

网络安全需要掌握什么课程

网络安全（Cybersecurity）是一个跨学科领域，涉及计算机科学、数学、法律、心理学等多方面知识。以下是系统化、层次化的课程学习路径，从基础 → 核心 → 进阶 → 专项，帮助你构建完整知识体系。

一、基础必备（本科低年级水平）

课程	为什么学	推荐资源
计算机组成原理	理解硬件如何工作，底层漏洞利用基础	《计算机组成与设计》(Patterson)
操作系统（Linux 重）	90% 攻防在 Linux 环境下	《现代操作系统》(Tanenbaum)、鸟哥私房菜
计算机网络	网络协议是攻击面核心	《计算机网络：自顶向下方法》(Kurose)
数据结构与算法	写工具、分析恶意代码必备	LeetCode、《算法导论》
离散数学 + 密码学数学基础	理解加密算法原理	数论、有限域、椭圆曲线

二、核心专业课（本科高年级 / 硕士）

课程	重点内容	实践建议
密码学（Cryptography）	对称/非对称加密、哈希、数字签名、PKI	做 RSA 手撕实现、AES-CTR 模式分析
网络安全（Network Security）	TCP/IP 漏洞、Wireshark 抓包、防火墙、IDS/IPS	搭建 VLAN + Snort 实验
系统安全（System Security）	缓冲区溢出、ROP、ASLR、SELinux	《Shellcoder's Handbook》
Web 安全	XSS、CSRF、SQLi、SSRF、RCE	OWASP Top 10 + PortSwigger Web Academy

课程	重点内容	实践建议
逆向工程与恶意软件分析	IDA Pro、Ghidra、动态调试、病毒行为分析	Practical Malware Analysis 实验

三、进阶实战类（红蓝对抗方向）

课程/方向	关键技能	平台推荐
渗透测试（Penetration Testing）	信息收集 → 漏洞利用 → 提权 → 横向 → 持久化	Hack The Box、TryHackMe、Vulnhub
红队攻防（Red Team）	C2 框架、免杀、域渗透	Cobalt Strike、Empire、Metasploit
蓝队防御（Blue Team）	SIEM、EDR、日志分析、事件响应	ELK Stack、Splunk、Microsoft Sentinel
数字取证（Digital Forensics）	内存取证、硬盘镜像、时间线分析	Autopsy、Volatility

四、专项方向（选择 1-2 个深耕）

方向	代表课程/证书	适合人群
物联网安全（IoT Security）	固件逆向、Zigbee 协议分析	嵌入式爱好者
云安全（Cloud Security）	AWS/Azure 安全、容器逃逸、K8s 安全	云原生工程师
移动安全（Mobile Security）	Android/iOS 逆向、Hook 框架	移动开发转安全
工控安全（ICS/SCADA）	Modbus/DNP3 协议、PLC 编程	工业互联网
AI 安全	提示注入、模型窃取、投毒攻击	AI 研究员

五、国际认证路线（加分项）

证书	难度	含金量
CompTIA Security+	★★★☆	入门

证书**难度****含金量**

CEH (Certified Ethical Hacker) ★★☆ 基础渗透

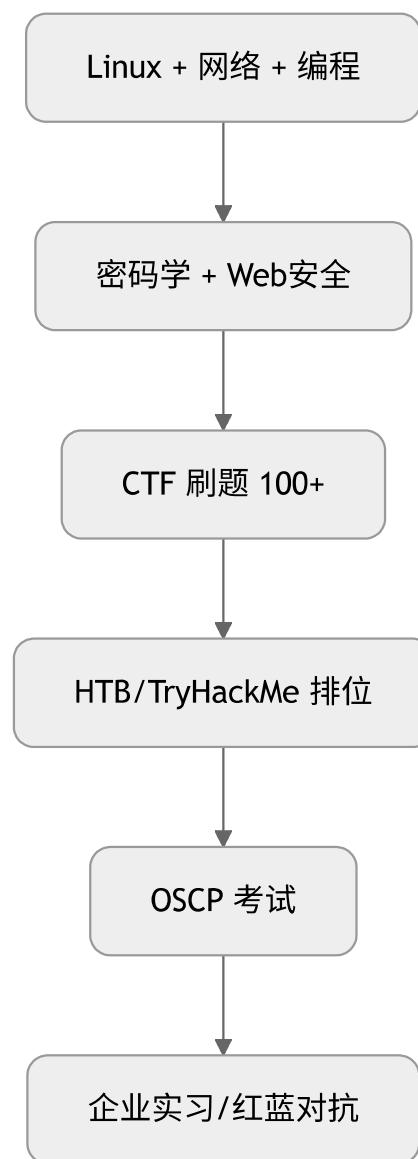
OSCP (Offensive Security Certified Professional) ★★★★ 含金量最高 (需实操 24h 考试)

