**[Cybersecurity Penetration Tester](https://www.seek.com.au/job/77449215?ref=search-standalone&type=standout&origin=jobTitle" \l "sol=a157a4ce394b964ddf9d7d5c12f4b91976191689" \t "_blank)**

**About ACME**

ACME is a world leading developer of cybersecurity technology, founded in Australia and is one of Australia’s fastest growing cybersecurity companies in the APAC region. ACME is a leader in security operations technologies and has redefined the industry more than once, with its global multi award winning Crystal Eye Consolidated security platform and XDR technology.

ACME leads the way globally in areas like Cyber Threat Intelligence and Network Detection and Response technologies, actively tracking threats and creating ways to defend against the ever-changing threat landscape. ACME is an official member of Team Defence Australia and is active in protecting Australia’s critical infrastructure across Defence, Space, Finance, Health, and other critical industries.

ACME’s global team are devoted and passionate professionals who are mission driven. Our team gets to work across not just vendor dashboards, but what makes security technologies work under the hood to solve the engineering challenges faced by organisations when dealing with Cyber Threats in today's world.

With your exceptional talent, enthusiasm, and willingness to roll up your sleeves and you want to be part of a rapidly growing team of professionals in pioneering security solutions, read on….

**About the role**

Are you passionate about cybersecurity and penetration testing? Do you have a strong attention to detail and proven track-record of delivering results?

We are looking for a motivated Penetration Tester to join our Security Operations Centre, based in our Perth office, who lives and breathes cybersecurity and customer satisfaction. You will work with a team of experts to deliver exemplary internal and external services by using your strong documentation skills, ability to collaborate with others, and determination and drive for constant improvement.

In addition to performing vulnerability assessments and penetration tests, you will be performing security monitoring, security and data/log analysis and forensic analysis, to detect security incidents, and incident response. You will also investigate and utilise new technologies and processes to enhance security capabilities and implement improvements.

**Key responsibilities**

* Perform Vulnerability Assessment and Penetration Testing, including web application and network
* Pre-sales support, scoping, report writing and presentation to clients
* Work with external parties (IT teams) to plan and remediate findings
* Monitor ACME and its clients’ networks, computers and applications
* Determine and identify the damage caused by detected intrusions and how it occurred
* Recommend safeguard against similar intrusions
* Perform security research with ACME intelligence systems and malware systems
* Monitor and investigate security breaches

**About You**

* Must have Industry OSCP certification with 2-5 years of industry experience
* Ability to demonstrate technical knowledge
* Understanding of systems administration, networking and risk/compliance.
* Ability to work as a part of a team or autonomously
* Good written and verbal communication skills
* Strong customer service and problem-solving skills
* Have a passion for information security and have a desire to be key player in developing Australia’s first Extended Detection and Response platform and services
* Experience in network and security implementation and/or operations
* Good awareness of security and risk management and their implications for technical solutions
* Knowledge in intrusion IDS/IPS, firewalls and WAF
* Wide Knowledge and experience in using security tools used in offensive and defensive infrastructures
* Strong understanding of exploits, malware and digital forensics
* Knowledge of different log technologies, sources and transport methods
* Familiar in a system administration supporting multiple platforms and applications
* Ability to communicate security issues to peers and management

**Desirables**

* Experience with scripting languages (javascript, python, bash, etc.)
* Industry Certifications OSCE, CISSP, CREST, NV1

**Clearance Requirements**

* Ability to obtain and maintain an Australian Police Clearance
* Must have full Australian working rights
* Ability to obtain Defence Clearance

# Interview Script

**Interview Question 1: Experience with Vulnerability Assessment and Penetration Testing**

**Interviewer:** "Can you describe your experience with vulnerability assessments and penetration testing, particularly with web applications and networks?"

**Less Effective Response**

**Interviewee:** "I've done some vulnerability assessments and penetration testing in the past. I used common tools and checked for weaknesses."

