–30 Days): Apply patches to mitigate SMBv1 vulnerabilities; disable weak SSL cipher suites; enhance network segmentation.
- Short-Term (30–90 Days): Review and Strengthen patch management processes; implement multi factor authentication; conduct security awareness training.
- Long-Term (6–12 Months): Deploy network intrusion detection systems; continuous vulnerability management; regular penetration testing cycles.

**The Penetration Test Report**

## 2. Assessment Scope

Scope as defined in the Vulnerability Assessment Plan (VAP):

Figure 1 - Table of In-Scope Systems

| Instance Name | IP Address | Operating System | Role / Function | Resources |
|---|---|---|---|---|
| DW-DC-OL1 | 172.16.1.205 | Windows Server 2016 | Domain Controller / Core Server | 16 vCPUs, 200GB, 16GB RAM |
| DW-WIN10-2 | 172.16.1.41 | Windows 10 Pro | User Workstation | 4 vCPUs, 200GB, 16GB RAM |
| DW-WIN10-1 | 172.16.1.93 | Windows 10 Pro | User Workstation | 4 vCPUs, 200GB, 16GB RAM |
| DW-FS-OL1 | 172.16.1.138 | Windows Server 2016 | File Server (per instance list) | 16 vCPUs, 200GB, 16GB RAM |
| Design-World-FA25-OL-1-Ubuntu-4 | 172.16.1.62 | Ubuntu Linux | Linux Server (general-purpose) | 4 vCPUs, 200GB, 16GB RAM |

|  |  |  |  |  |
|---|---|---|---|---|
| Design-World-FA25-OL-1-Ubuntu-3 | 172.16.1.94 | Ubuntu Linux | Linux Server (general-purpose) | 4 vCPUs, 200GB, 16GB RAM |
| Design-World-FA25-OL-1-Ubuntu-2 | 172.16.1.202 | Ubuntu Linux | Linux Server (general-purpose) | 4 vCPUs, 200GB, 16GB RAM |
| Design-World-FA25-OL-1-Ubuntu-1 | 172.16.1.183 | Ubuntu Linux | Linux Server (general-purpose) | 4 vCPUs, 200GB, 16GB RAM |

## 3. Methodology

The penetration test was conducted using a blend of automated scanning tools and manual exploitation techniques. The process involved multiple phases:

- Reconnaissance to identify hosts, services, and potential vulnerabilities.
- Vulnerability scanning targeting known CVEs, configuration weaknesses, and cryptographic flaws.
- Exploitation attempts of critical vulnerabilities, including Microsoft SMBv1 vulnerabilities (CE-2017 series).
- Post exploitation analysis to evaluate lateral movement potential and data access risks.

### 4. Tested Exploitable Vulnerabilities

The following exploitable vulnerabilities found during the vulnerability testing phase of the project were tested as follows:

Figure 2 - Tested exploitable vulnerabilities

| ID | CVE | Severity | **CVSS v3.1** | Title | Affected Host |
|---|---|---|---|---|---|
| F-001 | CVE-2016-2183 | High | 7.5 | SSL Medium Strength Cipher Suites Supported (SWEET32) | 172.16.1.41 |
| F-008 | CVE-2016-2183 | High | 7.5 | SSL Medium Strength Cipher Suites Supported (SWEET32) | 172.16.1.93 |
| F-015 | CVE-2016-2183 | High | 7.5 | SSL Medium Strength Cipher Suites Supported (SWEET32) | 172.16.1.138 |
| F-020 | CVE-2013-2566 | Medium | 6.5 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) | 172.16.1.138 |
| F-024 | CVE-2017-0267 CVE-2017-0268 CVE-2017-0269 CVE-2017-0270 CVE-2017-0271 CVE-2017-0272<br>CVE-2017-0273 CVE-2017-0274 CVE-2017-0275 CVE-2017-0276 CVE-2017-0277 CVE-2017-0278 CVE-2017-0279 CVE-2017-0280 | Critical | 9.8 | Microsoft Windows SMBv1 Multiple Vulnerabilities | 172.16.1.205 |
| F-025 | CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 | High | 8.1 | MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) | 172.16.1.205 |
| F-026 | CVE-2016-2183 | High | 7.5 | SSL Medium Strength Cipher Suites Supported (SWEET32) | 172.16.1.205 |

| | | | | | |
|---|---|---|---|---|---|
| F-031 | CVE-2013-2566 CVE-2015-2808 | Medium | 5.9 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) | 172.16.1.205 |

## Penetration Test Report — Network Scan Summary

The security engineering team conducted Nmap TCP scans on the eight hosts that were identified and listed. Furthermore, the Nmap service detection output of 9/29/25 was reviewed and interpreted. The findings and recommendations that follow are based exclusively on the scan outputs. The complete scan files are cited in the appendix.