CISSP ★★★ 管理岗

CCSP ★★★ 云安全

GREM ★★★★ 逆向工程

六、自学实战路线图（6-18 个月）



七、编程语言要求

语言	用途
Python	写扫描器、自动化脚本（必会）
C/C++	写 Exploit、Shellcode
Bash/PowerShell	系统管理、横向移动
Go/JavaScript	现代 C2 框架、Web 攻防

总结：核心课程清单（Top 10）

1. 操作系统（Linux）
2. 计算机网络
3. 密码学
4. Web 应用安全
5. 系统安全与漏洞利用
6. 逆向工程
7. 渗透测试方法学
8. 网络协议分析（Wireshark）
9. 恶意软件分析
10. 安全编程（Secure Coding）

建议：

- **70% 时间实战**（CTF、靶场、真实项目）
- **30% 时间理论**（看书、写笔记）
- 加入**安全社区**：FreeBuf、看雪论坛、X 安全圈、Discourse 论坛

需要我帮你定制**1年学习计划表**或**CTF入门靶机推荐**吗？

定制一年学习计划表

以下是「网络安全零基础 → OSCP 级实战」一年（52 周）学习计划表，专为每周可投入**15–25 小时**的自学者设计。

目标：第 52 周能独立拿下 Hack The Box Pro Labs / OSCP 考试

前提：已会 Linux 基础命令 + 简单 Python 脚本

节奏：每周 3-4 天学习 + 1 天 CTF/靶场实战 + 周末复盘



一年 52 周学习计划表（2026 年 1 月启动示例）

周次	主题	核心课程/书籍	实战任务	里程碑
1-2	Linux 强化	鸟哥私房菜 Ch1-10	搭建 Kali + Ubuntu 双系统	能流畅用 tmux + vim + grep
3-4	网络基础	《计算机网络：自顶向下》Ch1-4	Wireshark 抓 HTTP/TCP 包	画出三次握手时序图
5-6	Python 安全编程	Automate the Boring Stuff Ch1-12	写端口扫描器 + Banner 抓取	GitHub 提交第 1 个工具
7-8	Web 基础与 Burp Suite	PortSwigger Academy (免费)	完成 SQLi / XSS 全部 Lab	Burp 能熟练拦截修改
9-10	密码学入门	Crypto101.pdf + Coursera Cryptography I	手撕 RSA 加密小程序	理解 p*q=n 与陷门
11-12	CTF 入门 (Web)	CTFtime / 纳努 CTF 平台	刷 50 道 Web 题 (★★★)	排名进入平台前 30%
13	期中复盘周	整理笔记 + 写 1 篇技术博客	重做前 12 周错题	发布在 GitHub Pages



第 2 季度（14-26 周）——核心攻防

周次	主题	资源	实战	里程碑
14-15	SQL 注入进阶	PortSwigger SQLi Labs	盲注 + 时间注入脚本	写自动化 SQLi 工具
16-17	XSS 与 CSRF	OWASP XSS Game	构建反射/存储/DOM XSS	绕过 5 种常见 WAF
18-19	文件上传 + RCE	HackTricks File Upload	写 PHP/ASP 一句话木马	GetShell 3 种姿势

周次	主题	资源	实战	里程碑
20– 21	缓冲区溢出 (x86)	《Shellcoder's Handbook》 Ch1–3	SLMail / Protostar Stack0–5	成功溢出 EIP
22– 23	格式化字符串 + ROP 基础	LiveOverflow Bilibili 系列	Protostar Format/Stack	手写 ROP chain
24– 25	信息收集与枚举	HackTricks Enumeration	Nmap 脚本 + Enum4linux	写自动化信息收集脚本
26	季度复盘	整理 2 个完整 Web 渗透报告	模拟客户交付	能写出 CVE 级别 PoC

