DETEACT	https://pentest.deteact.ru/

Проект матрицы компетенций для понимания, как профессионально расти пентестеру. Ниже инструкция, как читать.

Skills: Примерный список основных вещей, которые уже пора бы знать.
Salary: Сферическая вилка в вакууме
Certification: Сертификации, на которые можно посмотреть, как на приблизительный ориентир (их наличие или отсутствие ничего не гарантирует)
How to grow: Варианты дальнейшего развития для этой стадии

Очевидно, что в пентесте есть много разных специализаций, и нельзя всё поделить на 6 уровней и 2 специальности.
Поэтому, нельзя список навыков считать полным или точным, поскольку это скорее должен быть не линейный список, а дерево.
Ещё одна проблема -- размытость формулировок. Что такое "знать"? Каждый интерпретирует по-разному.
В формате гугл-таблички полноценное описание дать слишком сложно.
Тем не менее, кажется, что процентов 80 в каждой строке можно считать обязательными (а какие именно 80% -- зависит от специализации).

Этот черновик может изменяться, дополняться.

Level	Experience	Skills	Salary	Certification	How to grow	Criteria
Intern	до 1 года	Знание принципов протокола HTTP; Умение пользоваться основными функциями Burp Suite и других популярных сканеров (ZAP / Acunetix / Netsparker / Arachni); Навыки OSINT и багхантерской разведки; Владение каким-то популярным стеком веб-технологий на уровне, чтоб мог разобраться в устройстве приложения (и прочитать код в случае чего); Знание сути багов из OWASP Top 10, и как их обнаружить, эксплуатировать и фиксить.	до 60 т. р.		OWASP Top 10 Лабы и инструменты	
Junior	~1 год	Знание Linux на уровне продвинутого пользователя; Умение писать простые скрипты для работы с сетью, чтоб парсить что-то (знание регулярных выражений), эксплуатировать баги и т. д; Знакомство с OWASP Testing Guide, понимание этапов анализа защищённости и соответствующего инструментария; Знание основ сетевых технологий (понимание сути TCP/IP, настройка маршрутизации).	60-90 т. р.		Программирование Учить всё про веб	
Middle-	1-2 года	Уверенное владение всем необходимым инструментарием (Burp Suite, расширения, различные сканеры и нюансы их конфигурации); Понимание методологии пентестов и подходов к аппсеку, умение формулировать стандартные рекомендации по исправлению багов; Базовые навыки сетевого пентеста (сканирование портов и уязвимостей, Metasploit, повышение привилегий и закрепление в Linux), Знание векторов эксплуатации SQL-инъекций (разные СУБД), XSS (разные контексты, браузеры), Умение придумывать логические атаки, эксплуатировать ошибки авторизации, состояния гонки и т. д.	90-120 т. р.	OSCP	Методологии пентеста Постановка задач Инфраструктурный пентест	Не менее полугода на предыдущей позиции Самостоятельно обнаруживает уязвимости на всех проектах Обеспечивает полноценное покрытие стандартными тестами в своей зоне ответственности Даёт адекватное описание и PoC для обнаруживаемых уязвимостей
Middle	2-3 года	Умение корректно оценивать уровень риска уязвимостей; Свои наработки и инструменты, умение писать эксплойты, скрипты или расширения для Burp Suite, эффективно работать с HTTP на своём рабочем ЯП; Уверенное владение одним стеком веб-технологий, умение читать код и разбираться в архитектуре 2-3 других стеков (например, практические умения кодить под Django + опыт анализа проектов на Node.JS); Знакомство с различными протоколами и атаками на них (OAuth, JWT, GraphQL, websockets, GWT, Faces, и т. д.); Понимание механизмов безопасности браузеров (SOP, cookies, CSP, HSTS, и т. д.).	120-160 т. р.	OSWE eWPTX	DevSecOps Application Security	Не менее полугода на предыдущей позиции
Middle+	3-4 года	Знакомство с фронтендом, умение отлаживать фронт, понимание принципов JS-фреймворков (React, Vue.JS); Умение обходить WAF, обфусцировать пейлоады Опыт написания рекомендаций по исправлению уязвимостей с учётом особенностей проекта; Умение разбивать пентест на подзадачи для управления собственным временем, для быстрого достижения результата или для делегирования; Умение анализировать архитектуру системы, строить модели угроз и продумывать сценарии эксплуатации, находить слабые точки.	160+ т. р.		Исследовательская работа Soft skills Консалтинг	Не менее полугода на предыдущей позиции
Senior	4-5 лет	Экспертное владение как минимум одним стеком веб-технологий, знание всех известных нюансов, методов эксплуатации, митигейшнов, обходов; Хороший опыт анализа защищённости 2-3 других стеков (было несколько больших проектов с десятками тысяч строк кода, есть понимание специфичных атак и нюансов ЯП); Знание различных парадигм программирования и паттернов проектирования; Знание особенностей различных СУБД, поднятия привилегий в СУБД; Базовые навыки криптоанализа (режимы шифрования, bit flipping, padding oracle); Знакомство с legacy-технологиями, устаревшими векторами атак, историей развития технологий взлома; Опыт исследования новых методов взлома или защиты или создания инструментов (не меньше нескольких тысяч строк кода); Более широкое понимание подходов appsec, DevSecOps, а также бинарных уязвимостей; Глубокое знание всех типов атак на веб-приложения (CWE, OWASP Top 10).	210+ т. р.		Глубокие исследования Бинарщина, железо Менеджмент Продажи	