It has been observed that several Windows hosts expose Remote Desktop (RDP) on TCP/3389. One of these hosts, identified as 172.16.1.205, functions as a domain controller (Active Directory) and exposes multiple AD services (DNS, LDAP, Kerberos, SMB, RDP). Exposed AD services represent the highest risk because if an attacker can reach and abuse them, they can escalate to domain compromise. A subsequent investigation of the scanned hosts revealed two possible scenarios. Firstly, in the case of other scanned hosts, no open TCP ports were returned, suggesting either that they were closed or filtered. Secondly, in some cases, only RDP/MSRPC was detected.

**Top priorities (critical → low):**

1. Protect the domain controller (172.16.1.205): restrict network access to LDAP/Kerberos/AD ports. (Critical)
2. Restrict RDP (3389) exposure on all hosts; enforce Network Level Authentication (NLA) and MFA. (High)

3. Harden certificate and patch posture where Windows builds are older (investigate product versions present). (Medium)

## 5. Findings (per-host)

### i) <u>**Host: 172.16.1.205 — Domain Controller (Highest risk)**</u>

**Evidence (from scan):** LDAP (389), Global Catalog (3268), Kerberos (88), DNS (53), NetBIOS/SMB (139/445), msrpc (135), RDP (3389). Nmap reports Windows Server 2016 Standard Evaluation (build 14393) and AD domain designworld.com, computer name DW-DC-OL1. Message signing appears enabled/required.

**Risk: Critical** — exposure of AD services to networks that can be reached by an attacker allows credential abuse, LDAP enumeration, Kerberos attacks, and potential domain compromise.

**Impact:** Full domain compromise, data exfiltration, account takeover, persistence.

**Recommendations (immediate & tactical):**

- Restrict network access: ensure LDAP (389/636), Kerberos (88), SMB (445/139), RPC (135), and Global Catalog (3268/3269) are reachable **only** from trusted management networks (jump hosts, internal subnets) and not broadly routable. Implement firewall rules (host-based + network).

- If LDAP is required externally, use LDAPS (636) behind an authenticated gateway or VPN; do NOT expose plain LDAP to untrusted networks.
- Move AD management behind an admin jump host and require multi-factor authentication for admin access.
- Verify that this is not an evaluation system in production; license/evaluate and patch to a supported build. The Standard Evaluation string suggests an evaluation install which may not have production SLAs.
- Harden DC: apply latest Windows Server 2016 security updates, enable Windows Defender/AV, and ensure auditing/central SIEM collection for AD anomalies.
- Rotate any service account credentials if there is suspicion of prior exposure.

ii) **Hosts: 172.16.1.41 and 172.16.1.93 — Windows endpoints with RDP & msrpc (High)**

**Evidence:** Both show TCP/3389 open with RDP; /135 msrpc open. DW-WIN10-2 (172.16.1.41) and DW-WIN10-1 (172.16.1.93) report Windows product version 10.0.19041 and present server certificate CNs DW-WIN10-2.designworld.com and DW-WIN10-1.designworld.com.

**Risk: High** — exposed RDP increases risk of brute force, RDP vulnerability exploitation, lateral movement.

**Impact:** Remote code execution / unauthorized remote desktop access → lateral movement to domain assets.

**Recommendations:**

- Block or limit RDP exposure at network perimeter. Allow RDP only via VPN or an authenticated bastion/jump host.
- Ensure **Network Level Authentication (NLA)** is enforced on RDP and configure RDP to use TLS + updated certificates. Verify TLS config and disable deprecated ciphers. (Scan shows TLS certs in use; confirm NLA is enabled in RDP settings.)
- Implement account lockout policies, strong passwords and MFA where possible.
- Keep Windows 10 builds patched; 10.0.19041 corresponds to Windows 10 2004/20H1 — ensure current security patches are applied.

iii) **Host: 172.16.1.138 — RDP open (High / Medium)**

**Evidence:** 3389 open, RDP certificate present: CN=DW-FS-OL1.designworld.com. Product Version reported as 10.0.14393 (older build).

**Risk: High/Medium** — RDP exposure plus an older Windows build (10.0.14393 corresponds to older Windows Server/Windows 10 baseline) may indicate reduced patching.

**Recommendations:**

- Same RDP protections as above (VPN/jump host, NLA, MFA).
- Investigate OS build/version and apply required updates; 10.0.14393 should be evaluated for support/end-of-support status and patched.

### iv) **Hosts: 172.16.1.62, 172.16.1.94, 172.16.1.183, 172.16.1.202 — no open ports / closed (Informational / Low)**

**Evidence:** Nmap reports all 1000 scanned TCP ports closed or in ignored states (conn-refused).

**Risk: Low/Informational** — firewalling is blocking external scans; keep monitoring for configuration drift.

**Recommendations:**

- Continue to firewall these hosts; perform periodic authenticated scanning or internal scans to confirm services expected to run are configured securely.