**More Effective Response**

**Interviewee:** "In my previous role, I conducted comprehensive vulnerability assessments and penetration tests for both web applications and network infrastructures. I utilized tools such as Burp Suite, Nessus, and Nmap to identify and exploit vulnerabilities. For instance, during a recent engagement, I uncovered a critical SQL injection vulnerability in a client's web application, which could have allowed unauthorized access to sensitive data. I demonstrated the exploit to the client, explained the potential impact, and provided detailed remediation steps. My approach includes not just identifying vulnerabilities but also working closely with development and IT teams to ensure effective mitigation and improved security posture."

**Interview Question 2: Pre-Sales Support and Client Interaction**

**Interviewer:** "How have you supported pre-sales activities, including scoping and presenting reports to clients?"

**Less Effective Response**

**Interviewee:** "I've been involved in some pre-sales activities. I usually just help out when needed, like preparing reports."

**More Effective Response**

**Interviewee:** "I have actively participated in pre-sales activities by assisting in scoping potential projects and developing tailored proposals. For example, I worked with a financial services client to outline a penetration testing engagement. I collaborated with the sales team to understand the client's specific needs and concerns, then prepared a comprehensive proposal detailing the testing scope, methodologies, and expected outcomes. After completing the testing, I presented the findings to the client's executive team, using clear and non-technical language to explain the risks and recommended actions. This not only demonstrated our expertise but also built trust and confidence with the client."

**Interview Question 3: Incident Detection and Response**

**Interviewer:** "Can you share an example of how you've detected and responded to a security incident?"

**Less Effective Response**

**Interviewee:** "I've been involved in incident response. When something suspicious comes up, I check the logs and take action."

**More Effective Response**

**Interviewee:** "In one instance, I detected unusual network activity that indicated a potential breach. I immediately initiated the incident response plan, isolating the affected systems to contain the threat. Using our SIEM and forensic tools, I analyzed the logs and identified the intrusion vector, which was an outdated third-party plugin. I documented the incident, including the timeline and impact, and presented a report to the management team. My recommendations included updating the affected systems, enhancing monitoring, and implementing additional security controls. This quick and structured response helped prevent further damage and strengthened our security posture."

**Interview Question 4: Security Research and Continuous Improvement**

**Interviewer:** "How do you stay updated on the latest cybersecurity threats and technologies, and how have you applied this knowledge in your work?"

**Less Effective Response**

**Interviewee:** "I follow cybersecurity news and blogs. I try to keep up with the latest threats and tools."

**More Effective Response**

**Interviewee:** "I stay updated on the latest cybersecurity threats and technologies by regularly participating in online forums, attending cybersecurity conferences, and reading industry publications. Additionally, I conduct independent research, often setting up lab environments to test new tools and techniques. For example, I recently explored advancements in XDR technologies and integrated these insights into our threat detection strategies. This proactive learning approach allows me to bring fresh perspectives to my role, continuously improving our security practices and ensuring that we are prepared to defend against the latest threats."

**Interview Question 5: Communication and Team Collaboration**

**Interviewer:** "Can you describe a situation where you effectively communicated a complex security issue to a non-technical audience or worked as part of a team to solve a security problem?"

**Less Effective Response**

**Interviewee:** "I usually explain security issues in simple terms. I work with the team to solve problems when they come up."

**More Effective Response**

**Interviewee:** "In a recent project, I identified a complex security vulnerability related to insecure deserialization in a client's application. To ensure the client understood the severity, I presented the issue using analogies and simplified explanations, emphasizing the potential risks to their data. I also collaborated with their development team to devise a solution, providing a detailed guide on securing the application and offering follow-up support. This approach not only resolved the issue but also educated the client and their team on secure coding practices. Effective communication and teamwork were crucial in achieving a successful outcome and enhancing the client's security awareness."

**Interview Question 6: Handling Advanced Persistent Threats (APTs)**

**Interviewer:** "Can you describe your experience with detecting and mitigating Advanced Persistent Threats (APTs)?"

**Less Effective Response**

**Interviewee:** "I've read about APTs and understand that they are serious. We try to monitor our systems closely to detect them."