第 3 季度 (27–39 周) —— 渗透测试方法学

周次	主题	资源	实战	里程碑
27– 28	Metasploit 框架	Offensive Security MSF 课程	利用 5 个真实 CVE	理解 auxiliary/exploit/payload
29– 30	提权 (Linux/Windows)	GTFOBins + 林间有风提权	10 台靶机本地提权	掌握 DirtyCow/Sudo
31– 32	横向移动	HackTricks Lateral Movement	Pass-the-Hash + Kerberoast	域内 GetSystem
33– 34	免杀与 C2 框架	Cobalt Strike 试用 / Covenant	写 Python 免杀 Loader	绕过 Windows Defender
35– 36	TryHackMe 完整路径	THM: Starting Point → Attacking Enterprise	完成 3 条完整路径	拿到 THM Rank Top 10%
37– 38	HTB 入门机器	Hack The Box Starting Point	拿下 10 台 Easy 机器	提交第 1 个血 (First Blood)

周次	主题	资源	实战	里程碑
39	季度复盘	写 1 份红队报告 (模板)	模拟 APT 攻 击链	能独立出报告

🏆 第 4 季度 (40–52 周) —— OSCP 冲刺

周次	主题	资源	实战	里程碑
40–41	PWK 课程 (购买 OSCP Lab)	Offensive Security PWK PDF + Video	完成 30+ Lab 机器	提交 Lab 报告
42–43	HTB Pro Labs	Dante / Rastalabs / Offshore	完整打通 1 个 Pro Lab	理解企业级渗透
44–45	缓冲区溢出进阶 (x64)	Exploit Education Nebula/Fusion	手写 64 位 ROP	绕过 ASLR/NX
46–47	AD 域渗透实战	THM: Attacktive Directory	血祭 3 台域控	DCSync 拿下域
48–49	OSCP 模拟考试	PG Practice / Proving Grounds	连续 24h 拿下 70 分	写完整渗透报告
50	弱点修复与防御思维	蓝队视角复盘所有漏洞	写 5 条加固建议	理解“防得住”
51	最终复盘 + 心态调整	整理所有笔记为 Notion 知识库	模拟 OSCP 考试流程	预约考试
52	OSCP 考试周	24h 实战 + 报告	目标：70 分通过	获得 OSCP 认书

📚 资源清单 (全免费/低成本)

类型	资源	链接
免费靶场	TryHackMe、Hack The Box、Vulnhub	tryhackme.com / hackthebox.com
CTF 平台	CTFtime、picoCTF、纳努	ctftime.org
文档	HackTricks、GTFOBins	hacktricks.xyz

类型	资源	链接
视频	LiveOverflow、ippsec、STÖK	YouTube/Bilibili
证书	OSCP (\$1499 含 90 天 Lab)	offensive-security.com

🎯 每周固定动作（养成习惯）

text

周一：学习新知识 (2h)
 周二：写代码/工具 (2h)
 周三：做 Lab/靶机 (3h)
 周四：CTF 刷题 (2h)
 周五：复盘 + 写博客 (1.5h)
 周末：自由攻防 / 社区答疑

📈 进度追踪表（复制到 Notion/Excel）

周次	完成任务	机器数量	博客/报告	证书
1	<input type="checkbox"/> Linux 基础	0	<input type="checkbox"/>	
...
52	<input type="checkbox"/> OSCP 通过	100+	12 篇	OSCP

💡 特别提醒

1. 第 26 周和第 52 周必须写完整渗透测试报告（客户可交付级别）
2. 每季度至少参加 1 次线下/线上 CTF 比赛
3. 加入 1 个安全社区（如 X 安全圈、看雪、Discourse）
4. 从第 30 周开始准备简历 + GitHub 作品集