### v) **Cross-cutting observations & recommendations**

1. **Network segmentation:** Ensure Domain Controllers and management services are on a protected network segment accessible only to admin subnets/jump hosts. Exposed AD services are the single largest risk.
2. **RDP posture:** RDP appears widely available on multiple hosts. Enforce NLA, require MFA, restrict via VPN/firewall, and consider removing RDP where unnecessary.

3. **Patch & Version Management:** Identify hosts reporting older product versions (10.0.14393, 10.0.19041) and ensure patch baselines are up-to-date. Aging builds may lack mitigations for critical vulnerabilities.
4. **Certificates & TLS:** Several hosts present TLS certs on RDP. Confirm certificate chains are valid and use modern cipher suites. Rotate/regenerate certs if weak keys or short lifetimes are used.
5. **Logging & Monitoring:** Enable centralized logging for all AD and RDP authentication events; trigger alerts on unusual Kerberos/LDAP queries or repeated RDP failures.

## 6. Suggested Remediation Roadmap (recommended order)

### Immediate (within 24–72 hours)

- Block public/unnecessary access to the domain controller's AD ports (389, 88, 445, 3268, 135) at perimeter and internal firewalls.
- Restrict RDP (3389) access to internal management networks only; disable direct external RDP.
- Enable NLA and enforce account lockout, strong passwords, and MFA for remote logins.

### Short term (1–2 weeks)

- Harden DC: apply missing security updates, verify evaluation license status, ensure AD backup/restore plans in place.
- Verify TLS configuration and rotate certificates as needed.

**Medium term (1–2 months)**

- Deploy admin jump hosts / bastion for privileged access. Move all AD admin work to jump hosts.
- Conduct credential and Kerberos hardening (service account review, implement constrained delegation only where needed).
- Run authenticated vulnerability scans and password audits to find weak credentials and missing patches.

**Long term**

- Implement Zero Trust principles for internal access to critical services. Network micro-segmentation around DCs. Continuous monitoring and periodic red-team exercises.

## 7. Conclusion

The largest and most immediate risk is the domain controller (172.16.1.205) exposing AD services. Remediation prioritizes isolating and protecting that host, followed by hardening any hosts exposing RDP. Upon containment of the immediate exposure, the above specified remediation roadmap will be followed, and a scheduled in-depth authenticated assessment will be conducted.

## 8. Next Steps

Upon completion of this Penetration Test Report, the next step is to produce a comprehensive Project Change Requests (PCR) with updated system design with updated drawings and a Security Hardening Plan.

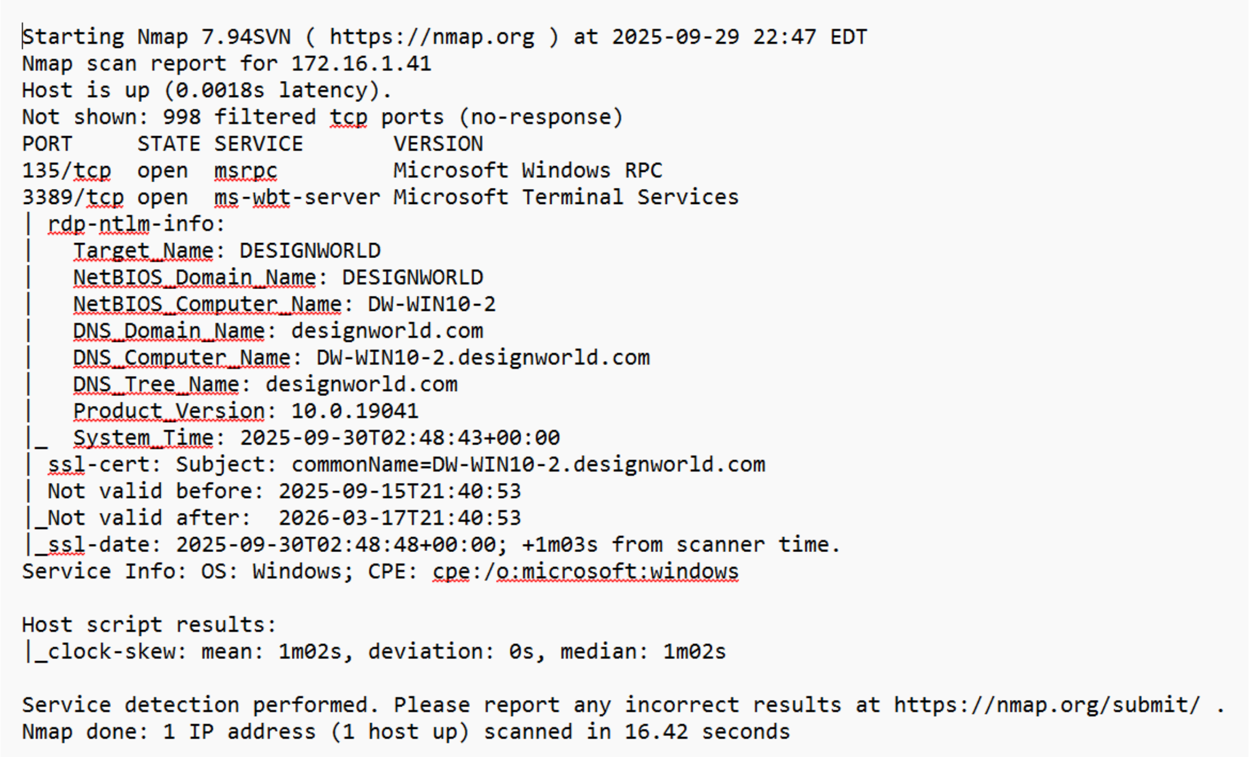
**Appendix - Evidence (detailed uploaded scan files below)**

