MODULE 01 // ESSENTIALS & ARCHITECTURE

Introduction to Ethical Hacking & Information Security

A strategic exploration of vulnerability discovery, governance models, and proactive defense.

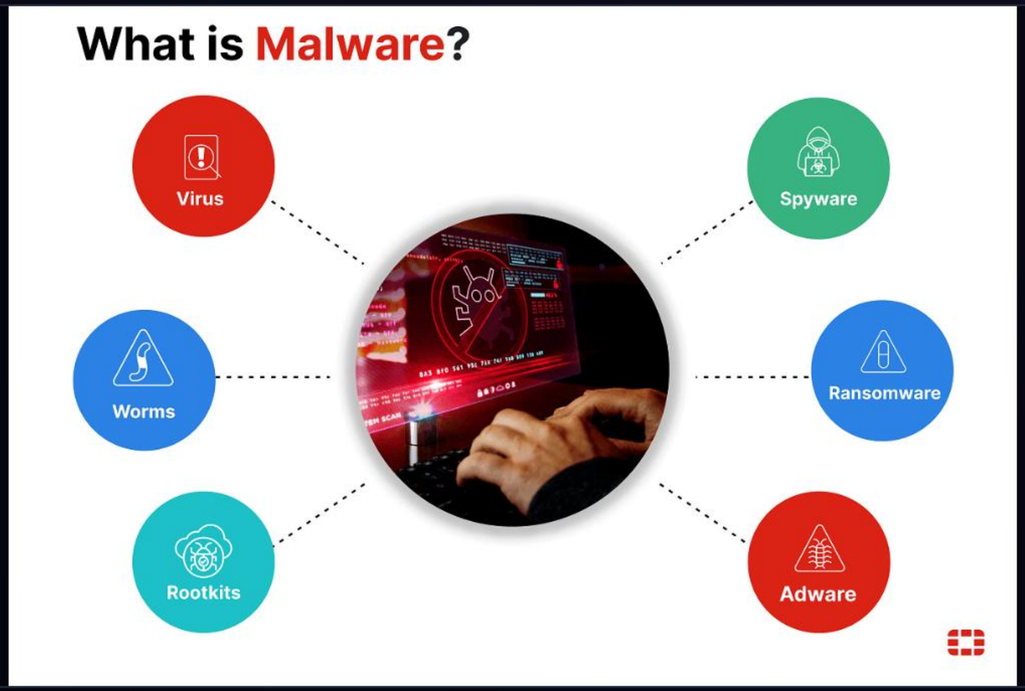
1. HACKING IMPACTS
2. THE PHASES MODULE
3. COMPLIANCE & POLICY
4. ATTACK VECTORS
5. SECURITY PROGRAMS
6. PROACTIVE PROTECTION

The Real Impact of Hacking

Devastating Cost of Breaches

Security breaches are no longer just an IT concern—they pose major, long-term risks to organizations.

- **Financial Depletion:** Severe direct loss and clean-up costs.
- **Regulatory Penalties:** Stringent fines for compliance failures.
- **Operational Failure:** Complete disruption of critical workflows.
- **Reputational Harm:** Permanent erosion of customer trust.



The Ethical Hacker Framework

1. Prep

Defining scope, testing boundaries, and establishing RoE.

2. Recon

Gathering passive intelligence and public profiles.

3. Scan

Mapping internal services, subnets, and live targets.

4. Analyze

Locating vulnerabilities and missing patches.

5. Exploit

Testing entry vectors safely to prove risk impact.

6. Report

Delivering strategic reports and integration plans.

Planning and Sound Operations

Planning the Assessment

Strategic foundations ensure all scanning and testing remains controlled:

- **Set Scope:** Explicitly delineate target IP addresses.
- **Formal Authorization:** Ensure legal written consent.
- **RoE Definition:** Agree on tools and test timing.
- **Target Assets:** Clarify critical servers to avoid.

Maintaining Sound Operations

Strict execution standards protect client systems from downtime:

- **Professional Integrity:** Secure storage of data.
- **Legal Compliance:** Avoid stepping outside agreed limits.
- **Timing Limits:** Schedule intrusive scans off-peak.
- **Session Log:** Log actions for verification.

Recon, Scan, and Analysis

Reconnaissance

The information-gathering phase. Using passive methods like WHOIS queries and active methods like basic web-header searches to outline target terrain.

Enumeration

Mapping details: cataloging users, identifying open services (DNS, SMB, LDAP), and finding specific configuration points across local hosts.

Vulnerability Analysis

Reviewing scans to identify security gaps. Testing systems against database patches to identify entry pathways.

Exploitation and Delivery

Validating and Patching Gaps

Exploitation demonstrates real risk by executing targeted payloads to verify if vulnerabilities can be used to bypass system boundaries.

The final analysis bridges the gap between active pen testing and executive board governance. Findings are packaged into an actionable deliverable, which is then integrated directly into development and operational workflows to build layered defenses.

Major Information Security Models

Computer Security

Hardens individual devices against exploits. Focuses on endpoint patching, disk encryption, local permissions, and registry safety controls.

Network Security

Defends connection channels. Implements perimeter next-gen firewalls, sub-net segmentation, and secure routing structures.

Service Security

Secures shared data. Protects core cloud and database workloads from API abuse and malicious data queries.

Application Security

Hardens running software code. Safeguards web applications from injection scripts, poor auth rules, and third-party dependencies.

The InfoSec Program Lifecycle

1. Identify

Cataloging key data and hardware assets.

2. Assess

Evaluating active threats and gaps.

3. Design

Formulating defensive control models.

4. Deploy

Implementing firewalls, patches, and MFA.

5. Monitor

Deploying continuous SIEM log streams.

6. Respond

Initiating playbooks to contain breaches.

7. Evolve

Iteratively updating plans after audits.

InfoSec Program Architecture

Program Key Component	Operational Objective	Mitigation Value
Security Policies & Procedures	Establish administrative rules and corporate configuration requirements.	Maintains consistent configurations and regulatory compliance.
Access Control & Auditing	Limit administrative credentials using role-based authentication rules.	Reduces threat movement and mitigates unauthorized changes.
Incident & Continuity Planning	Create responsive runbooks to isolate nodes and restore data.	Reduces recovery time and minimizes financial impact.
Compliance & Monitoring	Verify configurations against security frameworks.	Guarantees active auditing and compliance alignment.

Proactive Risk Management

The Role of Risk Analysis

Asset Worth: Gauge the value and criticality of systems containing sensitive data.

Likelihood Assessment: Multiply vulnerabilities by threat capabilities to evaluate real-world probability.

```
Objective: Pivot from generic patches to priority threat modeling.
```

The Role of Ethical Hacking

Proactive Assessment: Uncover hidden pathways and logical misconfigurations before real-world attacks occur.

Control Validation: Move beyond static assessments to demonstrate the actual resilience of defenses.

```
Goal: Prove threat impact to get board alignment and sign-off.
```

Image Sources

https://marvel-b1-cdn.bc0a.com/f00000000310757/www.fortinet.com/content/dam/fortinet/images/cyberglossary/what-is-malware.png

Source: www.fortinet.com

https://static.vecteezy.com/system/resources/previews/069/462/579/non_2x/mobile-data-protection-concept-with-digital-shield-icon-secure-information-storage-and-cybersecurity-defense-system-for-preventing-hacking-breaches-and-online-threats-encryption-technology-free-photo.jpg

Source: www.vecteezy.com