Level	Experience	Skills	Salary	Certification	How to grow	Criteria
Intern	до 1 года	Знание Linux на уровне продвинутого пользователя; Навыки OSINT и корпоративной разведки (поиск хостов и email); Знание основ сетевых технологий (понимание сути TCP/IP, настройка маршрутизации). Умение пользоваться Kali Linux, Metasploit, Nmap, Wireshark, Nessus, OpenVAS, masscan.	до 60 т. р.		HTB Лабы и инструменты	
Junior	~1 год	Знание принципов протокола HTTP; Умение пользоваться MSF DB, responder, mimikatz, incognito, psexec; Понимание всех практичных атак на Wi-Fi; Умение писать простые скрипты для работы с сетью, чтоб парсить что-то (знание регулярных выражений), эксплуатировать баги и т. д;;	60-90 т. р.	eJPT CEH Practical	Программирование Учить всё про пентест	
Middle-	1-2 года	Уверенное владение bash, powershell, cmd, навыки автоматизации атак; Понимание методологии и этапов пентеста, умение разделять скоуп; Умение осуществлять пивотинг, горизонтальное перемещение; Знание особенностей ОС Linux и Windows (система прав, конфигурирование пользователей и устройств, встроенные средства защиты) Знание методов повышения привилегий для Windows и Linux; Знание методов закрепления в системе и обхода антивирусов. Знание сути багов из OWASP Top 10, умение пользоваться Burp Suite.	90-120 т. р.	OSCP CCNA	Методологии пентеста Постановка задач Веб-пентест	Не менее полугода на предыдущей позиции Самостоятельно обнаруживает уязвимости на всех проектах Обеспечивает полноценное покрытие стандартными тестами в своей зоне ответственности Даёт адекватное описание и PoC для обнаруживаемых уязвимостей
Middle	2-3 года	Знание различных сетевых протоколов (в т.ч. Cisco), типов сетевого оборудования; Знание принципов работы, основных атак на AD и инструментов; Умение пользоваться продвинутыми функциями Metasploit, умение писать свои модули; Знание DCOM, WMI, PS Remoting, WinRM; Умение проводить тестирование бесшумно, не оставлять следов, проводить зачистку после работ; Навыки социальной инженерии, генерации разных типов пейлоадов, проведения рассылок, обзвонов, создания фейков и обхода антиспама; Знание основных атак на AWS, Google Cloud, Kubertnetes, Docker.	120-160 т. р.	OSCE CCNA Security eCCPTv2	Винда AD Сети	Не менее полугода на предыдущей позиции
Middle+	3-4 года	Отличное знание безопасности AD и Windows, умение проводить продвинутые атаки; Знакомство с OWASP Testing Guide, умение обнаруживать, эксплуатировать и исправлять типовые веб-уязвимости; Навыки анализа кода на C#/Java/Python; Умение проводить атаки на различные протоколы (STP, CDP, VLAN Hopping), пользоваться инструментом yersinia; Навыки программирования на C# и Python; Знания в области DevOps, сетевой архитектуры, систем мониторинга, средств защиты, SIEM/IPS/EDR.	160+ т. р.	eCPPTXv2 CCNP Security	Исследовательская работа Soft skills Консалтинг	Не менее полугода на предыдущей позиции
Senior	4-5 лет	Навыки разработки и отладки бинарных эксплойтов, шеллкодов; Умение имплементировать сетевые атаки (python scapy); Умение обходить средства защиты IDS/IPS/NGFW при помощи кастомных пейлоадов и туннелей; Умение осуществлять все этапы MITRE ATT&CK Kill Chain; Навыки Red Teaming, hardware hacking, создания прошивок для злых девайсов, работы с RFID; Обширные знания безопасности облачных технологий.	210+ т. р.		Глубокие исследования Бинарщина, железо Менеджмент Продажи	