Summary of Evidence (uploaded scan files)

- Nmap scan — 172.16.1.41 (RDP + msrpc).
- Nmap scan — 172.16.1.62 (no open TCP ports).
- Nmap scan — 172.16.1.93 (RDP + msrpc).
- Nmap scan — 172.16.1.94 (no open TCP ports).
- Nmap scan — 172.16.1.138 (RDP; older build).
- Nmap scan — 172.16.1.183 (no open TCP ports).
- Nmap scan — 172.16.1.202 (no open TCP ports).
- Nmap scan — 172.16.1.205 (Domain Controller — LDAP, Kerberos, DNS, SMB, RDP).

## Detailed Evidence (detailed uploaded scan files)

- Nmap scan — 172.16.1.41 (RDP + msrpc).

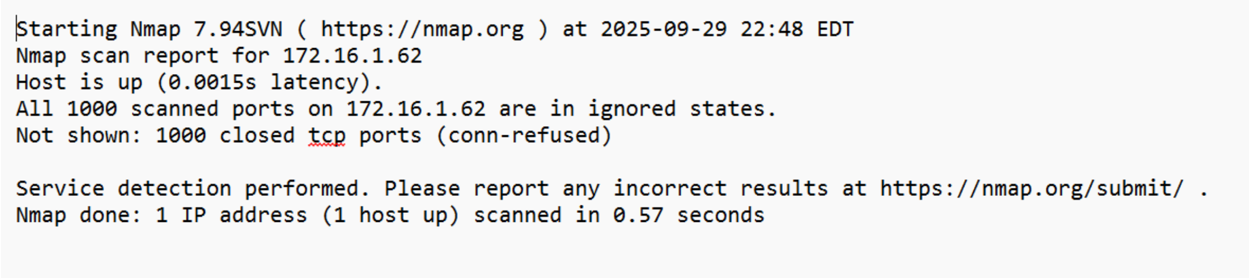


```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-29 22:47 EDT
Nmap scan report for 172.16.1.41
Host is up (0.0018s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: DESIGNWORLD
|   NetBIOS_Domain_Name: DESIGNWORLD
|   NetBIOS_Computer_Name: DW-WIN10-2
|   DNS_Domain_Name: designworld.com
|   DNS_Computer_Name: DW-WIN10-2.designworld.com
|   DNS_Tree_Name: designworld.com
|   Product_Version: 10.0.19041
|_  System_Time: 2025-09-30T02:48:43+00:00
| ssl-cert: Subject: commonName=DW-WIN10-2.designworld.com
| Not valid before: 2025-09-15T21:40:53
|_Not valid after:  2026-03-17T21:40:53
|_ssl-date: 2025-09-30T02:48:48+00:00; +1m03s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1m02s, deviation: 0s, median: 1m02s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.42 seconds
```

