PABLO CYBERSEC

PCP CREDENTIALS

Cartilha do Candidato

PabloCyberSec Certification Program (PCP)







Central de Certificações · pablocybersec.com.br
Versão 1.0 · Novembro de 2026

Sobre o programa PCP

O **PabloCyberSec Certification Program (PCP)** é a estrutura oficial da PabloCyberSec para reconhecer, registrar e validar competências em segurança ofensiva. Cada credencial exige **três fases**: exame técnico, laboratório prático com flags escondidas e entrevista ao vivo com professores e instrutores. O objetivo é certificar quem sabe fazer, explicar e agir com ética.

Princípios

- Prática acima de decoreba: cenários, logs, código e saídas de ferramentas.
- Autoria verificável: as três fases se confirmam mutuamente.
- Ética e legalidade: toda atividade ocorre em ambiente autorizado.
- Privacidade por padrão: validação pública com o mínimo de dados (LGPD).

As credenciais

Credencial	Exame (Fase 1)	Duração	Nota mín.	Flags (Fase 2)	Entrevista
PCPH · Júnior	30 questões	60 min	70%	4 de 5	Sim
PCCP · Pleno	30 questões	90 min	75%	6 de 8	Sim
PCSP · Sênior	10 teoria com código + 20 práticas	150 min	80%	8 de 10	Sim

PCPH · JÚNIOR	Professional Junior Penetration Tester
PCCP · PLENO	Professional Certified Penetration Tester
PCSP · SÊNIOR	Professional Certified Senior Penetration Tester

Validade das credenciais: 2 anos. Podem ser revogadas em caso de fraude ou violação do código de conduta. A validação é pública em pablocybersec.com.br (página Validar certificado).

As três fases

Fase 1 · Exame técnico

Prova online com cronômetro, tentativa única e correção no servidor. **PCPH e PCCP:** 30 questões objetivas de múltipla escolha com cenários, código e saídas de ferramentas. **PCSP:** 10 questões de teoria com código (revisão de código, falhas não óbvias) e 20 questões 100% práticas (logs, saídas, cenários de ataque e defesa). O gabarito não é divulgado; você recebe sua nota e o desempenho por domínio.

Fase 2 · Laboratório de flags

Uma aplicação web criada para o exame contém flags escondidas no formato `PCP{...}`. As flags são **únicas para cada candidato**. Você tem 48 horas após o primeiro acesso e precisa encontrar o mínimo exigido pelo seu nível. Todo o laboratório é isolado; atacar qualquer outro alvo é falta gravíssima.

Fase 3 · Entrevista ao vivo

Conversa com professores e instrutores da PabloCyberSec para verificar habilidades ao vivo: como você chegou às flags, como justificaria um achado, como lidaria com escopo e dados pessoais. Esperam-se clareza, método e ética.

Fluxo resumido

1. Inscrição	2. Fase 1	3. Fase 2	4. Fase 3	5. Certificado
Instrutores criam seu código de candidato	Exame online	Laboratório de flags (48 h)	Entrevista ao vivo	Emissão com código de validação pública

Domínios avaliados

Nível	Domínios e pesos aproximados
PCPH	Fundamentos 15% · Redes 20% · Linux 15% · Web/OWASP 25% · Criptografia e senhas 10% · Ética e LGPD 10% · Relatórios 5%
PCCP	Aplicações web e APIs 35% · Infraestrutura e AD 20% · Escalada de privilégio 10% · Redes e TLS 10% · Criptografia 5% · Detecção e logs 10% · Metodologia e risco 10%
PCSP	Teoria com código 33% · Prática AD, nuvem e contêineres 25% · Prática web avançado e APIs 25% · Prática detecção, resposta e relatórios 17%

Regras, conduta e ética

- Faça as fases pessoalmente. Não receba ajuda de terceiros nem use IA durante as fases, salvo autorização expressa.
- Não copie, fotografe, compartilhe ou divulgue questões, flags ou soluções. Flags idênticas entre candidatos são detectadas.
- Atue somente no ambiente indicado (/ctf/). Sem força bruta massiva, DoS ou varreduras agressivas.
- Nunca ataque o site oficial, a hospedagem, outros candidatos ou terceiros. Isso é crime (Lei 12.737/2012) e causa banimento.
- Se encontrar uma falha real na plataforma, pare e comunique ao e-mail de contato. Divulgação responsável será reconhecida.
- Guarde seu código de candidato; ele é pessoal e intransferível.