需要我帮你生成：

- Notion 模板（带进度条 + 资源链接）

- 每周提醒邮件模板
- OSCP 报告 Word 模板
- CTF 靶机推荐清单（100 台）

回复「我要 Notion 模板」或「发我 CTF 清单」即可领取！

作为EE工程的辅助技能，能不能精简点

以下是为 EE（电子/电气工程）工程师 量身定制的 「网络安全辅助技能」 精简版 1 年计划
(总投入 ≤ 8 小时/周，仅 26 周，不追求 OSCP，目标是 能看懂固件漏洞、调试 IoT 设备、参与硬件安全测试)。

🎯 目标 (EE 专属)

- 读懂 固件 Bin 文件
- 用 JTAG/SWD 调试芯片
- 发现 UART 后门、固件提权
- 写 简单 Exploit 辅助硬件逆向
- 不做 Web 渗透、不打 CTF、不考 OSCP

📅 26 周精简计划 (每周 6–8 小时)

周次	主题	核心内容 (EE 视角)	实战 (1 台设备)	产出
1–2	Linux + 工具链	Kali 安装、Binwalk、GDB	拆 1 台路由器	<code>ls /dev/tty*</code> 找到 UART
3–4	固件提取与分析	Binwalk、firmware.mod.kit	提取 TP-Link 固件	得到 <code>squashfs-root</code>
5–6	UART 通信	焊 UART、screen/minicom	接路由器 UART	拿到 <code>root@OpenWrt:/#</code>
7–8	二进制基础	file、strings、hexdump	分析 <code>httpd</code> 二进制	找到 <code>admin:admin</code> 硬编码
9–10	JTAG 调试	OpenOCD + GDB	用 Bus Pirate 连 STM32	暂停程序、读寄存器
11–12	缓冲区溢出 (嵌入式)	《嵌入式安全》Ch3	溢出路由器 <code>boa</code> 服务	拿到 shell

周次	主题	核心内容 (EE 视角)	实战 (1台设备)	产出
13	期中复盘	写 1 页硬件逆向报告	拍照 + 标注引脚	PDF 存档
14–15 固件修改与回刷 dd、mtd、sysupgrade 改密码后回刷 设备正常启动				
16–17 Python 自动化 写 UART 交互脚本 自动登录 + 执行命令 <code>router_auto.py</code>				
18–19 常见 IoT 漏洞 Mirai、CVE-2018-0296 复现 1 个真实 CVE 写 200 字说明				
20–21 无线协议嗅探 <code>monitor mode</code> + Wireshark 抓 Zigbee/Wi-Fi 包 看到明文密码				
22–23 硬件安全标准 ISO 21434、IEC 62443 读 1 篇标准摘要 能说出 3 个要求				
24–25 项目整合 选 1 台设备全流程 提取 → 逆向 → 提权 → 报告 5 页 PPT				
26 成果展示 内部分享 / 简历更新 演示 1 次 “会固件安全”写进简历				

🛠 必备硬件 (总预算 < 1500 元)

设备	用途	价格
1 台旧路由器 (TP-Link WR841N)	练手	50 元
USB-TTL 模块 (CH340)	UART	10 元
Bus Pirate / Shikra	JTAG/SWD	200 元
逻辑分析仪 (8 通道)	抓 SPI/I2C	100 元

📚 核心资源 (全免费)

类型	资源
文档	IOActive 固件逆向手册
视频	LiveOverflow 「Firmware」系列 (B站)
工具	Binwalk、Ghidra、OpenOCD、Radare2
社区	看雪论坛 - 硬件安全、RT-Thread 社区

🏅 最终产出 (可写进简历)

“具备嵌入式设备固件逆向能力，能通过 UART/JTAG 提取并分析固件，发现硬编码凭据与缓冲区溢出漏洞，完成完整硬件安全评估流程。”

💡 EE 专属建议

建议	原因
跳过 Web 安全	你不做网站
跳过域渗透	你不碰 AD
专注 UART + Binwalk	90% 硬件安全从这开始
每周只练 1 台设备	深入比广度重要

需要我发你：

- 26 周 Notion 模板（带硬件接线图）
- 5 台推荐练手设备清单（带购买链接）
- 固件分析报告 Word 模板（EE 版）

回复「发 Notion 模板」即可领取！