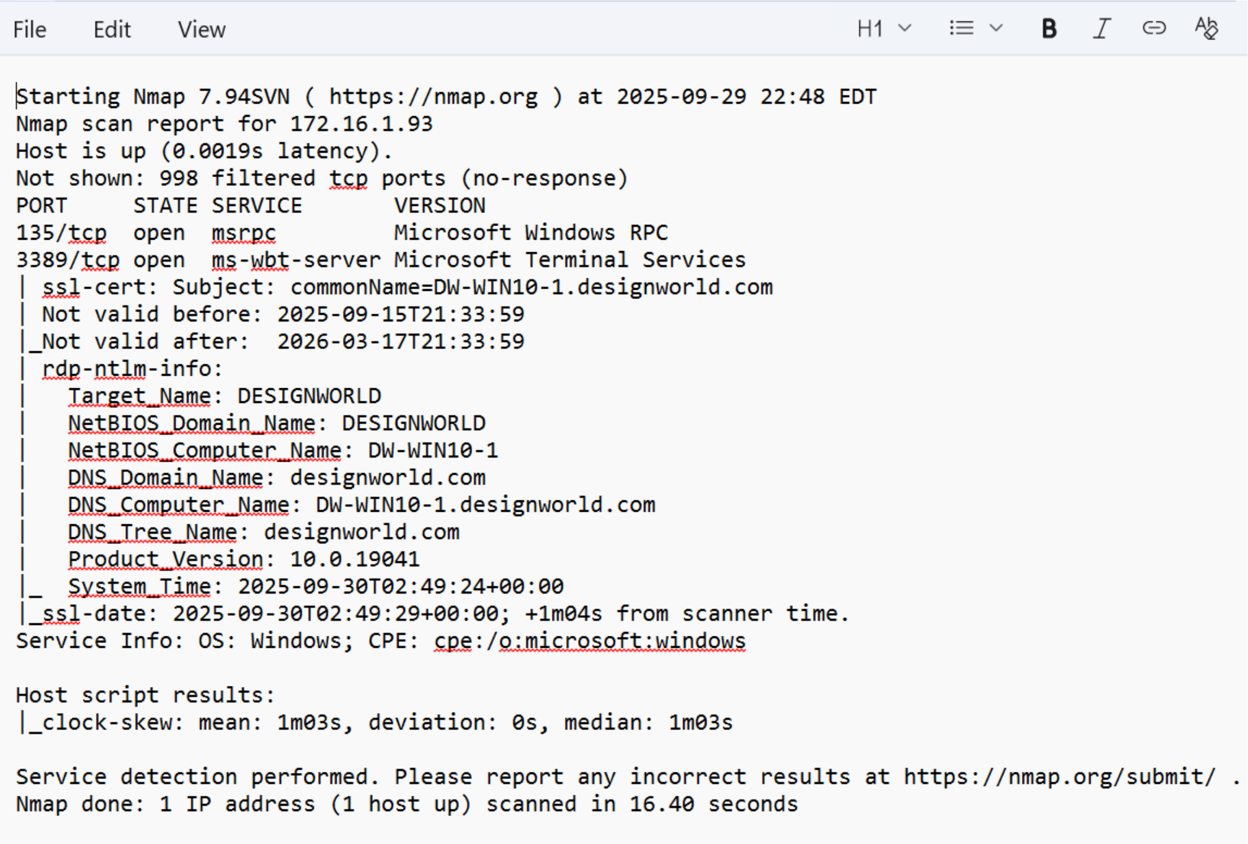
- Nmap scan — 172.16.1.62 (no open TCP ports).



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-29 22:48 EDT
Nmap scan report for 172.16.1.62
Host is up (0.0015s latency).
All 1000 scanned ports on 172.16.1.62 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

- Nmap scan — 172.16.1.93 (RDP + msrpc).

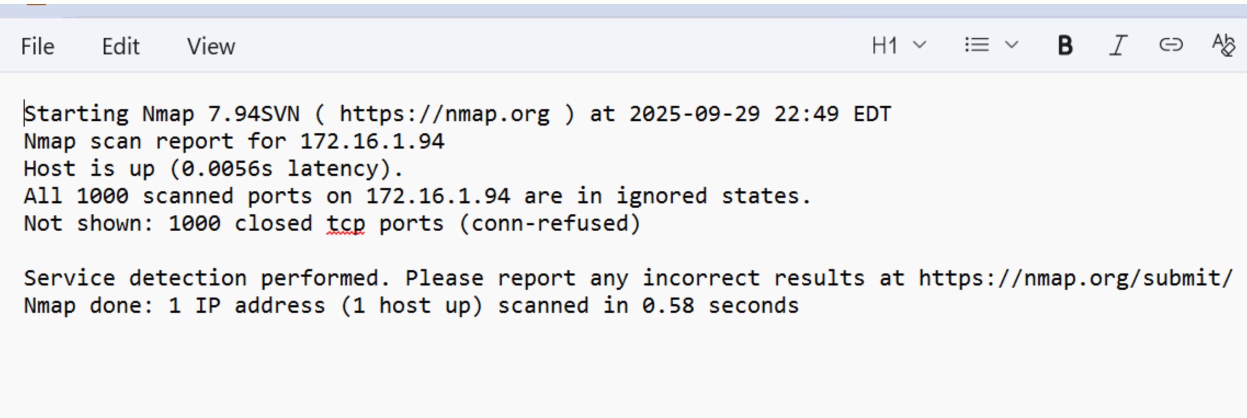


```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-29 22:48 EDT
Nmap scan report for 172.16.1.93
Host is up (0.0019s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DW-WIN10-1.designworld.com
| Not valid before: 2025-09-15T21:33:59
|_Not valid after:  2026-03-17T21:33:59
| rdp-ntlm-info:
|   Target_Name: DESIGNWORLD
|   NetBIOS_Domain_Name: DESIGNWORLD
|   NetBIOS_Computer_Name: DW-WIN10-1
|   DNS_Domain_Name: designworld.com
|   DNS_Computer_Name: DW-WIN10-1.designworld.com
|   DNS_Tree_Name: designworld.com
|   Product_Version: 10.0.19041
|_  System_Time: 2025-09-30T02:49:24+00:00
|_ssl-date: 2025-09-30T02:49:29+00:00; +1m04s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1m03s, deviation: 0s, median: 1m03s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.40 seconds
```