**More Effective Response**

**Interviewee:** "In a previous role, I was involved in a case where we suspected an APT targeting our client’s network. We noticed subtle signs of data exfiltration and unusually prolonged dwell time. To address this, I collaborated with our threat intelligence team to gather information on the threat actors and their typical TTPs (Tactics, Techniques, and Procedures). We implemented advanced monitoring using our SIEM system to detect further anomalies, and conducted a thorough forensic analysis to trace the intrusion path. Our response included isolating affected systems, eradicating the threat, and enhancing security measures such as network segmentation and endpoint protection. This experience highlighted the importance of continuous monitoring and a comprehensive response strategy in mitigating APTs."

**Interview Question 7: Experience with Security Tools and Technologies**

**Interviewer:** "What security tools and technologies are you most proficient with, and how have you used them in your work?"

**Less Effective Response**

**Interviewee:** "I've used various security tools like antivirus software and firewalls. They're essential for protecting systems."

**More Effective Response**

**Interviewee:** "I have extensive experience with a variety of security tools and technologies. For vulnerability assessments and penetration testing, I frequently use tools like Nessus for automated scans and Burp Suite for web application testing. I am proficient with Metasploit for exploit development and testing, and I utilize Wireshark for network traffic analysis. Additionally, I have experience with IDS/IPS systems like Snort and WAFs for protecting web applications. My role often involves integrating these tools into a cohesive security strategy, which includes using SIEM platforms like Splunk for monitoring and correlating security events. This diverse toolkit enables me to identify, analyze, and respond to a wide range of security threats effectively."

**Interview Question 8: Collaboration with External Parties and Clients**

**Interviewer:** "How do you collaborate with external IT teams or clients to address security findings and implement remediation measures?"

**Less Effective Response**

**Interviewee:** "I usually share the findings with the external teams and tell them what needs to be done. We discuss the next steps."

**More Effective Response**

**Interviewee:** "Collaboration with external IT teams and clients is crucial for effective remediation of security findings. After conducting a penetration test or vulnerability assessment, I present the findings to the relevant stakeholders, explaining the vulnerabilities in a clear and understandable manner. I prioritize the issues based on their severity and potential impact, and work closely with the client's IT team to develop a remediation plan. This often involves technical guidance on implementing patches, reconfiguring systems, or enhancing security controls. I also provide follow-up support to ensure that the remediation measures are correctly implemented and effective. This collaborative approach not only addresses the immediate issues but also strengthens the client’s overall security posture."

**Interview Question 9: Understanding and Mitigating Security Breaches**

**Interviewer:** "Can you discuss a time when you investigated a security breach and what steps you took to mitigate it?"

**Less Effective Response**

**Interviewee:** "We had a security breach once. I helped investigate and we fixed the problem as soon as we could."

**More Effective Response**

**Interviewee:** "In one notable incident, we detected a security breach involving unauthorized access to sensitive data. My role was to lead the investigation, starting with identifying the compromised systems and understanding the scope of the breach. We found that the attackers exploited a vulnerability in an outdated application. To mitigate the breach, we immediately isolated the affected systems to prevent further access, then worked on patching the vulnerability. We also performed a thorough review of access logs to determine the extent of the data exposure. Post-incident, I led a debriefing session with the team to analyze our response and implement additional security measures, including enhancing our incident detection capabilities and conducting more frequent vulnerability assessments. This experience underscored the importance of a rapid and coordinated response to security breaches."

**Interview Question 10: Contribution to Cybersecurity Research and Development**

**Interviewer:** "How have you contributed to cybersecurity research and the development of new security technologies or methodologies?"

**Less Effective Response**

**Interviewee:** "I've been interested in cybersecurity research. I've read about new technologies and sometimes share ideas with my team."

**More Effective Response**

**Interviewee:** "I have actively contributed to cybersecurity research and the development of new methodologies. At ACME, I participated in a research project focused on enhancing our Network Detection and Response (NDR) capabilities. My work involved analyzing current detection techniques and identifying gaps in our existing system. I proposed a new approach that incorporated machine learning algorithms to better identify anomalous patterns indicative of advanced threats. This led to the development of a prototype that significantly improved our threat detection rate. Additionally, I regularly contribute to our internal knowledge base, sharing insights on the latest vulnerabilities and attack vectors, and proposing new defense strategies. This involvement not only advances our technological capabilities but also helps keep our team informed and prepared for emerging threats."