Termos de uso e LGPD (resumo)

Controlador: PabloCyberSec. **Dados tratados:** nome, e-mail, nível, código, horários, respostas, pontuação, flags enviadas, resultado da entrevista, dados do certificado e logs de segurança (IP). **Bases legais:** execução do processo solicitado (art. 7º, V), legítimo interesse para prevenção a fraudes (art. 7º, IX) e consentimento para divulgação pública do nome completo (art. 7º, I).

Retenção: avaliação até 24 meses; certificado enquanto válido e até 5 anos para comprovação; logs até 6 meses. **Direitos (art. 18):** acesso, correção, anonimização/eliminação, portabilidade, informação sobre compartilhamento e revogação de consentimento. Solicitações: contato@pablocybersec.com.br.

Na validação pública aparecem apenas nome abreviado, nível, datas e status, salvo se você autorizar a divulgação completa. Os textos completos estão em Termos de Uso e Política de Privacidade no site.

Como estudar

- PCPH: redes (TCP/IP, DNS, HTTP), Linux, OWASP Top 10, senhas e hashes, escopo e ética.
- PCCP: explore aplicações web e APIs em laboratórios legais, treine análise de logs, AD, TLS, privilégios locais e CVSS com contexto.
- PCSP: pratique revisão de código em várias linguagens, leitura de saídas e logs reais, raciocínio sob ambiguidade e comunicação de risco.
- Em todos: pratique documentar evidências e explicar o raciocínio em voz alta. Será pedido na entrevista.

Prova de exemplo (lógica)

Estas questões são **apenas ilustrativas** do estilo de raciocínio cobrado. **Não fazem parte do banco real de provas.** O gabarito comentado está nas últimas páginas. Tente resolver antes de olhar.

PCPH · JÚNIOR Professional Junior Penetration Tester

1. Um servidor expõe as portas 22, 80 e 443. A política diz: 'somente serviços web podem ser acessíveis pela internet'. Qual porta contraria a política?

A) 22/tcp (SSH)
B) 80/tcp (HTTP)
C) 443/tcp (HTTPS)
D) Nenhuma delas

2. Qual senha tende a resistir melhor a um ataque de dicionário?

A) Pablo2024
B) qwerty123
C) cafe-lua-rio-trem-verde-47
D) P@ssw0rd

3. Premissas: (1) Todo administrador possui MFA. (2) Maria possui MFA. Conclusão: Maria é administradora. Essa conclusão é:

A) Válida
B) Inválida: afirma o consequente
C) Válida apenas se Maria for gerente
D) Impossível avaliar sem os logs

4. Seu escopo autorizado é 10.0.0.0/24 e você nota que o host 10.0.1.15 aparenta estar vulnerável. O que fazer?

A) Testar rapidamente, é só uma verificação
B) Não testar; registrar a observação e comunicar o contratante
C) Ignorar e apagar as anotações
D) Compartilhar com colegas para validar

PCCP · PLENO Professional Certified Penetration Tester

5. Com o token do usuário 11, a chamada GET /api/users/10 retorna 200 com os dados do usuário 10. Qual a hipótese principal?

A) BOLA/IDOR (falha de autorização por objeto)
B) XSS refletido
C) SQL Injection cega
D) Protocolo TLS fraco

6. Um cookie de sessão tem HttpOnly e Secure. Qual ataque o HttpOnly NÃO impede?

A) Leitura do cookie por document.cookie
B) CSRF, pois o navegador ainda envia o cookie automaticamente
C) Envio do cookie por HTTP sem criptografia
D) Captura do cookie em Wi-Fi aberto via HTTP

7. RDP (3389) exposto na internet, NLA desativado e sem política de bloqueio. Qual a ordem de recomendação mais coerente?