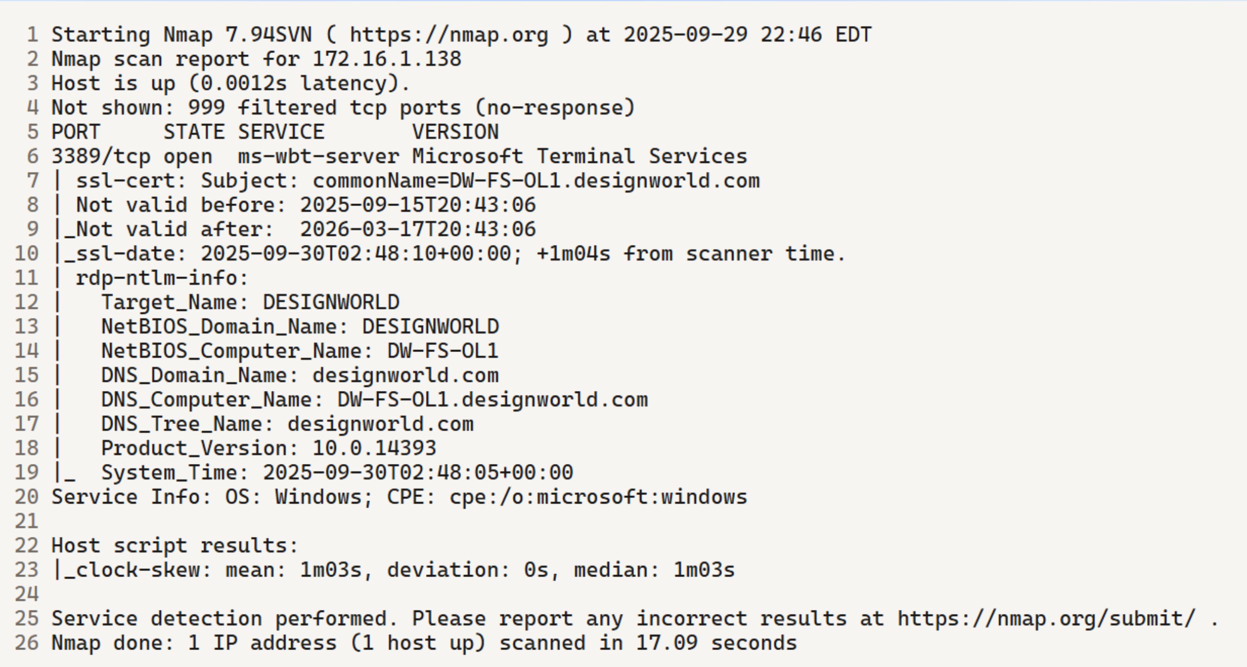
- Nmap scan — 172.16.1.94 (no open TCP ports).



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-29 22:49 EDT
Nmap scan report for 172.16.1.94
Host is up (0.0056s latency).
All 1000 scanned ports on 172.16.1.94 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

- Nmap scan — 172.16.1.138 (RDP; older build).

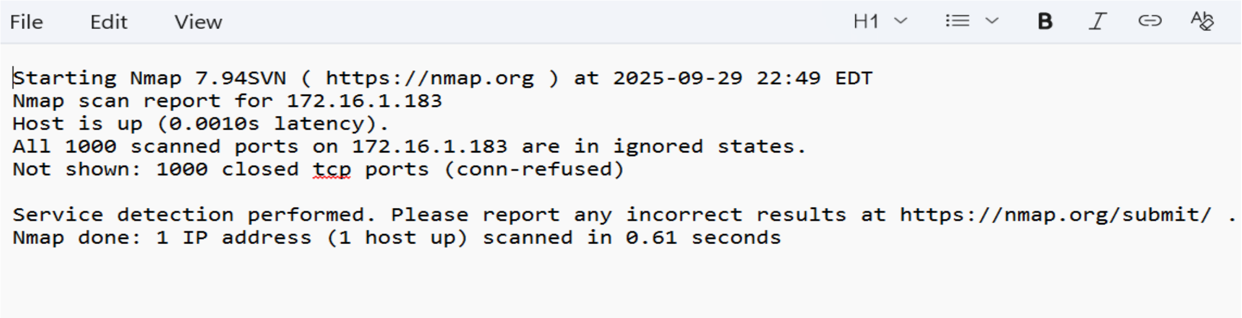


```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-29 22:46 EDT
Nmap scan report for 172.16.1.138
Host is up (0.0012s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DW-FS-OL1.designworld.com
| Not valid before: 2025-09-15T20:43:06
|_Not valid after:  2026-03-17T20:43:06
|_ssl-date: 2025-09-30T02:48:10+00:00; +1m04s from scanner time.
| rdp-ntlm-info:
|   Target_Name: DESIGNWORLD
|   NetBIOS_Domain_Name: DESIGNWORLD
|   NetBIOS_Computer_Name: DW-FS-OL1
|   DNS_Domain_Name: designworld.com
|   DNS_Computer_Name: DW-FS-OL1.designworld.com
|   DNS_Tree_Name: designworld.com
|   Product_Version: 10.0.14393
|_  System_Time: 2025-09-30T02:48:05+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1m03s, deviation: 0s, median: 1m03s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.09 seconds
```

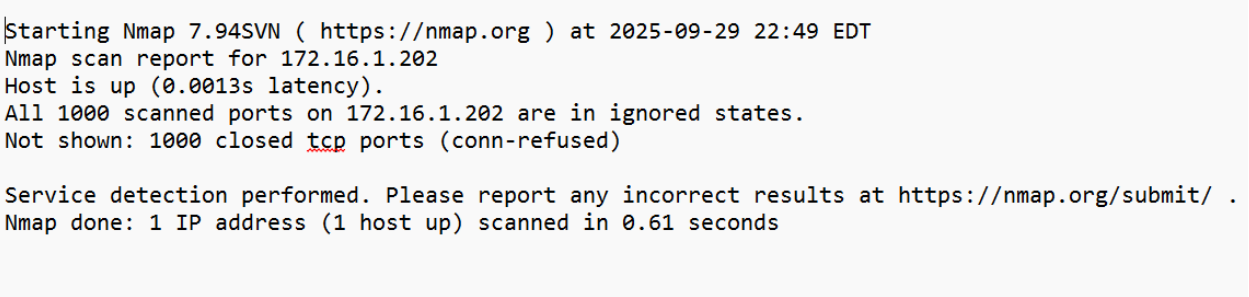
- Nmap scan — 172.16.1.183 (no open TCP ports).



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-29 22:49 EDT
Nmap scan report for 172.16.1.183
Host is up (0.0010s latency).
All 1000 scanned ports on 172.16.1.183 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
```

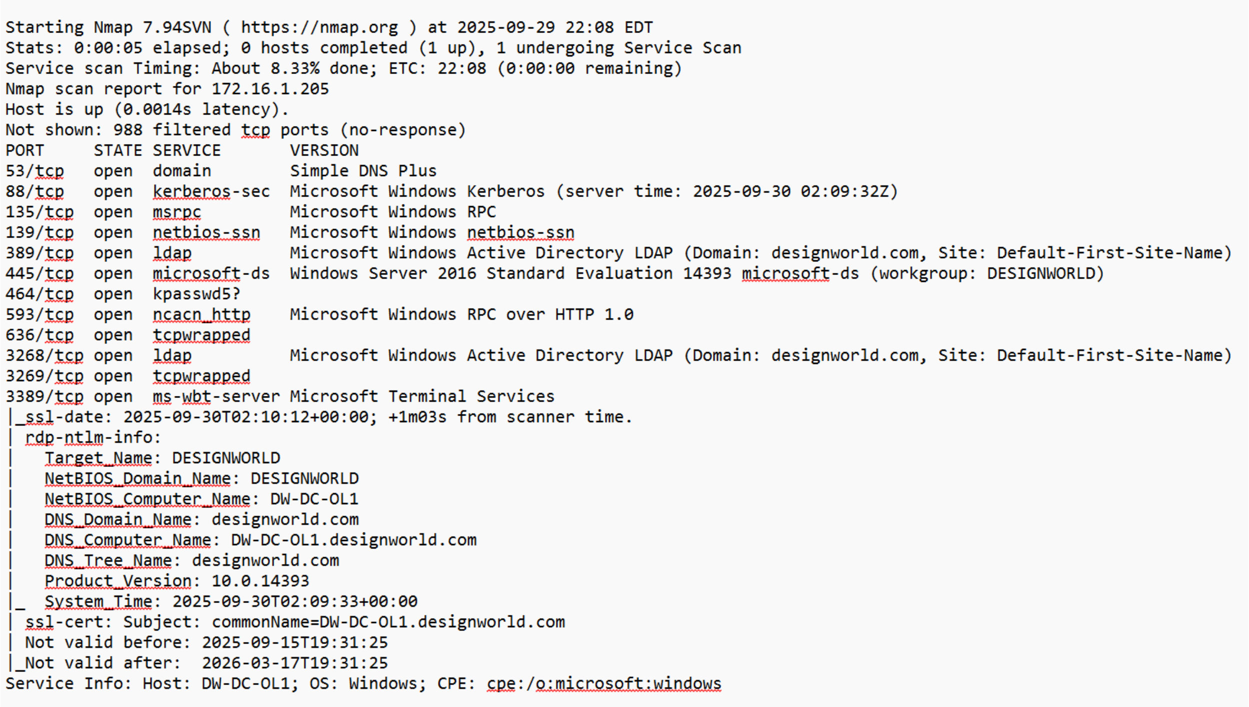
- Nmap scan — 172.16.1.202 (no open TCP ports).



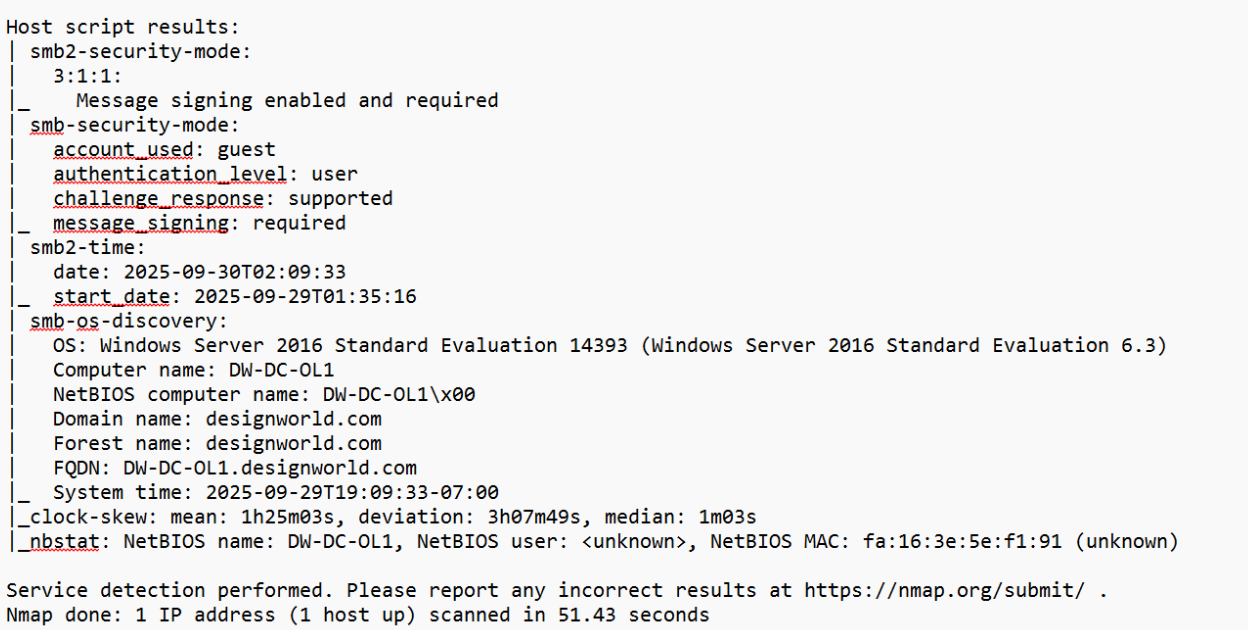
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-29 22:49 EDT
Nmap scan report for 172.16.1.202
Host is up (0.0013s latency).
All 1000 scanned ports on 172.16.1.202 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
```