A) Habilitar logs; mudar a porta; manter exposto

B) Remover a exposição direta (VPN/firewall); habilitar NLA e MFA; política de bloqueio; monitorar

C) Política de bloqueio; liberar a porta para todos; desligar o NLA

D) Apenas trocar o papel de parede da máquina

8. O login responde 'Usuário não encontrado' ou 'Senha incorreta', conforme o caso. Qual o problema?

A) Enumeração de usuários

B) SQL Injection

C) XXE

D) Clickjacking

PCSP · SÊNIOR Professional Certified Senior Penetration Tester

9. Analise o trecho. Qual a falha?

```
$stored = '0e462097431906509019562988736854';
if (md5($_POST['p']) == $stored) { login(); }
```

A) Type juggling: '==' trata strings '0e...' como número 0; usar hash_equals/=== e password_hash

B) SQL Injection

C) XSS armazenado

D) Apenas um problema de timing

10. O login retorna sempre a mesma mensagem de erro, mas leva 480 ms para usuários existentes e 12 ms para inexistentes. Qual a falha?

A) Enumeração por canal de tempo (timing); verificar um hash fictício quando o usuário não existe

B) Cache mal configurado

C) CORS permissivo

D) Nenhuma, a mensagem é idêntica

11. Um host interno, com saída permitida apenas na porta 443, conecta a cada 60 s (±10%) a um domínio registrado há 2 dias, com payloads pequenos e uniformes. Qual a melhor hipótese e ação?

A) Beaconing de C2 sobre HTTPS; investigar o processo, isolar se confirmado e bloquear o domínio

B) Atualização normal do sistema operacional

C) Falha de sincronização NTP

D) Backup automático da nuvem

12. Um achado classificado como 'Crítico' exige acesso prévio a uma rede administrativa isolada com MFA e jump host. Como tratar a severidade?

A) Manter 'Crítico' sem contexto

B) Ajustar com métricas ambientais e pré-condições, justificar e manter o achado com remediação recomendada

C) Remover do relatório

D) Elevar para 'Urgente' por segurança

Gabarito comentado da prova de exemplo

#	Nível	Resp.	Comentário
1	PCPH	A	HTTP e HTTPS são serviços web. O SSH só deveria estar exposto com exceção documentada e controles adicionais.
2	PCPH	C	Frases longas e aleatórias têm alta entropia. As demais seguem padrões comuns, presentes em listas de senhas.
3	PCPH	B	Ter MFA é consequência de ser administrador, não condição suficiente. Muitos usuários não administradores também têm MFA.
4	PCPH	B	Agir fora do escopo invalida a autorização. A conduta correta é parar e comunicar.
5	PCCP	A	A API não verifica se o objeto pertence ao usuário autenticado.
6	PCCP	B	HttpOnly bloqueia leitura por JavaScript. Não impede que o navegador anexe o cookie a requisições forjadas.
7	PCCP	B	Primeiro reduza a superfície de ataque; depois fortaleça a autenticação e, por fim, detecte e responda.
8	PCCP	A	Mensagens distintas revelam quais contas existem. Use mensagem genérica e controles de taxa.
9	PCSP	A	Duas strings numéricas em notação científica (0e...) são iguais a 0 numericamente. Hashes de entrada diferentes podem 'colidir' logicamente.
10	PCSP	A	A verificação do hash só ocorre quando o usuário existe, o que vaza informação pelo tempo.
11	PCSP	A	Periodicidade regular com jitter, domínio recente e payloads uniformes são indicadores clássicos de beaconing.
12	PCSP	B	Severidade deve refletir contexto. Omitir o achado é pior que reclassificá-lo com justificativa.

Glossário rápido

Termo	Significado
Flag	Texto secreto (PCP{...}) que prova que você encontrou um item no laboratório.
Escopo	Lista de alvos e ações autorizadas por escrito.
IDOR/BOLA	Acesso a objetos de outros usuários por falha de autorização.
SSRF	Fazer o servidor requisitar recursos em nome do atacante.
CVSS	Sistema de pontuação de severidade de vulnerabilidades.
MFA	Autenticação multifator.

Dúvidas: contato@pablocybersec.com.br · Validação de certificados: pablocybersec.com.br
As credenciais PCP são certificações educacionais da PabloCyberSec e não são afiliadas a CompTIA, EC-Council, OffSec ou outras entidades.