- Nmap scan — 172.16.1.205 (Domain Controller — LDAP, Kerberos, DNS, SMB, RDP).



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-29 22:08 EDT
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 8.33% done; ETC: 22:08 (0:00:00 remaining)
Nmap scan report for 172.16.1.205
Host is up (0.0014s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-09-30 02:09:32Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: designworld.com, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds  Windows Server 2016 Standard Evaluation 14393 microsoft-ds (workgroup: DESIGNWORLD)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: designworld.com, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-09-30T02:10:12+00:00; +1m03s from scanner time.
| rdp-ntlm-info:
|   Target_Name: DESIGNWORLD
|   NetBIOS_Domain_Name: DESIGNWORLD
|   NetBIOS_Computer_Name: DW-DC-OL1
|   DNS_Domain_Name: designworld.com
|   DNS_Computer_Name: DW-DC-OL1.designworld.com
|   DNS_Tree_Name: designworld.com
|   Product_Version: 10.0.14393
|_  System_Time: 2025-09-30T02:09:33+00:00
| ssl-cert: Subject: commonName=DW-DC-OL1.designworld.com
| Not valid before: 2025-09-15T19:31:25
|_Not valid after:  2026-03-17T19:31:25
Service Info: Host: DW-DC-OL1; OS: Windows; CPE: cpe:/o:microsoft:windows
```



```
Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-time:
|   date: 2025-09-30T02:09:33
|_  start_date: 2025-09-29T01:35:16
| smb-os-discovery:
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
|   Computer name: DW-DC-OL1
|   NetBIOS computer name: DW-DC-OL1\x00
|   Domain name: designworld.com
|   Forest name: designworld.com
|   FQDN: DW-DC-OL1.designworld.com
|_  System time: 2025-09-29T19:09:33-07:00
|_clock-skew: mean: 1h25m03s, deviation: 3h07m49s, median: 1m03s
|_nbstat: NetBIOS name: DW-DC-OL1, NetBIOS user: <unknown>, NetBIOS MAC: fa:16:3e:5e:f1:91 (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.43 seconds
```